OXFORD MATHEMATICAL MONOGRAPHS

G-Algebras and Modular Representation Theory

JACQUES THÉVENAZ

OXFORD SCIENCE PUBLICATIONS

Jacques Thévenaz

G-algebras
and
modular representation theory

Oxford University Press, Walton Street, Oxford OX2 6DP

Oxford New York
Athens Auckland Bangkok Bombay
Calcutta Cape Town Dar es Salaam Delhi
Florence Hong Kong Istanbul Karachi
Kuala Lumpur Madras Madrid Melbourne
Mexico City Nairobi Paris Singapore
Taipei Tokyo Toronto

and associated companies in
Berlin Ibadan

Oxford is a trade mark of Oxford University Press

Published in the United States
by Oxford University Press Inc., New York

A catalogue record for this book is available from the British Library

Library of Congress Cataloging in Publication Data
(Data available)

ISBN 0 19 853587 2

Typeset by the author

Printed and bound in Great Britain by
Biddles Ltd, Guildford and King's Lynn

to Georges Vincent

who first taught me algebra

Preface

This book presents a new approach to the modular representation theory of a finite group G. Its aim is to provide a comprehensive treatment of the theory of G-algebras and to show how this theory is used to solve various problems in representation theory. Significant results have been obtained over the last 15 years by means of this approach, which also sheds new light on modular representation theory. So it appears that a need has arisen for an expository book on the subject. I hope to meet this need and to introduce a wider audience to these new ideas.

The modular representation theory originated in the pioneering work of R. Brauer, who defined and studied blocks of characters of finite groups, developed many important ideas, proved deep structural results, and applied with success the theory to the structure of finite groups. The next important stage in the development of the theory is due to J.A. Green, who started the systematic study of indecomposable modules over group algebras and found many of their important properties. He also introduced some crucial concepts which unify and extend earlier work; he showed in particular that G-algebras can be used as a tool for handling both the block theory and the G-module theory.

A major new stage started in the late seventies with the work of J.L. Alperin, M. Broué, and L. Puig, who set the foundations of the p-local theory of blocks and representations. Alperin and Broué introduced the Brauer pairs (also called subpairs) and these were used by Broué and Puig in their work on nilpotent blocks. Refining this notion, Puig defined the concept of pointed group on a G-algebra and developed during the eighties the general theory of pointed groups. Some deep results were proved by means of this new approach, the most striking achievement being Puig's theorem on nilpotent blocks which determines entirely the representation theory of such a block.

This book is a systematic treatment of Puig's theory of G-algebras and pointed groups, with applications to block theory and G-module theory. Many classical results of modular representation theory are also included, but often stated or proved in a non-classical way. First the general theory is developed: the defect theory of pointed groups, source algebras, multiplicity modules, the Puig and Green correspondences, and various other general results. Then the module theory is discussed: the parametrization of indecomposable G-modules, p-permutation modules, endo-permutation modules, sources of simple modules, diagrams, almost split sequences and their defect groups. The next topic is block theory: source algebras of blocks, Brauer pairs, the classical main theorems of Brauer, blocks with a normal defect group, structural results about source algebras, and Robinson's theorem on the number of blocks with a given defect group. A whole chapter is concerned with control of fusion and nilpotent blocks: Alperin's fusion theorem, Puig's theorem on the source algebras of nilpotent blocks, and the computation of ordinary characters of nilpotent blocks. Finally, the last chapter presents a generalization of the defect theory of pointed groups to the case of maximal ideals in G-functors.

Some further developments of the theory of G-algebras are not treated in this book, in particular source algebras of blocks with cyclic defect group or Klein four defect group, extensions of nilpotent blocks, blocks of symmetric groups and Chevalley groups, the parametrization of primitive interior G-algebras, and the analogue of Brauer's second main theorem for G-modules. However this text should be a sufficient introduction to the research papers concerned with these topics. It should also be noted that many other aspects of modular representation theory are not mentioned here and appear in other books.

Apart from a systematic introduction to the theory of G-algebras and pointed groups, the main aim of the book is to show how Puig's new point of view can be applied in various situations. This approach is not used in other books about modular representation theory, with the single exception of the short lecture notes by Külshammer [1991a]. However the aim of Külshammer's book is essentially to prove Puig's theorem about nilpotent blocks in characteristic p. The more difficult result in characteristic zero is included here and of course the theory of G-algebras is also developed in many other directions.

I have not tried to attribute each result of this text to some mathematician, but I have rather included short notes (at the end of the first chapter and then at the end of each section from Section 10 onwards). I tried in these notes to give credit to the mathematicians who contributed significantly to some of the results of the text and I sometimes made some remarks about further developments. At the end of each section, I have also gathered a few exercises. Many of them are just easy applications of the theory and none of them is supposed to be difficult. In fact I have often included generous hints which sometimes are close to a complete solution.

This book would not have existed without Lluis Puig's influence. Of course his contribution to the mathematical results presented here is essential, but I also benefitted from numerous conversations with him. He

explained to me many aspects of his work, including unpublished results and open questions, and gave me copies of various personal notes which were very helpful. Finally he made valuable comments and suggestions about the first chapters of this book. It is a great pleasure to thank him for all the help he gave me during the many years of our acquaintance.

I am also indebted to many other people for assisting me with this work. In a private lecture about Puig's theorem, Markus Linckelmann explained to me all the details of the proof and on this occasion found a significant simplification of one of Puig's arguments. He also read the first chapters of this book and made numerous suggestions. Paul Boisen read carefully the first six chapters, spotted various mistakes, and often contributed to the improvement of the text by correcting my English. Burkhard Külshammer made useful comments about several chapters. Some parts of the manuscript were also read by J.L. Alperin, D. Arlettaz, L. Barker, M. Broué, H. Fottner, J.A. Green, M. Harris, G.I. Lehrer, M. Ojanguren, P. Symonds, and P. Webb, who made useful remarks and suggestions. I wish to express my gratitude to all these people for their help. I also thank Walter Feit for allowing me to include his conjecture about sources of simple modules and Marc Burger who convinced me of the need to write a detailed introduction to the subject and who made useful comments about it. Finally, I am grateful to Nicolas Repond and Pierre Joyet who solved the numerous problems I faced while preparing the manuscript in TeX.

I have to apologize for the style in which this book is written. English is a beautiful language which ought to be reserved to native writers. I am sorry that the rules of the international scientific world have encouraged me to write this book in a language which is foreign to me. As a result, the style of this text is as far from actual English as ordinary sounds are from music.

Jacques Thévenaz
Lausanne, October 1994

Contents

Introduction

Within the representation theory of a finite group G, the modular theory deals with a fixed prime number p and is concerned with all the finer properties of representations which can be obtained by looking specifically at p. The prime p comes into play essentially in two ways. Firstly representations can be realized over some ring of integers and reduced modulo p, so that one ends up with representations over a field of characteristic p; the interplay between characteristic zero and characteristic p is crucial. Secondly one deals with all elements of G whose order is either prime to p or a power of p; more generally one considers also all subgroups of G whose order is a power of p (called p-subgroups).

In this introduction, we wish to convey some of the main ideas of the subject and show how the development of the theory leads to several new concepts which are studied in this book. Before we can discuss the modular theory, it is necessary to recall some standard results of ordinary representation theory.

Ordinary representation theory

Let K be a field of characteristic zero. We suppose that K is large enough in the sense that K contains all $|G|$-th roots of unity, where $|G|$ denotes the order of the group G. In the classical theory, K is the field of complex numbers, but this does not play any important role and we shall actually need another choice of K. The group algebra of G with coefficients in K is the K-algebra KG having G as a basis, with bilinear multiplication induced by the product of basis elements. A KG-module is also called a *representation* of G over K. We assume that all modules are finitely generated and this amounts here to the condition that they have finite dimension as K-vector spaces.

By Maschke's theorem, the group algebra KG is semi-simple. Since K is large enough, it follows from Wedderburn's theorem that the group algebra is isomorphic to a direct product of matrix algebras

$$KG \cong \prod_{i=1}^{r} M_{n_i}(K) \, .$$

Moreover any KG-module V can be written $V = \bigoplus_{i=1}^{r} V_i$, where V_i is a module over $M_{n_i}(K)$ (with zero action of the other factors of the product). In other words the category $\text{mod}(KG)$ of KG-modules decomposes as the direct product of the categories $\text{mod}(M_{n_i}(K))$. Now there is only one simple $M_{n_i}(K)$-module S_i up to isomorphism and every $M_{n_i}(K)$-module is isomorphic to a direct sum of copies of S_i. This reduces the classification of KG-modules to the listing of the r distinct simple modules S_i, called the *irreducible* representations of G over K.

The *character* of a KG-module V is the function $\chi_V : G \to K$ mapping g to the trace of the action of g on V (that is, the trace of the matrix representing the action of g with respect to some K-basis of V). By elementary properties of the trace, every character is a central function, that is, it is constant on every conjugacy class of group elements. The *irreducible characters* are the characters χ_i of the simple KG-modules S_i and the *character table* of G is the matrix $(\chi_i(g))$ where χ_i runs over the set of all irreducible characters and g runs over the set of all elements of G up to conjugation. A basic result asserts that the character table is a square matrix. Many properties of the group G are encoded in this matrix. For instance all the normal subgroups of G can be reconstructed from the knowledge of the character table.

One of the purposes of the modular representation theory is to find new information on this table by working with a fixed prime number p. One of the original ideas of R. Brauer, who initiated the modular theory, was to deduce results about the structure of G from this new kind of information. He applied this programme with success and proved deep group theoretical results by means of this approach.

Block theory

In order to be able to reduce modulo p, we need a suitable ring of integers in K, hence a suitable choice of K. We choose a principal ideal domain $\mathcal{O}$ with field of fractions K of characteristic zero, and since we have fixed a single prime p, it is enough to work with a local domain (in other words a discrete valuation ring). We let $\mathfrak{p}$ be the unique maximal ideal of $\mathcal{O}$ and we assume that the residue field $k = \mathcal{O}/\mathfrak{p}$ has characteristic p. As in the case of ordinary representation theory, the main theory is developed over an algebraically closed field; so we assume that k is algebraically closed. Finally, for technical reasons, we assume that $\mathcal{O}$ is complete with respect to the $\mathfrak{p}$-adic topology; this allows us to lift roots of polynomials from k to $\mathcal{O}$ (Hensel's lemma) and also to lift idempotents in algebras. We note that it is a standard result of ring theory that such a ring $\mathcal{O}$ exists.

We consider the group algebra $\mathcal{O}G$ with coefficients in $\mathcal{O}$ and its reduction modulo $\mathfrak{p}$, namely the group algebra kG. In contrast with the situation over K, we cannot in general decompose $\mathcal{O}G$ as a direct product of matrix algebras, but we can obviously decompose it as much as possible. We let

$$\mathcal{O}G \cong \prod_{j=1}^{m} B_j$$

be the finest possible decomposition as a direct product (which is unique up to isomorphism) and we let b_j be the corresponding central idempotent of $\mathcal{O}G$ (namely b_j projects to 1 in B_j and to zero in all the other factors). In other words we have a decomposition $1 = \sum_{j=1}^{m} b_j$ into central idempotents which are *orthogonal* (that is, $b_j b_i = 0$ if $j \neq i$) and *primitive* in the centre of $\mathcal{O}G$ (that is, b_j cannot be decomposed as a sum of two non-zero orthogonal central idempotents). Thus we have $B_j \cong \mathcal{O}Gb_j$, called a *block algebra*, while the idempotent b_j itself is called a *block idempotent* of $\mathcal{O}G$. We shall also simply call b_j a block of G. We note that the blocks are uniquely determined central elements of $\mathcal{O}G$. We also note that $\mathcal{O}Gb$ is a subalgebra of $\mathcal{O}G$, but with a different unity element, namely b.

Let b be a block of G and let $\mathcal{O}Gb$ be the corresponding block algebra. By reduction modulo $\mathfrak{p}$, we obtain over k a block algebra $\mathcal{O}Gb/\mathfrak{p}{\cdot}\mathcal{O}Gb = kG\bar{b}$, where $\bar{b}$ is the image of b. Since $\mathcal{O}$ is complete, this k-algebra is indecomposable (because one can lift idempotents from kG to $\mathcal{O}G$). Therefore, for the block decomposition of the group algebra, it is immaterial whether one works over k or over $\mathcal{O}$. Note that $\mathcal{O}Gb$ is free as an $\mathcal{O}$-module and the image in $kG\bar{b}$ of an $\mathcal{O}$-basis of $\mathcal{O}Gb$ is a k-basis of $kG\bar{b}$.

We can also extend scalars to the field of fractions K of $\mathcal{O}$ and consider the K-algebra KGb. Any $\mathcal{O}$-basis of $\mathcal{O}Gb$ is also a K-basis of KGb. Considering the decomposition of KG as the direct product of matrix algebras, we see that KGb is isomorphic to the direct product of a certain subset of the set of matrix algebras appearing in the decomposition of KG. But every matrix algebra corresponds to an irreducible representation of G over K. So we have partitioned the set of irreducible representations of G over K into "blocks": with each block algebra $\mathcal{O}Gb$ are associated certain irreducible representations of G over K; explicitly the block idempotent b acts as the identity map on each of them and annihilates all the irreducible representations associated with other blocks.

Similarly indecomposable $\mathcal{O}G$-modules are associated with a block. If V is an indecomposable $\mathcal{O}G$-module or kG-module, then $V = bV$ for some block idempotent b, and b acts as the identity map (while V is annihilated by the other block idempotents). In fact the whole representation theory over $\mathcal{O}$ or over k is partitioned naturally into blocks. In particular the set of simple kG-modules (also called modular irreducible representations) is partitioned by the blocks of G.

One of the main goals of modular representation theory is to understand the structure of a block algebra $\mathcal{O}Gb$ and of the associated module category $\mathrm{mod}(\mathcal{O}Gb)$ (which includes $\mathrm{mod}(kG\bar{b})$ since any $kG\bar{b}$-module can be viewed as an $\mathcal{O}Gb$-module). By the Krull–Schmidt theorem (which holds because $\mathcal{O}$ is complete), every module decomposes into indecomposable summands in a unique way up to isomorphism. It should be noted that there are in general infinitely many non-isomorphic indecomposable $kG\bar{b}$-modules. Thus the module category of $\mathcal{O}Gb$ can be considerably more complicated than that of KGb.

It may happen that a block algebra $\mathcal{O}Gb$ is simply isomorphic to a matrix algebra $M_n(\mathcal{O})$, in which case $KGb \cong M_n(K)$ (so that there is a unique simple KG-module associated with b) and similarly $kG\bar{b} \cong M_n(k)$ (so that there is also a unique simple kG-module associated with b). Such a block is called a block of *defect zero*, and it is the most elementary possibility. If p does not divide $|G|$, each block is of this form; in particular the representation theory over k is just the same as that over K if p does not divide $|G|$. So we really only have to consider groups of order divisible by p. For those who know about groups of Lie type, we note that any Chevalley group in natural characteristic p always has a block of defect zero, whose unique simple module is the Steinberg module.

We need to consider blocks with a higher level of complexity. The first invariant which measures this complexity is the *defect group* of the block, which will be defined later. It is a p-subgroup of G (unique up to conjugation), hence sandwiched somewhere between the trivial subgroup and a Sylow p-subgroup. This subgroup is trivial precisely for a block of defect zero. At the other extreme, it is a Sylow p-subgroup if the block is for instance the *principal block*, namely the unique block which contains the trivial one-dimensional representation of G.

Now we can explain one of the most crucial ideas of block theory. When one allows G to vary (for instance in some specific class of finite groups), there are numerous examples of an infinite family of blocks which all look the same: they all have equivalent module categories and they all have identical behaviour as far as character values are concerned (more precisely they all have the same matrix of generalized decomposition numbers, see below). So all these blocks are equivalent, in a sense which will be made precise when we introduce source algebras. A natural necessary condition for this phenomenon to happen is that all these equivalent blocks have the same defect group (which must therefore be a subgroup of all finite groups under consideration). As an example of this, all blocks of defect zero are equivalent.

This kind of observation immediately leads to the question of classifying blocks up to equivalence. It is conjectured that for a given p-group P, there are finitely many equivalence classes of blocks with defect group P. We shall return to this point.

Character theory and decomposition theory

We already understand the concept of the character of a KG-module and this is called an *ordinary character*. There is also the notion of *modular character*, which is attached to every kG-module M. This is a function $\phi_M : G_{\mathrm{reg}} \to K$ defined on the set of all elements of G of order prime to p (called p-regular elements), with values in the field K of characteristic zero. If $s \in G_{\mathrm{reg}}$, we can restrict M to the cyclic subgroup S generated by s and get a kS-module, written $\mathrm{Res}^G_S(M)$. Since p does not divide $|S|$, we can lift $\mathrm{Res}^G_S(M)$ uniquely to a KS-module $\widetilde{M_S}$ (because the representation theories over k and over K are the same). Now we can take the ordinary character of $\widetilde{M_S}$ and evaluate it on s; this gives the definition of $\phi_M(s)$. If M is a simple kG-module, then its modular character ϕ_M is called *irreducible*. We note that it would not be a good idea to define modular characters by simply using traces over k, because if a diagonal entry of a matrix appears p times then its contribution to the trace is zero and one loses quite a lot of information. This is why we use the process of lifting from k to K. Another reason is that we can now compute everything in K and therefore relate ordinary characters and modular characters.

Ordinary characters and modular characters are connected by means of the generalized decomposition numbers, which we now define. First recall that any element $g \in G$ can be written uniquely as a product $g = us$, where s is p-regular, u is a p-element (that is, the order of u is a power of p), and u and s commute. Thus for any p-element u, we have to consider all p-regular elements which commute with u, and this is the set $C_G(u)_{\mathrm{reg}}$, where $C_G(u)$ denotes the centralizer of u. Now the modular characters of the group $C_G(u)$ are functions on $C_G(u)_{\mathrm{reg}}$. If χ is an ordinary irreducible character of G and if we fix a p-element u, then the function

$$C_G(u)_{\mathrm{reg}} \longrightarrow K\,, \qquad s \mapsto \chi(us)$$

is a central function on $C_G(u)_{\mathrm{reg}}$ and therefore is uniquely a linear combination of the irreducible modular characters ϕ (because they form in fact a basis of the space of central functions on $C_G(u)_{\mathrm{reg}}$). The coefficient of ϕ is an element of K (which is actually a sum of roots of unity). It is written $d_\chi(u,\phi)$ and is called a *generalized decomposition number* (it is not called generalized in case $u = 1$). Therefore the ordinary character value of χ on the element $g = us$ can be written

$$\chi(us) = \sum_\phi d_\chi(u,\phi)\phi(s)$$

where ϕ runs over the set of all irreducible modular characters of $C_G(u)$.

We have already hinted that the blocks partition the whole representation theory and this is crucial here. Indeed one can show that the blocks of G partition the irreducible modular characters of $C_G(u)$, so that every such character ϕ is associated with some block of G. Moreover, if the ordinary character χ is associated with a block b but if ϕ is not associated with b, then $d_\chi(u,\phi) = 0$. Thus in some sense the character values of χ can be computed within the block b.

Another important fact is that $d_\chi(u,\phi) = 0$ if u does not belong to a defect group of b. In particular χ necessarily vanishes on us if u is not contained in a defect group of b. This is a very strong restriction on the character table of G: if for instance b is a block of defect zero, then its unique ordinary character χ vanishes on all elements of order divisible by p.

The numbers $d_\chi(u,\phi)$ form a matrix with rows indexed by the set of all ordinary characters χ associated with b and columns indexed by conjugacy classes of pairs (u,ϕ), where u is a p-element in a defect group of b and ϕ is an irreducible modular character of $C_G(u)$ associated with b. This is in fact a square matrix called the *generalized decomposition matrix* of the block b.

We have already mentioned the idea that many blocks of various finite groups are equivalent. It will turn out that equivalent blocks all have exactly the same generalized decomposition matrix. This is the part of the information which is called *p-local*, in the sense that it depends only on p-elements (or more generally p-subgroups). In contrast the modular character values $\phi(s)$ are not local since they depend on $C_G(u)$ and this group is highly dependent upon G. Thus in the above expression of $\chi(us)$ as a sum, there is a p-local part consisting of all generalized decomposition numbers $d_\chi(u,\phi)$ and this part is the same for all equivalent blocks.

In order to give a not too difficult example of this phenomenon, we consider a fixed p-group P and all possible blocks b of finite groups G such that P is central in G and is a defect group of b. In this case the generalized decomposition matrix of b is simply the ordinary character table of P. This only depends on P and so is part of the p-local information. In fact all blocks with a fixed central defect group P are equivalent (and it is easy to see that there are infinitely many such blocks).

Another remarkable example is the case where the p-group P is cyclic. The generalized decomposition matrix of a block with a cyclic defect group was completely described by E.C. Dade, and this is one of the important achievements of the theory. Moreover all indecomposable modules associated with such a block have been classified. It is the only case where there are actually finitely many such indecomposable modules up to isomorphism.

Module theory

A very large part of block theory and decomposition theory is due to the pioneering work of R. Brauer, from the forties to the sixties. The next important stage in the development of modular representation theory is due to J.A. Green, who started in the early sixties the systematic study of indecomposable $\mathcal{O}G$-modules and found many of their important properties. A basic tool is *induction*, which already plays a crucial role in ordinary representation theory. If H is a subgroup of G and if L is an $\mathcal{O}H$-module, then the induced module $\mathrm{Ind}_H^G(L)$ is the $\mathcal{O}G$-module $\mathcal{O}G \otimes_{\mathcal{O}H} L$. Given an indecomposable $\mathcal{O}G$-module M, consider a minimal subgroup P such that M is isomorphic to a direct summand of $\mathrm{Ind}_P^G(L)$ for some indecomposable $\mathcal{O}P$-module L. Then P is a p-subgroup of G, called a *vertex* of M, while the corresponding indecomposable $\mathcal{O}P$-module L is called a *source* of M. The important point here is that such a minimal pair (P, L) is unique up to conjugation. The concept of vertex is the counterpart for modules of the concept of defect group for blocks. Moreover if M is associated with a block b, then a vertex of M is always contained in a defect group of b. We also mention an important tool, called the *Green correspondence*, which is a bijection between the set of all indecomposable $\mathcal{O}G$-modules with vertex P and the set of all indecomposable $\mathcal{O}N_G(P)$-modules with vertex P. This was used for instance in the classification of modules associated with a block with a cyclic defect group.

Green's theory of vertices and sources in some sense reduces the study of $\mathcal{O}G$-modules to the case of a p-group P. This case is quite hard to handle in general because the categories $\mathrm{mod}(\mathcal{O}P)$ and $\mathrm{mod}(kP)$ are almost always *wild*, in a sense which can be defined precisely. (We note in passing that there is a fruitful approach, developed by J.F. Carlson and others in the eighties, which is based on associating an algebraic variety with every kG-module.) However, there are still some very deep questions of finiteness. In particular W. Feit conjectured that, for a given p-group P, there are only finitely many kP-modules which can be the source of some simple kG-module for some finite group G. Here G runs over the infinitely many finite groups having P as a subgroup. There are known infinite families of simple modules which all have the same source and this is part of the evidence for the conjecture.

It was shown in the seventies by M. Auslander and I. Reiten that the category of modules may be endowed with extra structure. With each indecomposable kG-module M is associated another indecomposable kG-module L and a short exact sequence

$$S_M \,:\, 0 \longrightarrow L \longrightarrow E \longrightarrow M \longrightarrow 0$$

called the *almost split sequence* terminating in M. By definition the sequence does not split but every homomorphism $f : X \to M$ can be lifted to a homomorphism $\widetilde{f} : X \to E$, except if f is a split epimorphism (because otherwise this would force the splitting of S_M). The remarkable fact is that S_M is unique up to isomorphism (for any given M). For trivial reasons, we have to assume in this discussion that M is not a projective kG-module. Almost split sequences have turned out to be very useful objects both in module theory and block theory. Other types of diagrams of $\mathcal{O}G$-modules (such as complexes or cycles) have also been considered with significant success.

G-algebras

It was first observed by J.A. Green that a common concept can be used for handling both the block theory and the module theory. He defined a *G-algebra* to be an $\mathcal{O}$-algebra endowed with an action of G by algebra automorphisms. The group algebra $\mathcal{O}G$ and any block algebra $\mathcal{O}Gb$ are G-algebras for the conjugation action of G. On the other hand if M is an $\mathcal{O}G$-module, then $\mathrm{End}_{\mathcal{O}}(M)$ is also a G-algebra for the conjugation action of G. It was later emphasized by L. Puig that it is important to view these examples as instances of *interior G-algebras*, namely algebras A endowed with a group homomorphism $G \to A^*$ (where A^* denotes the group of invertible elements of A). Any interior G-algebra is a G-algebra by conjugation. The importance of the concept of interior G-algebra stems from the fact that an induction procedure is available for interior G-algebras, but not for G-algebras.

Whenever a group acts on a set, it is useful to look at fixed points. For every subgroup H of G, we let A^H be the set of all elements of the G-algebra A which are fixed under H. Then $\mathrm{End}_{\mathcal{O}}(M)^H = \mathrm{End}_{\mathcal{O}H}(M)$, the subalgebra of all endomorphisms of M which commute with the action of H. In particular any projection onto a direct summand of M as an $\mathcal{O}G$-module is an idempotent of $\mathrm{End}_{\mathcal{O}}(M)^G$. In the other example, $(\mathcal{O}G)^G$ is the centre of $\mathcal{O}G$, where all the block idempotents lie. If M is indecomposable, then $\mathrm{End}_{\mathcal{O}}(M)^G$ has no idempotent except 0 and 1. Similarly if $\mathcal{O}Gb$ is a block algebra, then $(\mathcal{O}Gb)^G$ has no non-trivial idempotent. We say in that case that the G-algebra is *primitive*.

A useful way of constructing fixed elements is to sum all the elements of a G-orbit. If H is a subgroup of G and if $a \in A^H$, we write

$$t_H^G(a) = \sum_{g \in [G/H]} g \cdot a$$

where $[G/H]$ denotes a set of representatives of cosets of G modulo H. This defines a linear map $t_H^G : A^H \to A^G$, called the *relative trace map*.

If A is a primitive G-algebra, we can now define a *defect group* of A to be a minimal subgroup P such that t_P^G is surjective. The important property is that a defect group is unique up to conjugation (this is where the primitivity of the G-algebra comes into play). When $A = \mathcal{O}Gb$, this provides the definition of a defect group of the block b. When $A = \mathrm{End}_{\mathcal{O}}(M)$ where M is an indecomposable $\mathcal{O}G$-module, one actually recovers the concept of a vertex of M (the equivalence between the two definitions is known as Higman's criterion).

We have now unified in some way block theory and module theory under the single concept of G-algebra. Apart from the obvious advantage of elegance, this approach has many other benefits. First of all the concept also applies to other objects, such as diagrams of $\mathcal{O}G$-modules and in particular short exact sequences of $\mathcal{O}G$-modules, yielding a new method for handling these objects. For instance, with every almost split sequence is associated a primitive G-algebra (hence a defect group and so forth), which reflects the structure of the sequence. The next feature is that some invariants or constructions which have been used successfully in one theory can be introduced for arbitrary G-algebras and applied to other objects. This procedure sheds some new light on the subject and turns out to yield decisive new results.

Pointed groups

During the eighties, L. Puig extended Green's work on G-algebras and developed a new approach to the modular representation theory. He introduced new invariants, gave a new point of view on classical topics, proved structural results, and proposed difficult open problems. The cornerstone of Puig's approach is the notion of pointed group which we are now going to define.

If M is an $\mathcal{O}G$-module and if H is a subgroup of G, then a direct summand N of M as an $\mathcal{O}H$-module corresponds to an idempotent projection $e \in A^H$, where $A = \mathrm{End}_{\mathcal{O}}(M)$ is the corresponding G-algebra. Moreover N is indecomposable if and only if e is a *primitive* idempotent of A^H (that is, e cannot be decomposed as the sum of two non-zero idempotents annihilating each other). Finally two such direct summands N and N' are isomorphic if and only if the corresponding idempotents e and e' are conjugate in A^H. Thus the important notion is that of conjugacy class of primitive idempotents.

For any $\mathcal{O}$-algebra B, a conjugacy class of primitive idempotents is called a *point* of B. It is not difficult to prove that any point of B is contained in all maximal two-sided ideals of B except one, and this provides a bijection between the set of points of B and the set of maximal two-sided ideals of B. (This explains the terminology, in analogy with commutative algebra, where a geometric point corresponds to a maximal ideal.) If $A = \mathrm{End}_{\mathcal{O}}(M)$ as above, a point of A^H corresponds to an isomorphism class of indecomposable direct summands of M, viewed as an $\mathcal{O}H$-module by restriction. If for instance M is indecomposable with vertex P and source L, then there is a unique point of A^G consisting of the singleton id_M (because M is indecomposable), while the isomorphism class of L corresponds to a point of A^L, called a *source point* of A.

If A is an arbitrary G-algebra and if we consider the points of all subalgebras A^H where H runs over all subgroups of G, we are led to introduce pairs (H, α) where H is a subgroup and α is a point of A^H. Such a pair is called a *pointed group* on the G-algebra A and is always written H_α, both for notational convenience and because pointed groups are usually treated as generalizations of subgroups. For instance there is an easy notion of containment between two pointed groups which generalizes the containment relation between subgroups.

We have seen what a pointed group is in module theory. Similarly it is clear how to define the direct sum of two diagrams of $\mathcal{O}G$-modules (for instance short exact sequences) and the resulting notion of direct summand can be reinterpreted as a pointed group on the G-algebra corresponding to the diagram. We now turn to the question of how useful this notion is in the case of a group algebra.

If U is a p-subgroup of G, there is a surjective algebra homomorphism $br_U : (\mathcal{O}G)^U \to kC_G(U)$ (called the *Brauer homomorphism*) mapping $C_G(U)$ to itself by the identity map and mapping all the other basis elements to zero. (One needs to reduce modulo $\mathfrak{p}$ in order to get a ring homomorphism.) Moreover any simple $kC_G(U)$-module V is specified by a surjective algebra homomorphism $\pi : kC_G(U) \to \mathrm{End}_k(V)$. The composition $\widetilde{\pi} = \pi\, br_U$ is a surjective homomorphism $\widetilde{\pi} : (\mathcal{O}G)^U \to \mathrm{End}_k(V)$ onto a simple algebra, so its kernel is a maximal ideal. By the bijection between points and maximal ideals, this defines a point α of $(\mathcal{O}G)^U$, hence a pointed group U_α on the group algebra $\mathcal{O}G$. So any simple $kC_G(U)$-module, and hence any irreducible modular character of $C_G(U)$, corresponds to a pointed group U_α on $\mathcal{O}G$.

Let χ be an ordinary irreducible character of G. If we apply this observation to the subgroup U generated by a p-element u, we see that the generalized decomposition number $d_\chi(u, \phi)$ actually depends on a point α of $(\mathcal{O}G)^U$ rather than a modular character ϕ. It turns out that the value of $d_\chi(u, \phi)$ is simply equal to $\chi(uj)$ where j is an arbitrary idempotent in the point α. Thus any generalized decomposition number is in fact a character value on a suitable element of the group algebra. Instead of using Brauer's classical approach explained before, we can now *define* generalized decomposition numbers as being the values $\chi(uj)$ and derive from this all the classical results of Brauer. This point of view also provides the way of computing these numbers via source algebras (see below). This is a very good example of how Puig's approach to a classical notion yields more precise results.

Source algebras

If M is an indecomposable $\mathcal{O}G$-module with vertex P and source L, we have seen that the source module L can be viewed as a point γ of A^P, where $A = \mathrm{End}_{\mathcal{O}}(M)$. Similarly, for any primitive G-algebra A, one associates with A a defect group P and a source point γ of A^P, hence a pointed group P_γ, called a *defect pointed group* of A. The main fact still holds: all defect pointed groups are conjugate. Now with any primitive idempotent i in the source point γ, we can construct the algebra iAi, called a *source algebra* of A. This is a P-algebra (because i is fixed under P by construction) and moreover it is primitive (because i is primitive). The choice of i does not change the source algebra up to isomorphism. If A has an interior G-algebra structure, then the source algebra is also an interior P-algebra (and this improvement is actually crucial for blocks).

So we have now constructed a new invariant of a primitive G-algebra, the source algebra, unique up to conjugation. If M is an indecomposable $\mathcal{O}G$-module with vertex P and source L and if $A = \mathrm{End}_{\mathcal{O}}(M)$ is the G-algebra associated with M, then the source algebra iAi is simply the P-algebra associated with the source L (because i is the projection onto L and $i\,\mathrm{End}_{\mathcal{O}}(M)i \cong \mathrm{End}_{\mathcal{O}}(L)$). But this new notion is also defined for other objects, in particular for blocks. It turns out that source algebras of blocks contain all the p-local information about blocks and have many remarkable properties, so that they should be considered as one of the crucial objects to be studied in block theory.

The first main result is that the source algebra S of a block algebra $\mathcal{O}Gb$ is Morita equivalent to $\mathcal{O}Gb$. This means that the module categories $\mathrm{mod}(\mathcal{O}Gb)$ and $\mathrm{mod}(S)$ are equivalent. So we do not lose the kind of information we want by passing to the source algebra. In particular the simple modules for the block are in bijection with the simple modules for the source algebra.

The second main result is that the generalized decomposition numbers of the block b can be computed from the source algebra S. Recall that these numbers have the form $\chi(uj)$ where χ is an ordinary irreducible character, u is a p-element, and j is a primitive idempotent of $(\mathcal{O}G)^u$. One can show that j can be chosen in its conjugacy class so that it belongs to the source algebra and the result essentially follows from this.

Now we can define the notion of equivalence for blocks which we mentioned earlier. Two blocks are equivalent if they have the same defect group and isomorphic source algebras. In particular they necessarily have the same module categories and the same generalized decomposition matrix. So the classification of blocks up to equivalence reduces to the problem of classifying all possible source algebras for a given defect group. This is a hard problem which is far from being solved. Many properties of source algebras of blocks are known, but they do not suffice yet to characterize them.

In analogy with Feit's conjecture about sources of simple kG-modules, L. Puig conjectured that, for a given defect group P, there are only finitely many interior P-algebras which can be the source algebra of some block. Thus there would only be finitely many equivalence classes of blocks with a given defect group. It was proved by Puig that, for a given defect group P, there are only finitely many possible source algebras of any given dimension; thus Puig's conjecture reduces to the statement that the dimension of source algebras is bounded (in terms of P).

A number of results are known about source algebras of blocks. For blocks with a cyclic defect group, Puig's conjecture has been recently proved by Linckelmann, using deep structural theorems which extend the results of Dade already mentioned. The structure of source algebras has also been described when the defect group is a Klein four group, when the block is nilpotent (see below), when the group is p-soluble, and for some blocks of Chevalley groups. Weaker forms of Puig's conjecture have also been proved, for instance for blocks of p-soluble groups only, or symmetric groups only.

Fusion and nilpotent blocks

We have already mentioned that, whenever Q is a p-subgroup of G, the blocks of G partition the set of simple $kC_G(Q)$-modules (or in other words the set of irreducible modular characters of $C_G(Q)$). But there is an even more precise fact: the blocks of G partition the set of blocks of $kC_G(Q)$, so that every block e of $C_G(Q)$ is associated with some block b of G. More precisely e is associated with b if and only if it appears in a decomposition of $br_Q(b)$, where br_Q is the Brauer homomorphism.

Let b be a block of G. A *Brauer pair* associated with b is a pair (Q, e) where Q is a p-subgroup of G and e is a block of $kC_G(Q)$ associated with b. The use of such pairs started with Brauer (in a special case) and was systematically introduced by J.L. Alperin and M. Broué in the late seventies. They defined a partial order relation on the set of Brauer pairs and obtained a poset (partially ordered set). Their idea was to view Brauer pairs as generalizations of p-subgroups and the poset of Brauer pairs as analogous to the poset of p-subgroups. The maximal elements of this poset are all conjugate (their first components are in fact the defect groups of b) and they play the role of the Sylow p-subgroups. This work of Alperin and Broué set the foundations of the p-local theory of blocks.

Refining this notion, one can consider pairs (Q, ϕ) where Q is a p-subgroup of G and ϕ is an irreducible modular character of $kC_G(Q)$ associated with b. This is a refinement since every such ϕ is necessarily associated with some block e of $C_G(Q)$. But we have already mentioned that any such ϕ can be lifted uniquely to a point α of $(\mathcal{O}G)^Q$. Thus these new pairs are just pointed groups on $\mathcal{O}G$ and this is in fact the original reason why L. Puig introduced pointed groups.

If P is a Sylow p-subgroup of G, two p-subgroups Q and Q' of P can be conjugate in G without being conjugate in P. This type of phenomenon is called "fusion" and happens also with both the Brauer pairs and the finer notion of pointed group. Without giving the precise definition of fusion, we simply mention that an element $g \in N_G(Q)$ induces a fusion of Q with itself, but this fusion is considered to be trivial if $g \in C_G(Q)$ because g induces the trivial automorphism of Q. In the so-called p-local group theory (which is at the heart of the classification of finite simple groups), one of the first standard results, due to Frobenius, asserts that a group in which there is no phenomenon of fusion must necessarily be p-nilpotent (that is, a Sylow p-subgroup must have a normal complement). In analogy, a block is called *nilpotent* if there is no phenomenon of fusion in the poset of Brauer pairs, or equivalently in the finer poset of pointed groups. This notion (which of course can be made precise) is due to Broué and Puig, who proved many of the remarkable properties of such blocks. For instance they proved that any nilpotent block has a unique simple module over k, hence a unique irreducible modular character, and they computed the generalized decomposition numbers.

The structure of a source algebra of a nilpotent block was later determined by Puig. This is a remarkable achievement, but in some way it is only the first step of the p-local theory of blocks, since by definition there is no fusion in the case of nilpotent blocks. More complicated structures should appear if non-trivial fusion occurs.

Puig's theorem asserts that a source algebra of a nilpotent block b with defect group P is isomorphic to $S \otimes_{\mathcal{O}} \mathcal{O}P$, where $S = \mathrm{End}_{\mathcal{O}}(M)$ is the endomorphism algebra of an *endo-permutation* $\mathcal{O}P$-module M. This means by definition that S has a P-invariant basis. As a result $\mathcal{O}Gb$ is Morita equivalent to $S \otimes_{\mathcal{O}} \mathcal{O}P$, hence to $\mathcal{O}P$ since S is a matrix algebra (a matrix algebra plays no role for an equivalence of module categories). However, S plays a role for the computation of the generalized decomposition matrix. If $S = \mathcal{O}$, that is, if a source algebra is simply $\mathcal{O}P$ (as in the case of blocks with a central defect group), then the generalized decomposition matrix is the character table of P. In the general case, each generalized decomposition number has to be modified by a sign which comes from the action of P on M (that is, from the interior P-algebra structure of S).

We note that the condition that S is an endo-permutation module is a very strong one. Those modules were first introduced by E.C. Dade in the seventies and play a prominent role in modular representation theory. There are several open questions about them, including the tantalizing problem of their classification.

Multiplicity modules

Another important concept of Puig's theory is that of defect multiplicity module. Let A be a primitive G-algebra with defect group P and source point γ (or in short with defect pointed group P_γ). We know that the point γ corresponds to a maximal ideal $\mathfrak{m}$ of A^P , hence to a simple algebra $A^P/\mathfrak{m}$, which we can write $A^P/\mathfrak{m} \cong \mathrm{End}_k(V(\gamma))$ for some k-vector space $V(\gamma)$ (because k is algebraically closed). The stabilizer $N_G(P_\gamma)$ of P_γ acts on this simple algebra and P acts trivially by construction, so that $\mathrm{End}_k(V(\gamma))$ is an $\overline{N}$-algebra, where $\overline{N} = N_G(P_\gamma)/P$. Using the Skolem–Noether theorem, it is elementary to deduce that $V(\gamma)$ is canonically endowed with a structure of module over a twisted group algebra of the group $\overline{N}$ (in other words $V(\gamma)$ is a "projective" representation in Schur's sense). The crucial fact is that this module is indecomposable projective. It is called the *defect multiplicity module* of A and is an interesting invariant of A . If A is a block algebra, this notion specializes to Brauer's notion of root, but it is also defined for other objects, in particular for $\mathcal{O}G$-modules.

We have now three invariants of a primitive G-algebra: the defect group, the source algebra, and the defect multiplicity module, defined up to conjugacy. For an *interior* G-algebra A (still primitive), a remarkable fact is that these three invariants essentially characterize A up to isomorphism. We have added the word "essentially" because the third invariant has to be handled with some care. In fact we obtain a *parametrization* of primitive interior G-algebras with three invariants. In particular indecomposable $\mathcal{O}G$-modules can be parametrized by the conjugacy classes of their three invariants: vertex, source, and defect multiplicity module. Similarly blocks are parametrized by their defect group, their source algebra, and their root. The problem here is that we do not know yet what sort of interior algebras occur as source algebras of blocks, although there are numerous restrictions. This is precisely the problem which was mentioned earlier.

An important tool of the theory of G-algebras is the *Puig correspondence*, which can be viewed as a generalization of the Green correspondence. If A is a G-algebra which is not necessarily primitive, then each point of A^G still has a defect pointed group. If we fix such a defect pointed group P_γ , we can still consider the corresponding simple algebra $\mathrm{End}_k(V(\gamma))$ and $V(\gamma)$ is still a module over a twisted group algebra of the group $\overline{N}$. However, this module need not be indecomposable projective. The Puig correspondence is a bijection between the set of all points of A^G with defect pointed group P_γ and the set of all isomorphism classes of indecomposable direct summands of $V(\gamma)$ which are projective. This correspondence can be considered as a reduction to the case of indecomposable projective modules over a (twisted) group algebra and in this sense it is more powerful than the Green correspondence. In fact the Green correspondence can easily be deduced from the Puig correspondence. In the special case where A is primitive, the Puig correspondence reduces to a bijection between the unique point $\{1\}$ of A^G and the defect multiplicity module of A, as mentioned above.

We note that the Puig correspondence is the crucial tool used for the parametrization of primitive interior G-algebras (and in particular indecomposable $\mathcal{O}G$-modules). We also note that the use of defect multiplicity modules provides a fruitful new point of view on various subjects, including trivial source modules, endo-permutation modules, almost split sequences, Knörr's theorem on vertices of irreducible modules, and Robinson's theorem about the number of blocks with a given defect group.

CHAPTER 1

Algebras over a complete local ring

In this chapter, we develop the general theory of algebras and points which is used in this text. We work over a commutative complete local noetherian ring $\mathcal{O}$ with an algebraically closed residue field k of prime characteristic p. This allows us to deal with primitive idempotents, which play a prominent role in this book. These assumptions suffice for the essential part of the representation theory of finite groups.

We prove a strong version of the theorem on lifting idempotents and use it to deduce a number of basic properties of $\mathcal{O}$-algebras and modules. We also study semi-simple subalgebras of $\mathcal{O}$-algebras and we introduce symmetric algebras. Finally we discuss the notion of Morita equivalence between $\mathcal{O}$-algebras.

In non-commutative algebra, many properties and results involve conjugation, in particular some uniqueness statements, and it turns out that it is often much more convenient to work with the conjugacy classes of objects rather than the objects themselves. For this reason, we define several concepts as conjugacy classes: a point is a conjugacy class of primitive idempotents and an exomorphism is a conjugacy class of homomorphisms. These notions play a prominent role throughout this book.

§ 1 PRELIMINARIES

In this section, we list without proof some basic results which are proved in many textbooks. For instance most proofs can be found in Curtis–Reiner [1981], Feit [1982], Landrock [1983]. Most results are concerned with semi-simple rings, the Jacobson radical, and basic facts about groups and modules. We end the section with a survey of some elementary properties of group cohomology needed in this text.

Unless otherwise stated, all rings have a unity element, all modules are finitely generated left modules and all homomorphisms act on the left. The unity element of a ring A is written 1_A, or sometimes simply 1. All algebras are associative algebras with a unity element. We assume the reader is familiar with some basic notions of ring theory, in particular the concepts of noetherian ring, local ring, and principal ideal domain.

We shall be mainly concerned with non-commutative rings. If a and u are two elements of a ring A and if u is invertible, we write $a^u = u^{-1}au$ and ${}^u a = uau^{-1}$. We shall use more often the latter notation because we usually choose to work with *left* actions. Two elements a and b are called *conjugate* if there exists an invertible element $u \in A^*$ such that $b = {}^u a$. Here A^* denotes the group of invertible elements of A. It is clear that conjugation is an equivalence relation and an equivalence class is called a *conjugacy class*.

By an ideal in a ring A, we shall always mean a two-sided ideal of A (unless otherwise stated). We denote by $\mathrm{Max}(A)$ the set of all maximal ideals of A. If A is a finite dimensional algebra over a field, then $\mathrm{Max}(A)$ is a finite set. We denote by $\mathrm{Irr}(A)$ the set of isomorphism classes of simple A-modules (also called irreducible A-modules). We often abusively identify a simple A-module with its isomorphism class. The *Jacobson radical* $J(A)$ of a ring A is the intersection of all maximal left ideals of A. It is a two-sided ideal and is in fact also the intersection of all maximal right ideals of A. Any maximal ideal of A contains $J(A)$, so that $J(A) \subseteq \bigcap_{\mathfrak{m} \in \mathrm{Max}(A)} \mathfrak{m}$. An important property of the Jacobson radical is Nakayama's lemma.

(1.1) PROPOSITION (Nakayama's lemma). *Let A be a ring and let V be a finitely generated A-module. If $J(A) \cdot V = V$, then $V = 0$.*

One often needs to apply Nakayama's lemma to a module of the form V/W where W is a submodule of V. In that case the result can be restated as follows: if $W + J(A)V = V$, then $W = V$.

(1.2) PROPOSITION. *If* A *is a commutative noetherian ring, then* $\bigcap_{n\geq 0} J(A)^n = 0$.

Note that the proof consists essentially in applying Nakayama's lemma to the ideal $\bigcap_{n\geq 0} J(A)^n$.

Recall that if $\mathcal{O}$ is a commutative ring and if M is an $\mathcal{O}$-module, then M is called *free* if M has a basis. In that case the number of elements of a basis is independent of the choice of basis (because $\mathcal{O}$ is commutative); it is called the *dimension* of M and is written $\dim_{\mathcal{O}}(M)$. Thus M is isomorphic to a direct sum of $\dim_{\mathcal{O}}(M)$ copies of $\mathcal{O}$.

If A is a not necessarily commutative ring, then a free A-module of rank r is an A-module isomorphic to a direct sum of r copies of A . We use here the word *rank* rather than dimension, because we shall apply this to the case of an $\mathcal{O}$-algebra A which is free as an $\mathcal{O}$-module. Thus a free A-module has both a rank (over A) and a dimension (over $\mathcal{O}$). If $\dim_{\mathcal{O}}(A) = n$, then a free A-module of rank r has dimension rn over $\mathcal{O}$.

Another easy consequence of Nakayama's lemma is the following result (see Exercise 1.3).

(1.3) PROPOSITION. *Let* $\mathcal{O}$ *be a local commutative ring with unique maximal ideal* $\mathfrak{p}$ *and residue field* $k = \mathcal{O}/\mathfrak{p}$. *Let* M *and* N *be two finitely generated free* $\mathcal{O}$*-modules, and let* $\overline{M} = M/\mathfrak{p}M$ *and* $\overline{N} = N/\mathfrak{p}N$.

(a) *Let* $f : M \to N$ *be an* $\mathcal{O}$*-linear map and let* $\overline{f} : \overline{M} \to \overline{N}$ *be its reduction modulo* $\mathfrak{p}$. *If* $\overline{f}$ *is surjective, then* f *is surjective. If* $\overline{f}$ *is an isomorphism, then* f *is an isomorphism.*

(b) *Let* $x_1, \ldots, x_n \in M$. *If their images* $\overline{x}_1, \ldots, \overline{x}_n$ *in* $\overline{M}$ *form a* k*-basis of* $\overline{M}$, *then* $\{x_1, \ldots, x_n\}$ *is an* $\mathcal{O}$*-basis of* M .

(1.4) COROLLARY. *Let* $\mathcal{O}$ *be a local commutative ring. Then any direct summand of a finitely generated free* $\mathcal{O}$*-module is free.*

Another way of obtaining free modules is the following. Recall that an $\mathcal{O}$-module M is called *torsion-free* if, whenever $\lambda \cdot m = 0$ for some $\lambda \in \mathcal{O}$ and some non-zero $m \in M$, then $\lambda = 0$.

(1.5) PROPOSITION. *Let* $\mathcal{O}$ *be a principal ideal domain. Any finitely generated torsion-free* $\mathcal{O}$*-module is free. In particular any submodule of a finitely generated free* $\mathcal{O}$*-module is free.*

A ring A is called *simple* if A has precisely two ideals, namely 0 and A . Thus A is non-zero and 0 is the unique maximal ideal of A . We shall only deal with simple rings which are finite dimensional algebras over a field k . Their structure is described by the following result. Denote by $M_n(D)$ the ring of $n \times n$-matrices with coefficients in the ring D .

(1.6) THEOREM (Wedderburn). *Let k be a field and let A be a finite dimensional k-algebra. The following conditions are equivalent.*
(a) A is a simple ring.
(b) $A \cong M_n(D)$ for some integer n and some finite dimensional division k-algebra D.
(c) $A \cong \mathrm{End}_D(V)$ for some finite dimensional division k-algebra D and some finite dimensional D-vector space V.
If these conditions are satisfied, then V is a simple A-module and is the unique simple A-module (up to isomorphism); thus $\mathrm{Irr}(A)$ contains a single element. Moreover $D \cong \mathrm{End}_A(V)^{\mathrm{op}}$, so that the k-algebra D is uniquely determined up to isomorphism.

If the endomorphism algebra $\mathrm{End}_A(V) \cong D^{\mathrm{op}}$ of the unique simple A-module V is isomorphic to k, then the simple k-algebra A is called *split*. In that case $A \cong \mathrm{End}_k(V) \cong M_n(k)$.

Since we shall usually be concerned with algebraically closed fields, we mention the following special case.

(1.7) PROPOSITION. *Let k be an algebraically closed field.*
(a) Any finite dimensional division algebra D over k is isomorphic to k.
(b) Any finite dimensional simple k-algebra is split, hence isomorphic to $\mathrm{End}_k(V) \cong M_n(k)$, where V is a k-vector space of dimension n.

The previous results contain implicitly Schur's lemma, which we now state in full.

(1.8) LEMMA (Schur). *Let k be a field, let A be a finite dimensional k-algebra, and let V and W be two simple A-modules.*
(a) $\mathrm{Hom}_A(V, W) = 0$ if V and W are not isomorphic.
(b) $\mathrm{End}_A(V)$ is a division algebra. In particular $\mathrm{End}_A(V) \cong k$ if k is algebraically closed.

Another important result about simple rings is the Skolem–Noether theorem.

(1.9) THEOREM (Skolem–Noether). *Let S be a simple finite dimensional algebra over a field k and assume that the centre of S is k. Then every k-algebra automorphism of S is an inner automorphism.*

A finite dimensional k-algebra is called *semi-simple* if it is isomorphic to a finite direct product of simple k-algebras. It is moreover called *split* if every simple factor is split. A module is called *semi-simple* if it is isomorphic to a direct sum of simple modules. Note that this direct sum must be finite since all of our modules are finitely generated.

(1.10) THEOREM. *Let* k *be a field and let* A *be a finite dimensional* k*-algebra. The following conditions are equivalent.*

(a) A *is a semi-simple algebra.*

(b) A *is a semi-simple left* A*-module.*

(c) Every left A*-module is semi-simple.*

(d) $J(A) = 0$.

If these conditions are satisfied, then $A \cong \prod_{\mathfrak{m} \in \mathrm{Max}(A)} A/\mathfrak{m}$. *Moreover the annihilator of a simple* A*-module is a maximal ideal and this sets up a bijection between* $\mathrm{Irr}(A)$ *and* $\mathrm{Max}(A)$.

Let A be a finite dimensional k-algebra. A simple A-module V is called *absolutely simple* if $k' \otimes_k M$ is a simple $k' \otimes_k A$-module for every field extension k' of k .

(1.11) PROPOSITION. *Let* k *be a field, let* A *be a finite dimensional* k*-algebra, and let* V *be a simple* A*-module. Then* V *is absolutely simple if and only if* $\mathrm{End}_A(V) \cong k$.

In particular, a semi-simple k-algebra A is split if and only if every simple A-module is absolutely simple. In that case A is isomorphic to a direct product of matrix algebras over k . We shall only occasionally need the following result and for simplicity we assume that k has characteristic zero in order to avoid questions of separability.

(1.12) PROPOSITION. *Let* k *be a field of characteristic zero and let* A *be a semi-simple* k*-algebra. There exists a finite extension* k' *of* k *such that* $k' \otimes_k A$ *is split.*

As we shall deal with rings which have many properties in common with finite dimensional k-algebras, the next result is particularly important for our purposes.

(1.13) THEOREM. *Let* k *be a field and let* A *be a finite dimensional* k*-algebra. Then the following properties hold.*

(a) $J(A)$ *is nilpotent and every nilpotent ideal of* A *is contained in* $J(A)$.

(b) $\mathrm{Max}(A)$ *is finite.*

(c) $J(A) = \bigcap_{\mathfrak{m} \in \mathrm{Max}(A)} \mathfrak{m}$.

(d) $A/J(A)$ *is semi-simple.*

(e) $A/J(A) \cong \prod_{\mathfrak{m} \in \mathrm{Max}(A)} A/\mathfrak{m}$.

(f) $\mathrm{Irr}(A) = \mathrm{Irr}(A/J(A))$ *is in bijection with* $\mathrm{Max}(A)$.

(g) A *is noetherian.*

Now we recall some facts about idempotents. An *idempotent* of a ring A is an element $e \in A$ such that $e^2 = e$. There are always two idempotents in A, namely 0 and 1, called *trivial* idempotents. If e is an idempotent, then so is $1 - e$. Two idempotents e and f are called *orthogonal* if $ef = 0$ and $fe = 0$. In particular any idempotent e is orthogonal to $1 - e$. An idempotent e is called *primitive* if $e \neq 0$ and whenever $e = f + g$ where f and g are orthogonal idempotents, then either $f = 0$ or $g = 0$.

A *decomposition* of an idempotent e is a finite set I of pairwise orthogonal idempotents such that $e = \sum_{i \in I} i$. The decomposition is called *primitive* if every idempotent $i \in I$ is primitive. Note that $i = ei = ie$, so in particular e commutes with each i. The latter two equalities are equivalent to the single equality $i = eie$ (as one checks by multiplying by e on the left and on the right). Conversely if f is an idempotent which satisfies $f = efe$, then f appears in some decomposition of e, because $e = f + (e - f)$ is an orthogonal decomposition. These elementary observations will be used repeatedly. Instead of referring to a decomposition of an idempotent e as being a set I, we shall often say abusively that the expression $e = \sum_{i \in I} i$ is a decomposition of e.

Recall that two idempotents e and f are called *conjugate* if there exists $u \in A^*$ such that $f = {}^{u}e$. Most of the concepts and constructions which we are going to introduce for idempotents will depend on conjugacy classes of idempotents rather than idempotents themselves. We define a *point* of A to be a conjugacy class of primitive idempotents of A. The set of points of A will be written $\mathcal{P}(A)$. The relevance of this notion will become clear in Section 4, where we will have strong assumptions on A. For the moment, we only mention what are the points of a semi-simple algebra, starting with the case of a simple algebra.

(1.14) PROPOSITION. *Let $S = \mathrm{End}_D(V)$ be a simple k-algebra, where k is a field, D is a division algebra, and V is a finite dimensional D-vector space.*

(a) S has a single point, that is, all primitive idempotents of S are conjugate.

(b) An idempotent e of S is primitive if and only if e is a projection onto a one-dimensional D-subspace of V.

(c) Two idempotents of S are conjugate if and only if they have the same rank as D-linear maps (that is, the dimensions over D of their images are equal).

(d) Any two primitive decompositions of 1_S are conjugate under S^*.

(1.15) PROPOSITION. *Let* k *be a field and let* $A = S_1 \times \ldots \times S_n$ *be a semi-simple* k*-algebra, where each* S_i *is a simple* k*-algebra.*

(a) *Every primitive idempotent of* A *has the form* $(0, \ldots, 0, e, 0, \ldots, 0)$ *where* e *is a primitive idempotent of* S_i .

(b) *Every maximal ideal of* A *has the form* $S_1 \times \ldots \times S_{i-1} \times S_{i+1} \times \ldots \times S_n$, *where* $1 \leq i \leq n$.

(c) *For every point* α *of* A , *there is a unique maximal ideal* $\mathfrak{m}$ *of* A *such that* $e \notin \mathfrak{m}$ *for some* $e \in \alpha$. *In fact* $e \notin \mathfrak{m}$ *for every* $e \in \alpha$.

(d) *The correspondence in (c) sets up a bijection between the sets* $\mathcal{P}(A)$ *and* $\mathrm{Max}(A)$.

(e) *For every point* α *of* A , *there is a unique simple* A*-module* V *(up to isomorphism) such that* $e \cdot V \neq 0$ *for some* $e \in \alpha$. *In fact* $e \cdot V \neq 0$ *for every* $e \in \alpha$ *and* $V \cong Ae$.

(f) *The correspondence in (e) sets up a bijection between the sets* $\mathcal{P}(A)$ *and* $\mathrm{Irr}(A)$.

(g) *Any two primitive decompositions of* 1_A *are conjugate under* A^* .

The theorem on lifting idempotents allows us to generalize (c)–(g) to any finite dimensional k-algebra, but we shall consider in Section 3 an even more general situation. The following result is another useful fact about decompositions of idempotents.

(1.16) PROPOSITION. *Let* A *be a ring.*

(a) *Let* $1_A = \sum_{i \in I} i$ *be a decomposition of the unity element. Then* A *decomposes as the direct sum of left ideals* $A = \oplus_{i \in I} Ai$.

(b) *Let* $A = \oplus_{\lambda \in \Lambda} V_\lambda$ *be a finite direct sum decomposition of* A *into left ideals. Then there exists a decomposition of the unity element* $1_A = \sum_{\lambda \in \Lambda} i_\lambda$ *such that* $V_\lambda = Ai_\lambda$.

(c) *An idempotent* e *of* A *is primitive if and only if the left ideal* Ae *is indecomposable.*

(d) *If* A *is noetherian, there exists a primitive decomposition of the unity element* 1_A .

There is an important localization procedure which we now describe. If e is an idempotent in A, then eAe is a subalgebra of A with unity element $1_{eAe} = e$. Note that an element $a \in A$ belongs to eAe if and only if $ea = a = ae$ (or in other words $a = eae$). Any decomposition (respectively primitive decomposition) of e in A is a decomposition (respectively primitive decomposition) of the unity element e of eAe in eAe (because if $e = f_1 + f_2$ with f_1, f_2 orthogonal, then $ef_1 = f_1$ and $f_1 e = f_1$). In particular e is primitive in A if and only if the only idempotents of eAe are the trivial ones, namely 0 and e. Thus the effect of passing from A

to eAe is that one "forgets" about all of the idempotents which are orthogonal to e, and one only keeps idempotents appearing in a decomposition of e. This explains why the procedure is called a "localization" (see exercise 1.1 for a mathematical reason). For example if $S = \mathrm{End}_D(V)$ is a simple k-algebra and if e is a primitive idempotent of S, then $eSe \cong D$ (because e is a projection onto a one-dimensional subspace).

(1.17) PROPOSITION. *Let A be a ring and let e be an idempotent of A.*
(a) $J(eAe) = eJ(A)e$.
(b) If A is a finite dimensional k-algebra over a field k, then e is primitive if and only if eAe is a local ring. In that case $eJ(A)e$ is the unique maximal ideal of eAe.

In the second part of this first section, we recall some standard notions of group theory and module theory and we also fix some notation. Let H be a subgroup of a group G. If $g \in G$, we use the following notation for the conjugate subgroup:

$$ {}^gH = gHg^{-1} \qquad \text{and} \qquad H^g = g^{-1}Hg\,. $$

As we usually choose to work with *left* actions, we shall in general use the first notation. Similarly ${}^gh = ghg^{-1}$ for every $h \in G$. The *normalizer* of H is the subgroup

$$ N_G(H) = \{\, g \in G \mid {}^gH = H \,\}, $$

while the *centralizer* of H is the subgroup

$$ C_G(H) = \{\, g \in G \mid {}^gh = h \text{ for all } h \in H \,\}. $$

If G acts on the left on some set X, we write $G\backslash X$ for the set of orbits and $[G\backslash X]$ for a set of representatives in X of the set of orbits. In the case of right actions, we use the notation X/G and $[X/G]$.

The subgroup H acts on G by left multiplication and the orbit Hg of g is called a *left coset* of H. Some authors call this a right coset but we prefer to be consistent with the notion of left orbit. Similarly gH is a *right coset*. If K is another subgroup of G, the group $H \times K$ acts (on the left) on G via left and right multiplication: explicitly the action of (h,k) on g is equal to hgk^{-1}. An orbit HgK for this action is called a *double coset*. As a special case of the above notation we have the set $H\backslash G$ of left cosets, the set G/H of right cosets, and we also write $H\backslash G/K$ for the set of double cosets. We shall often consider sums indexed by representatives $g \in [G/H]$ or $g \in [H\backslash G/K]$, and it will always be the case that the value of the sum does not depend on the choice of representatives. A set of representatives $[G/H]$ is also called a *transversal* of H in G.

Let X and Y be two sets and let $f : X \to Y$ be a map. If there exists a map $s : Y \to X$ such that $fs = id_Y$, then s is called a *section* of f (and then f is necessarily surjective). If there exists a map $r : Y \to X$ such that $rf = id_X$, then r is called a *retraction* of f (and then f is necessarily injective). If X and Y are groups and if f is a group homomorphism, then a *section* of f is a group homomorphism $s : Y \to X$ such that $fs = id_Y$ (and similarly for retractions). If X and Y are modules and if f is a module homomorphism, then a *section* of f is a module homomorphism $s : Y \to X$ such that $fs = id_Y$ (and similarly for retractions). Similar definitions apply for other algebraic structures. It will always be clear in the context if a section or a retraction refers to a set-theoretic map, a group-theoretic map, or a module-theoretic map.

We assume the reader is familiar with the notion of exact sequence of groups or modules. The trivial group will be written simply 1 (because groups are written multiplicatively), while the trivial module is written 0. A short exact sequence of modules

$$0 \longrightarrow L \xrightarrow{j} M \xrightarrow{q} N \longrightarrow 0$$

is said to be *split* if q has a section, or equivalently if j has a retraction. In that case M is isomorphic to the direct sum $L \oplus N$. A short exact sequence of groups

$$1 \longrightarrow A \xrightarrow{j} E \xrightarrow{q} G \longrightarrow 1$$

is called a *group extension* with kernel group A and factor group G, or also an extension of G by A. Such an extension is called *central* if the image of A in E is a central subgroup of E. The group extension is said to be *split* if q has a section s. In that case one can use the injection s to identify G with a subgroup of E and it follows that E is isomorphic to the semi-direct product $A \rtimes G$ with respect to the conjugation action of G on A. Note that one obtains a stronger condition if one requires the existence of a retraction r of j. Indeed in that case the kernel of r is a *normal* subgroup of E isomorphic to G and it follows that E is isomorphic to the *direct* product $A \times G$.

We now define the notion of pull-back. Let $f : X \to Z$ and $g : Y \to Z$ be two maps with the same codomain. A *pull-back* of the pair of maps (f, g) is a triple $(P, \widetilde{f}, \widetilde{g})$, where P is a set and $\widetilde{f} : P \to Y$, $\widetilde{g} : P \to X$ are maps satisfying $g\widetilde{f} = f\widetilde{g}$, such that the following universal property holds: for every triple $(P', \widetilde{f}', \widetilde{g}')$ where P' is a set and $\widetilde{f}' : P' \to Y$, $\widetilde{g}' : P' \to X$ are maps satisfying $g\widetilde{f}' = f\widetilde{g}'$, there exists a unique map $h : P' \to P$ such that $\widetilde{f}h = \widetilde{f}'$ and $\widetilde{g}h = \widetilde{g}'$. We shall sometimes abusively call P a pull-back of (f, g), without mentioning the maps $\widetilde{f}$ and $\widetilde{g}$.

As always with a universal property, we have uniqueness in a strong sense. If $(P_1, \widetilde{f}_1, \widetilde{g}_1)$ and $(P_2, \widetilde{f}_2, \widetilde{g}_2)$ are pull-backs of (f, g), there exists a unique isomorphism $h : P_1 \to P_2$ such that $\widetilde{f}_2 h = \widetilde{f}_1$ and $\widetilde{g}_2 h = \widetilde{g}_1$. For this reason we shall refer to *the* pull-back of (f, g) as being any one of them. In practice, one can choose the following construction of pull-backs, which shows at the same time that they always exist. We define

$$P = \{ (x, y) \in X \times Y \mid f(x) = g(y) \}$$

and we let $\widetilde{g} : P \to X$ and $\widetilde{f} : P \to Y$ be the first and second projections respectively. Then clearly $g \widetilde{f} = f \widetilde{g}$ and it is straightforward to check that the universal property holds.

Pull-backs for groups or modules are defined in exactly the same way. In the whole discussion above, it suffices to replace sets by groups (respectively modules) and maps by group homomorphisms (respectively module homomorphisms). In particular the explicit construction using the direct product of X and Y works in the same way.

If $(P, \widetilde{f}, \widetilde{g})$ is the pull-back of (f, g) and if f is surjective, then it is easy to see that $\widetilde{f}$ is surjective. Moreover if we are dealing with modules (or groups), then one can check that $\mathrm{Ker}(f) \cong \mathrm{Ker}(\widetilde{f})$, so that we have a commutative diagram of short exact sequences

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Ker}(\widetilde{f}) & \longrightarrow & P & \xrightarrow{\widetilde{f}} & Y & \longrightarrow & 0 \\
 & & \downarrow{\cong} & & \downarrow{\widetilde{g}} & & \downarrow{g} & & \\
0 & \longrightarrow & \mathrm{Ker}(f) & \longrightarrow & X & \xrightarrow{f} & Z & \longrightarrow & 0\,.
\end{array}$$

This creates some sort of dissymmetry in the construction of pull-backs. We shall often encounter this situation and for convenience we shall say that $\widetilde{f} : P \to Y$ is the *pull-back* of $f : X \to Z$ *along* $g : Y \to Z$.

When dealing with group extensions, we shall occasionally need some standard results about group cohomology. In fact we shall only use the first two cohomology groups $H^1(G, A)$ and $H^2(G, A)$, where G is a finite group and A is a G-module (that is, an abelian group endowed with a $\mathbb{Z}$-linear action of G). The required properties of group cohomology can be found in many textbooks (for instance Huppert [1967] or Brown [1982]). The main facts that we need are gathered in the following proposition.

(1.18) PROPOSITION. *Let G be a group and let A be a G-module.*

(a) *If G is finite, its order $|G|$ annihilates the abelian group $H^n(G,A)$ for all $n \geq 1$. In particular $H^n(G,A) = 0$ if A is finite of order prime to $|G|$.*

(b) *There is a bijection between $H^2(G,A)$ and the equivalence classes of group extensions with factor group G and kernel A (with its G-module structure coming from the conjugation action of the factor group G), such that the class of the split extension (semi-direct product) corresponds to the zero element of $H^2(G,A)$.*

(c) *For a given split extension E with kernel A and factor group G, there is a bijection between $H^1(G,A)$ and the conjugacy classes of complements of A in E (or equivalently the A-conjugacy classes of sections $G \to E$ of the surjection $E \to G$).*

(d) *If $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ is an exact sequence of G-modules, then there exists an exact sequence of abelian groups*

$$0 \longrightarrow A^G \xrightarrow{f_*} B^G \xrightarrow{g_*} C^G \xrightarrow{\delta} H^1(G,A) \xrightarrow{f_*} H^1(G,B) \xrightarrow{g_*} H^1(G,C)$$
$$\xrightarrow{\delta} H^2(G,A) \xrightarrow{f_*} H^2(G,B) \xrightarrow{g_*} H^2(G,C) \xrightarrow{\delta} \dots$$

where f_* and g_* are induced by f and g respectively, and δ denotes the connecting homomorphism.

In fact we shall mainly use Proposition 1.18 when A is a trivial G-module, in which case the extensions with kernel A and factor group G are precisely the central extensions, and a split extension is isomorphic to the direct product $A \times G$. For a split extension $E = A \times G$, the group $H^1(G,A)$ is in bijection with the actual set of sections $G \to E$, because the action of the central subgroup A is trivial.

Exercises

(1.1) Let e be a primitive idempotent of a finite dimensional k-algebra A. Prove that if A is commutative, then $A \cong Ae \times A(1-e)$ and Ae is the localization of A with respect to the maximal ideal $J(A)e \times A(1-e)$.

(1.2) Prove the following more precise version of the Skolem–Noether theorem. If T_1 and T_2 are two simple subalgebras of the simple k-algebra $S = \mathrm{End}_k(V)$ and if $f : T_1 \to T_2$ is an isomorphism of k-algebras, then f extends to an inner automorphism of S. [Hint: The vector space V has two T_1-module structures, the first via $T_1 \hookrightarrow S$ and the second via

$T_1 \xrightarrow{f} T_2 \hookrightarrow S$. Since T_1 is simple, any two T_1-modules of the same dimension are isomorphic. The isomorphism in this case is an element $g \in S$ and the inner automorphism defined by g is the required extension. Note that a slight modification of the proof yields the same result for an arbitrary simple k-algebra $S = \mathrm{End}_D(V)$ with centre k .]

(1.3) Prove Proposition 1.3. [Hint: For the proof of part (a), first apply Nakayama's lemma to $\mathrm{Coker}(f)$ to reduce to the case where f is surjective. Then f splits because N is free, and one can apply Nakayama's lemma to $\mathrm{Ker}(f)$. For the proof of part (b), let F be a free $\mathcal{O}$-module with basis $y_1, \ldots, y_n$ and apply (a) to the homomorphism $f : F \to M$ mapping y_i to x_i .]

(1.4) Let A and B be two rings and let n and m be two positive integers. Prove that $M_n(A \times B) \cong M_n(A) \times M_n(B)$ and $M_n(M_m(A)) \cong M_{nm}(A)$.

§ 2 ASSUMPTIONS AND BASIC PROPERTIES OF ALGEBRAS

In this section, we set the scene which is used throughout this book. We introduce algebras over complete local rings and discuss the main results concerning the Jacobson radical of such algebras.

We first describe the ring which will be used as a base ring throughout this book. Let $\mathcal{O}$ be a commutative local noetherian ring with unique maximal ideal $\mathfrak{p} = J(\mathcal{O})$ and residue field $k = \mathcal{O}/\mathfrak{p}$ of prime characteristic p . We assume that $\mathcal{O}$ is *complete* with respect to the $\mathfrak{p}$-adic topology. Recall that the ideals $\mathfrak{p}^n$ form a system of fundamental (closed) neighbourhoods of 0 and that $\bigcap_{n \geq 0} \mathfrak{p}^n = \{0\}$ by Proposition 1.2 (because $\mathcal{O}$ is noetherian). The completeness assumption means that $\mathcal{O}$ is isomorphic to the inverse limit of rings $\varprojlim \mathcal{O}/\mathfrak{p}^n$. In other words, if $(a_k)_{k \geq 0}$ is a sequence of elements of $\mathcal{O}$ such that for every $n \geq 0$ there exists N with $a_k - a_{k+1} \in \mathfrak{p}^n$ for $k \geq N$ (that is, a Cauchy sequence in $\mathcal{O}$), then there exists $a \in \mathcal{O}$ such that for every $n \geq 0$ there exists N with $a - a_k \in \mathfrak{p}^n$ for $k \geq N$ (that is, a_k converges to a).

The next assumption which will be in force is that the residue field k is algebraically closed. In many cases this assumption is irrelevant, but when we come to the heart of representation theory, it becomes an important simplification which still conveys the essential part of the theory.

(2.1) ASSUMPTION. As a base ring, we take a commutative local noetherian ring $\mathcal{O}$ with maximal ideal $\mathfrak{p}$, complete with respect to the $\mathfrak{p}$-adic topology, and such that the field $k = \mathcal{O}/\mathfrak{p}$ is algebraically closed of characteristic p.

(2.2) EXAMPLES. (a) We do not exclude the possibility $\mathfrak{p} = 0$, in which case $\mathcal{O} = k$ is simply an algebraically closed field of characteristic p.

(b) The second case of interest occurs when $\mathcal{O}$ is a complete *discrete valuation ring* of characteristic zero. Recall (Serre [1962]) that this means that $\mathcal{O}$ is a local principal ideal domain. Thus the unique maximal ideal $\mathfrak{p}$ is principal, generated by some element π. It is proved in Serre's book that such a ring exists for any given perfect residue field k of characteristic p, thus in particular when k is algebraically closed. Moreover $\mathcal{O}$ is unique up to isomorphism if we assume further that it is *absolutely unramified*; this means by definition that the prime number p is a generator of $\mathfrak{p}$. The other possibilities for $\mathcal{O}$ are then obtained by means of *totally ramified* extensions (that is, extensions with a trivial residue field extension). This example is particularly important for the representation theory of finite groups because such a ring establishes the link between a field of characteristic zero (the field of fractions of $\mathcal{O}$) and the field k of characteristic p, by reduction modulo $\mathfrak{p}$. Note however that one does not need a principal ideal domain to pass from characteristic zero to characteristic p. Indeed the largest part of modular representation theory works as well with a complete local domain of characteristic zero with a higher Krull dimension. If G is a finite group of order n, one usually needs n-th roots of unity for the representation theory of G. By Hensel's lemma (see Section 4), all roots of unity of order prime to p lie in $\mathcal{O}$ because they lie in k. If one needs p^r-th roots of unity, then one can always enlarge $\mathcal{O}$ by considering an appropriate finite extension (necessarily totally ramified).

(c) Any factor ring of $\mathcal{O}$ satisfies again the assumption 2.1, and so can be used as a base ring. For instance it is sometimes useful to work with $\mathcal{O}/\mathfrak{p}^n$.

Since $\mathcal{O}$ is a local ring, any element outside $\mathfrak{p}$ is invertible and therefore the group homomorphism $\mathcal{O}^* \to k^*$ is surjective and its kernel is $1+\mathfrak{p}$. We shall occasionally use the following result, which is proved in Serre [1962].

(2.3) LEMMA. *The short exact sequence* $1 \to 1+\mathfrak{p} \to \mathcal{O}^* \to k^* \to 1$ *splits uniquely. In other words* k^* *can be identified with a subgroup of* $\mathcal{O}^*$.

By an $\mathcal{O}$-algebra A, we shall always mean an associative $\mathcal{O}$-algebra which is finitely generated as an $\mathcal{O}$-module and which has a unity element, denoted 1_A, or sometimes simply 1. In most cases A will be either free as an $\mathcal{O}$-module, or annihilated by $\mathfrak{p}$ in which case A is in fact a finite dimensional k-algebra. Of course other cases may occur, including algebras over $\mathcal{O}/\mathfrak{p}^n$. By the finite generation assumption and since $\mathcal{O}$ is noetherian, an $\mathcal{O}$-algebra A is noetherian.

(2.4) CONVENTION. Throughout this book (except in Chapter 8), we assume that every $\mathcal{O}$-algebra A is finitely generated as an $\mathcal{O}$-module. Also the word "module" will always mean "finitely generated module", and all modules are left modules, unless otherwise stated. Thus an A-module, being finitely generated over A, is also finitely generated over $\mathcal{O}$.

(2.5) EXAMPLE. Let G be a finite group and let $\mathcal{O}G$ be the free $\mathcal{O}$-module with basis G. The product in the group G gives rise to a multiplication of basis elements in $\mathcal{O}G$ which can be extended by $\mathcal{O}$-bilinearity to a multiplication in $\mathcal{O}G$. Thus $\mathcal{O}G$ is an $\mathcal{O}$-algebra, called the *group algebra* of G.

(2.6) EXAMPLE. Let V be an $\mathcal{O}$-module. The algebra $\mathrm{End}_{\mathcal{O}}(V)$ of all $\mathcal{O}$-linear endomorphisms of V is an $\mathcal{O}$-algebra. If V is a free $\mathcal{O}$-module of dimension n, then a choice of basis for V yields an isomorphism $\mathrm{End}_{\mathcal{O}}(V) \cong M_n(\mathcal{O})$.

Let A be an $\mathcal{O}$-algebra and let $J(A)$ be the Jacobson radical of A. Since A is a finitely generated $\mathcal{O}$-module, so is any simple left A-module V and it follows from Nakayama's lemma that $\mathfrak{p}\cdot V \neq V$, so that $\mathfrak{p}\cdot V = 0$ (because $\mathfrak{p}\cdot V$ is an A-submodule of V). If M is a maximal left ideal of A, then A/M is a simple A-module and therefore M contains $\mathfrak{p}\cdot A$. This proves that $\mathfrak{p}\cdot A \subseteq J(A)$. It follows that $J(A)$ is the inverse image in A of the Jacobson radical $J(B)$ of the finite dimensional k-algebra $B = A/\mathfrak{p}{\cdot}A$. Consequently $A/J(A) \cong B/J(B)$.

Any maximal (two-sided) ideal $\mathfrak{m}$ of A contains $J(A)$ and therefore $\mathfrak{m}$ is the inverse image of some maximal ideal $\widetilde{\mathfrak{m}}$ of B. Thus the set $\mathrm{Max}(A)$ of maximal ideals of A is in bijection with $\mathrm{Max}(B)$. Similarly the set $\mathrm{Irr}(A)$ of all isomorphism classes of simple A-modules is in bijection with $\mathrm{Irr}(B)$ (because $J(A)$ annihilates any simple A-module W).

By Theorem 1.13, $J(B)$ is nilpotent and is equal to the intersection of all maximal ideals of B. Moreover the set $\mathrm{Max}(B)$ is finite and $B/J(B)$ is isomorphic to a direct product of simple k-algebras

$$A/J(A) \cong B/J(B) \cong \prod_{\widetilde{\mathfrak{m}}\in\mathrm{Max}(B)} B/\widetilde{\mathfrak{m}} \cong \prod_{\mathfrak{m}\in\mathrm{Max}(A)} A/\mathfrak{m}\,.$$

By Wedderburn's theorem, every simple k-algebra $A/\mathfrak{m} \cong B/\widetilde{\mathfrak{m}}$ is isomorphic to the algebra $\mathrm{End}_k(V)$ of all endomorphisms of a finite dimensional k-vector space V (because k is algebraically closed). Now V is the only simple $\mathrm{End}_k(V)$-module up to isomorphism and we can view V as a simple module for B, or for A.

Any simple A-module W arises in this way (up to isomorphism) because the Jacobson radical of A annihilates W, so that W is in fact a simple $A/J(A)$-module, thus a simple module over one of the simple k-algebras $A/\mathfrak{m}$, with the other simple factors of $A/J(A)$ annihilating W. Moreover since there is a single isomorphism class of simple modules over the finite dimensional simple k-algebra $A/\mathfrak{m} \cong \mathrm{End}_k(V)$, the simple module W is isomorphic to V. Note also that $\mathfrak{m}$ is the annihilator of V. Therefore the set $\mathrm{Irr}(A)$ is in bijection with $\mathrm{Max}(A)$.

We now summarize the analysis above.

(2.7) THEOREM. *Let A be an $\mathcal{O}$-algebra (finitely generated as an $\mathcal{O}$-module) and let $J(A)$ be the Jacobson radical of A.*

(a) We have $\mathfrak{p}\cdot A \subseteq J(A)$. Moreover there exists an integer n such that $J(A)^n \subseteq \mathfrak{p}\cdot A$.

(b) $A/J(A)$ is a finite dimensional semi-simple k-algebra and we have

$$A/J(A) \cong \prod_{V \in \mathrm{Irr}(A)} \mathrm{End}_k(V) .$$

(c) Every maximal two-sided ideal $\mathfrak{m}$ of A is the annihilator of some $V \in \mathrm{Irr}(A)$, that is, the kernel of one of the canonical surjections $A \to \mathrm{End}_k(V)$. Moreover this sets up a bijection between $\mathrm{Max}(A)$ and $\mathrm{Irr}(A)$.

(d) $J(A) = \bigcap_{\mathfrak{m} \in \mathrm{Max}(A)} \mathfrak{m}$.

Another important property of $\mathcal{O}$-algebras is the following.

(2.8) PROPOSITION. *If A is an $\mathcal{O}$-algebra, then A is complete in the $J(A)$-adic topology.*

Proof. See Feit [1982], Theorem 9.11. □

Let A and B be two $\mathcal{O}$-algebras. By a *homomorphism* from A to B, we shall always mean a homomorphism $f : A \to B$ of $\mathcal{O}$-algebras which is *not* required to map 1_A to 1_B. Thus f is $\mathcal{O}$-linear and satisfies $f(ab) = f(a)f(b)$ for all $a, b \in A$. If a homomorphism $f : A \to B$ satisfies $f(1_A) = 1_B$, then f is called *unitary*. In the general case $f(1_A)$ is an idempotent of B and the image of f is contained in the subalgebra $f(1_A)Bf(1_A)$ of B. For example if e is an idempotent of A, the inclusion of eAe into A is a homomorphism. It is in fact precisely in order to be able to consider these inclusions that one does not require homomorphisms to be unitary. So another way of visualizing a homomorphism $f : A \to B$ is to view it as a unitary homomorphism $f : A \to eBe$, for some idempotent e of B, followed by the inclusion $eBe \to B$. Note that if $a \in A^*$, then $f(a)$ is in general not invertible (unless f is unitary). But if one adds the complementary idempotent $1_B - f(1_A)$, then $f(a) + (1_B - f(1_A))$ is invertible in B, with inverse $f(a^{-1}) + (1_B - f(1_A))$. Indeed the product of $f(a)$ with $1_B - f(1_A)$ (in either order) is zero. Therefore f induces a group homomorphism $A^* \to B^*$, $a \mapsto f(a) + (1_B - f(1_A))$.

After morphisms, we consider subobjects. By a *subalgebra* B of an $\mathcal{O}$-algebra A, we mean a subset of A which is an $\mathcal{O}$-algebra and such that the inclusion $B \to A$ is a homomorphism. Thus we do not require B to have the same unity element as A. In particular the subalgebras $B = eAe$ (where e is some idempotent of A) will play an extremely important role in the theory of pointed groups.

Exercises

(2.1) Let B be a subalgebra of an $\mathcal{O}$-algebra A.
(a) Prove that $J(A) \cap B \subseteq J(B)$.
(b) If $A = B + J(A)$, prove that $J(A) \cap B = J(B)$.

(2.2) If $f : A \to B$ is a surjective homomorphism of $\mathcal{O}$-algebras, prove that $f(J(A)) \subseteq J(B)$, so that f induces a homomorphism of k-algebras $\overline{f} : A/J(A) \to B/J(B)$. Construct an example of a non-surjective homomorphism for which these properties fail to hold.

(2.3) Let A be an $\mathcal{O}$-algebra. Prove that $\bigcap_{n \geq 1} J(A)^n = \{0\}$.

(2.4) Let A be a non-zero $\mathcal{O}$-algebra. Prove that the subgroup k^* of $\mathcal{O}^*$ (see Lemma 2.3) maps injectively into A^*, so that k^* can be identified with a subgroup of A^*. [Hint: The kernel of the ring homomorphism $\mathcal{O} \to A$ is contained in $\mathfrak{p}$.]

(2.5) Let A be an $\mathcal{O}$-algebra and let n be a positive integer. Prove that $J(M_n(A)) = M_n(J(A))$ and $M_n(A)/J(M_n(A)) \cong M_n(A/J(A))$.

§ 3 LIFTING IDEMPOTENTS

In this section we prove the fundamental theorem on lifting idempotents. Although many of the results appear in other textbooks, our treatment includes material which is less standard. In particular we show that idempotents can be lifted from any quotient of an $\mathcal{O}$-algebra.

Let $\mathcal{O}$ be a ring satisfying Assumption 2.1. Recall that a *point* of an $\mathcal{O}$-algebra A is a conjugacy class of primitive idempotents of A. The set of points of A will be written $\mathcal{P}(A)$. We shall see in the next section that $\mathcal{P}(A)$ is in bijection with $\mathrm{Max}(A)$, hence also with $\mathrm{Irr}(A)$. But we first need to prove the theorem which allows us to lift idempotents as well as invertible elements from $A/J(A)$ up to A.

(3.1) THEOREM. *Let A be an $\mathcal{O}$-algebra, let $\overline{A} = A/J(A)$, and denote by $\overline{a}$ the image of an element $a \in A$ in $\overline{A}$.*

(a) If $\overline{a}$ is invertible in $\overline{A}$, then a is invertible in A. Thus there is an exact sequence of groups

$$1 \longrightarrow 1 + J(A) \longrightarrow A^* \longrightarrow \overline{A}^* \longrightarrow 1 .$$

(b) For any idempotent $e \in \overline{A}$, there exists an idempotent $\widetilde{e} \in A$ such that $\overline{\widetilde{e}} = e$.

(c) Two idempotents $e, f \in A$ are conjugate in A if and only if $\overline{e}$ and $\overline{f}$ are conjugate in $\overline{A}$. More precisely if $\overline{e} = \overline{u}\overline{f}\overline{u}^{-1}$, then $\overline{u}$ lifts to an invertible element $u \in A^*$ such that $e = ufu^{-1}$. In particular if $\overline{e} = \overline{f}$, then there exists $u \in (1 + J(A))$ such that $e = ufu^{-1}$.

(d) An idempotent $e \in A$ is primitive in A if and only if $\overline{e}$ is primitive in $\overline{A}$.

(e) The map $A \to \overline{A}$ induces a bijection $\mathcal{P}(A) \to \mathcal{P}(\overline{A})$.

(f) If $e \in A$ is an idempotent and if $\overline{I}$ is a decomposition (respectively a primitive decomposition) of $\overline{e}$ in $\overline{A}$, then $\overline{I}$ lifts to a decomposition I (respectively a primitive decomposition) of e in A.

(g) Let I be a decomposition of an idempotent $e \in A$ and let J be a decomposition of an idempotent $f \in A$. If $\overline{I} = \overline{u}\overline{J}\overline{u}^{-1}$ for some $\overline{u} \in \overline{A}^*$, then $\overline{u}$ lifts to an element $u \in A^*$ such that $I = uJu^{-1}$. In particular if $\overline{I} = \overline{J}$, then there exists $u \in (1 + J(A))$ such that $I = uJu^{-1}$.

(h) If $\mathfrak{a}$ is an ideal of A and if e is an idempotent of A, then $e \in \mathfrak{a}$ if and only if $\overline{e} \in \overline{\mathfrak{a}}$.

Proof. (a) If $a \in A$ is not invertible, then either Aa or aA is not equal to A (in fact both) and we assume $Aa \neq A$. Then $a \in M$ for some maximal left ideal M by Zorn's lemma. Since $M \supseteq J(A)$, its image $\overline{M}$ is a maximal left ideal of $\overline{A}$ and we have $\overline{a} \in \overline{M}$. Thus $\overline{a}$ is not invertible.

(b) Choose $a_1 \in A$ such that $\overline{a}_1 = e$ and let $b_1 = a_1^2 - a_1$. Define by induction two sequences of elements of A:

$$a_n = a_{n-1} + b_{n-1} - 2a_{n-1}b_{n-1} \quad \text{and} \quad b_n = a_n^2 - a_n .$$

We show by induction that $a_n^2 \equiv a_n \pmod{J(A)^n}$, or in other words that $b_n \in J(A)^n$. Assuming that this holds for n, we have $b_n^2 \in J(A)^{n+1}$ (because $(J(A)^n)^2 \subseteq J(A)^{n+1}$), and since $a_n^2 = a_n + b_n$ we obtain

$$\begin{aligned} a_{n+1}^2 &\equiv a_n^2 + 2a_nb_n - 4a_n^2b_n = a_n + b_n + 2a_nb_n - 4(a_n+b_n)b_n \\ &\equiv a_n + b_n - 2a_nb_n = a_{n+1} \pmod{J(A)^{n+1}} . \end{aligned}$$

It follows that (b_n) converges to 0 and that (a_n) is a Cauchy sequence (in the $J(A)$-adic topology). Since A is complete (by Lemma 2.8), (a_n) converges to some element $\widetilde{e} \in A$ and $\widetilde{e}^2 - \widetilde{e} = \lim b_n = 0$. Moreover $\overline{\widetilde{e}} = \overline{a}_1 = e$. Without reference to the sequence (b_n), one can also define directly $a_n = 3a_{n-1}^2 - 2a_{n-1}^3$.

(c) It is clear that $\overline{e}$ and $\overline{f}$ are conjugate if e and f are conjugate. Conversely assume that $\overline{e}$ and $\overline{f}$ are conjugate by some element $\overline{u} \in \overline{A}^*$. Then by (a), we know that any lift $u \in A^*$ is invertible and so, replacing f by ufu^{-1}, we can assume $\overline{e} = \overline{f}$. Now let $v = 1_A - e - f + 2ef$. Then by (a), $v \in A^*$, because $\overline{v} = 1_{\overline{A}}$. Moreover one has $ev = ef = vf$ and it follows that $e = vfv^{-1}$.

(d) We use localization. Recall that e is primitive in A if and only if e and 0 are the only idempotents of eAe. Since $J(eAe) = eJ(A)e = J(A) \cap eAe$ by Proposition 1.17, we have $eAe/J(eAe) \cong \overline{eAe} = \overline{e}\overline{A}\overline{e}$. If $\overline{f}$ is a non-trivial idempotent of $\overline{e}\overline{A}\overline{e}$, then by (b) applied to the algebra eAe, the idempotent $\overline{f}$ lifts to an idempotent $f \in eAe$. This proves that $\overline{e}$ is primitive if e is primitive. Conversely if e is not primitive, there exists a non-trivial idempotent $f \in eAe$. Then f is not conjugate (that is, not equal) to 0 nor to the unity element e. By (c) it follows that $\overline{f}$ is a non-trivial idempotent of $\overline{e}\overline{A}\overline{e}$.

(e) This follows immediately from (b), (c) and (d).

(f) Replacing A by eAe, we can assume that $e = 1$. We write $\overline{I} = \{\overline{i}_1, \ldots, \overline{i}_n\}$ and we use induction on n. If f is an idempotent which lifts $\overline{f} = \overline{i}_1 + \ldots + \overline{i}_{n-1}$, there exists a decomposition $f = i_1 + \ldots + i_{n-1}$ such that i_r lifts $\overline{i}_r$ for $1 \leq r \leq n-1$. Letting $i_n = 1 - f$, we obtain a decomposition $1 = i_1 + \ldots + i_n$ and i_n lifts $\overline{i}_n$ as required. Moreover by (d), i_r is primitive if and only if $\overline{i}_r$ is primitive.

(g) We can first lift u arbitrarily and replace J by uJu^{-1} (because u is invertible by (a)). Thus we can assume that $\overline{I} = \overline{J}$. Next we know by (c) that $e = vfv^{-1}$ for some $v \in (1 + J(A))$ and, replacing J by vJv^{-1}, we can assume as well that $e = f$. Write

$$I = \{ i_1, \ldots, i_n \} \qquad \text{and} \qquad J = \{ j_1, \ldots, j_n \},$$

labelled in such a way that $\overline{i}_r = \overline{j}_r$ for $1 \le r \le n$. Now let

$$w = \sum_{r=1}^{n} i_r j_r + (1 - e).$$

We have $\overline{w} = 1$, so that $w \in (1 + J(A))$. Moreover $i_r w = i_r j_r = w j_r$ and it follows that $w j_r w^{-1} = i_r$.

(h) One implication is trivial. Assume that $\overline{e} \in \overline{\mathfrak{a}}$. Then we have $e \in (\mathfrak{a} + J(A))$ and since e is idempotent, $e \in (\mathfrak{a} + J(A))^n \subseteq \mathfrak{a} + J(A)^n$ for all n. But $(\mathfrak{a} + J(A))/\mathfrak{a} = J(A/\mathfrak{a})$ and $(\mathfrak{a} + J(A)^n)/\mathfrak{a} = J(A/\mathfrak{a})^n$. Since $\bigcap_{n \ge 0} J(A/\mathfrak{a})^n = \{0\}$ by Proposition 1.2 (because $A/\mathfrak{a}$ is noetherian), we have $\bigcap_{n \ge 0} (\mathfrak{a} + J(A)^n) = \mathfrak{a}$, and it follows that $e \in \mathfrak{a}$. □

Our first application of Theorem 3.1 is a generalization of that theorem which allows us to lift idempotents from a quotient $A/\mathfrak{b}$ for an arbitrary ideal $\mathfrak{b}$.

(3.2) THEOREM. *Let A be an $\mathcal{O}$-algebra, let $\mathfrak{b}$ be an ideal of A, let $\overline{A} = A/\mathfrak{b}$, and denote by $\overline{a}$ the image of an element $a \in A$ in $\overline{A}$.*

(a) The map $A^* \to \overline{A}^*$ is surjective.

(b) For any idempotent $\overline{e} \in \overline{A}$ and any primitive decomposition $\overline{I}$ of $\overline{e}$, there exists an idempotent $e \in A$ lifting $\overline{e}$ and a primitive decomposition I of e lifting $\overline{I}$.

(c) Let $e \in A$ be an idempotent. If e is primitive, then $\overline{e}$ is either zero or primitive. If conversely $\overline{e}$ is primitive, then there exists an orthogonal decomposition $e = e' + f$ where e' is primitive and $f \in \mathfrak{b}$ (so that $\overline{e}' = \overline{e}$).

(d) Let I be a primitive decomposition of an idempotent $e \in A$ such that $i \notin \mathfrak{b}$ for every $i \in I$ and let J be a primitive decomposition of an idempotent $f \in A$ such that $j \notin \mathfrak{b}$ for every $j \in J$. If $\overline{I} = \overline{u}\overline{J}\overline{u}^{-1}$ for some $\overline{u} \in \overline{A}^*$, then $\overline{u}$ lifts to an element $u \in A^*$ such that $I = uJu^{-1}$. In particular if $\overline{I} = \overline{J}$, then there exists $u \in A^*$ with $\overline{u} = 1$ such that $I = uJu^{-1}$.

(e) The map $A \to \overline{A}$ induces a bijection $\mathcal{P}(A - \mathfrak{b}) \to \mathcal{P}(\overline{A})$, where $\mathcal{P}(A - \mathfrak{b})$ denotes the set of points of A which do not lie in $\mathfrak{b}$.

(f) If $\mathfrak{a}$ is an ideal of A and if e is a primitive idempotent of $A - \mathfrak{b}$, then $e \in \mathfrak{a}$ if and only if $\overline{e} \in \overline{\mathfrak{a}}$.

Proof. Consider the following diagram where π_A and $\pi_{\overline{A}}$ denote the canonical surjections:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & J(A) & \longrightarrow & A & \xrightarrow{\pi_A} & A/J(A) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & J(\overline{A}) & \longrightarrow & \overline{A} & \xrightarrow{\pi_{\overline{A}}} & \overline{A}/J(\overline{A}) & \longrightarrow & 0
\end{array}$$

All vertical maps are surjective because $J(\overline{A}) = (J(A)+\mathfrak{b})/\mathfrak{b} = \overline{J(A)}$. Since $A/J(A)$ is semi-simple, we have $A/J(A) \cong \overline{A}/J(\overline{A}) \times B$ where B is a semi-simple algebra (in fact $B = (\mathfrak{b}+J(A))/J(A)$ as an ideal of $A/J(A)$). It follows that the map on the right hand side has a section $s : \overline{A}/J(\overline{A}) \to A/J(A)$ which is an algebra homomorphism (mapping 1 to an idempotent of $A/J(A)$). Now consider the corresponding diagram for invertible elements:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & 1+J(A) & \longrightarrow & A^* & \xrightarrow{\pi_A} & (A/J(A))^* & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & 1+J(\overline{A}) & \longrightarrow & \overline{A}^* & \xrightarrow{\pi_{\overline{A}}} & (\overline{A}/J(\overline{A}))^* & \longrightarrow & 0
\end{array}$$

By Theorem 3.1, both horizontal sequences are exact. Since $J(A)$ maps onto $J(\overline{A})$, the vertical map on the left hand side is surjective. The one on the right hand side is surjective too because $(A/J(A))^*$ is isomorphic to the direct product $(\overline{A}/J(\overline{A}))^* \times B^*$. Therefore by elementary diagram chasing, the middle vertical map is surjective, which proves (a).

(b) It is clear that any primitive decomposition of an idempotent in $\overline{A}/J(\overline{A})$ can be lifted to $A/J(A)$ via the section s. Applying this to $\pi_{\overline{A}}(\overline{I})$ (which is a primitive decomposition by Theorem 3.1) and then lifting the result to A, one obtains an idempotent $e \in A$ and a primitive decomposition J of e such that $\pi_{\overline{A}}(\overline{J}) = \pi_{\overline{A}}(\overline{I})$. By Theorem 3.1, there exists $\overline{u} \in (1+J(\overline{A}))$ such that $\overline{I} = \overline{u}\overline{J}\overline{u}^{-1}$. Lifting $\overline{u}$ to $u \in (1+J(A))$, one gets a primitive decomposition $I = uJu^{-1}$ which maps to $\overline{I}$ in $\overline{A}$. This completes the proof of (b).

(c) By Theorem 3.1, the primitivity of idempotents can be read in semi-simple quotients. Thus it suffices to prove that $\pi_A(e)$ is primitive if and only if $\pi_{\overline{A}}(\overline{e})$ is primitive. But this is clear because the assumption on e implies that in the decomposition $A/J(A) \cong \overline{A}/J(\overline{A}) \times B$, the idempotent $\pi_A(e)$ has zero component in $B = (\mathfrak{b}+J(A))/J(A)$ (using part (h) of Theorem 3.1), while the other component is $\pi_{\overline{A}}(\overline{e})$.

(d) We have $\overline{I} = \overline{u}\overline{J}\overline{u}^{-1}$ by assumption and we know by (a) that $\overline{u}$ lifts to an invertible element of A. Thus we can replace J by a conjugate and assume that $\overline{I} = \overline{J}$. Consider the images $\pi_A(I)$ and $\pi_A(J)$

in $A/J(A) \cong \overline{A}/J(\overline{A}) \times B$. By assumption the primitive idempotents in I and J do not belong to $\mathfrak{b}$ and this implies that their images in B are zero. On the other hand the images of I and J in $\overline{A}/J(\overline{A})$ are both equal to $\pi_{\overline{A}}(\overline{I}) = \pi_{\overline{A}}(\overline{J})$. Therefore $\pi_A(I) = \pi_A(J)$. It follows from Theorem 3.1 that I and J are conjugate.

The more precise statement that I and J are conjugate by an element v such that $\overline{v} = 1$ follows from the proof of part (g) of Theorem 3.1. The details are left as an exercise for the reader.

(e) This is a direct consequence of (b), (c) and (d).

(f) This is an easy exercise. The result is also a special case of Corollary 4.11 which is proved in the next section. □

Exercises

(3.1) Let M be a left ideal in an $\mathcal{O}$-algebra A . Prove that either M contains an idempotent or we have $M \subseteq J(A)$.

(3.2) Let e and f be two idempotents of an $\mathcal{O}$-algebra A . Prove that if $e = ab$ and $f = ba$ for some $a, b \in A$, then e and f are conjugate (and conversely). [Hint: Reduce the problem to the case where A is a matrix algebra over k and then use Proposition 1.14.]

(3.3) Let a and b be two elements of an $\mathcal{O}$-algebra A such that $ab = 1$. Prove that $ba = 1$. [Hint: Use exercise 3.2.]

(3.4) Complete the details of the proof of parts (d) and (f) of Theorem 3.2.

§ 4 IDEMPOTENTS AND POINTS

We use the main theorem on lifting idempotents to derive various important results on idempotents and points. In particular we show that primitive decompositions are unique up to conjugation and that there are bijections between points, maximal ideals, and simple modules. We also include proofs of the Krull–Schmidt theorem, Hensel's lemma and Rosenberg's lemma. We continue with our base ring $\mathcal{O}$ satisfying Assumption 2.1.

First we combine Theorem 3.1 with Proposition 1.15 to obtain the following two basic theorems.

(4.1) THEOREM. *Let A be an $\mathcal{O}$-algebra. Any two primitive decompositions of 1_A are conjugate under A^*.*

In the commutative case, the theorem takes the following form, which is often useful.

(4.2) COROLLARY. *If A is a commutative $\mathcal{O}$-algebra, then there exists a unique primitive decomposition of 1_A. In particular any two primitive idempotents of A are either equal or orthogonal.*

The other theorem which follows from Theorem 3.1 and Proposition 1.15 is the following.

(4.3) THEOREM. *Let A be an $\mathcal{O}$-algebra. The set $\mathcal{P}(A)$ of points of A is in bijection with both $\mathrm{Max}(A)$ and $\mathrm{Irr}(A)$. If $\alpha \in \mathcal{P}(A)$, the corresponding maximal ideal $\mathfrak{m}_\alpha$ is characterized by the property $e \notin \mathfrak{m}_\alpha$ for some $e \in \alpha$ (or equivalently for every $e \in \alpha$), while the corresponding simple A-module $V(\alpha)$ is characterized by the property $e \cdot V(\alpha) \neq 0$ for some $e \in \alpha$ (or equivalently for every $e \in \alpha$). Also $V(\alpha) \cong Ae/J(A)e$ if $e \in \alpha$.*

For every point $\alpha \in \mathcal{P}(A)$, the notation $\mathfrak{m}_\alpha$ and $V(\alpha)$ of the theorem will be in force throughout this book. Also the simple algebra $A/\mathfrak{m}_\alpha$ will be written $S(\alpha)$. Thus we have $S(\alpha) \cong \mathrm{End}_k(V(\alpha))$ and the notation for the semi-simple quotient of A becomes

$$A/J(A) \cong \prod_{\alpha \in \mathcal{P}(A)} S(\alpha) \, .$$

An important application of Theorem 4.1 is the Krull–Schmidt theorem. Recall that a module M is called *indecomposable* if $M \neq 0$ and if M cannot be decomposed as the direct sum of two non-zero submodules.

(4.4) THEOREM (Krull–Schmidt). *Let A be an $\mathcal{O}$-algebra and let M be an A-module (finitely generated).*

(a) There exists a decomposition $M = \bigoplus_{\lambda \in \Lambda} M_\lambda$ as a finite direct sum of indecomposable A-modules.

(b) For any decomposition of M as a finite direct sum of indecomposable A-modules $M = \bigoplus_{\delta \in \Delta} M'_\delta$, there exist a bijection $\sigma : \Lambda \xrightarrow{\sim} \Delta$ and an A-linear automorphism ϕ of M such that $\phi(M_\lambda) = M'_{\sigma(\lambda)}$ for every $\lambda \in \Lambda$.

Proof. By Proposition 1.16, a direct sum decomposition of M corresponds to an idempotent decomposition of id_M in $\mathrm{End}_A(M)$. Explicitly, if $M = \bigoplus_{\lambda \in \Lambda} M_\lambda$, then $id_M = \sum_\lambda e_\lambda$ where e_λ is the projection onto M_λ with kernel $\bigoplus_{\mu \neq \lambda} M_\mu$. Moreover M_λ is indecomposable if and only if e_λ is primitive. Since M is finitely generated and A is finitely generated as an $\mathcal{O}$-module, M is finitely generated as an $\mathcal{O}$-module and therefore so is $\mathrm{End}_{\mathcal{O}}(M)$, as well as its subalgebra $\mathrm{End}_A(M)$. In particular $\mathrm{End}_A(M)$ is noetherian and by Proposition 1.16, there exists a primitive decomposition of id_M, proving (a).

If the decomposition $M = \bigoplus_{\delta \in \Delta} M'_\delta$ into indecomposable summands corresponds to a primitive decomposition $id_M = \sum_\delta e'_\delta$, then by Theorem 4.1, this decomposition is conjugate to the given one by some element $\phi \in \mathrm{End}_A(M)^*$, that is, $\phi e_\lambda \phi^{-1} = e'_{\sigma(\lambda)}$ for some bijection $\sigma : \Lambda \xrightarrow{\sim} \Delta$. Then for every $\lambda \in \Lambda$, we have

$$\phi(M_\lambda) = \phi(e_\lambda M) = \phi e_\lambda \phi^{-1} M = e'_{\sigma(\lambda)} M = M'_{\sigma(\lambda)},$$

as required. □

(4.5) COROLLARY. *Let A be an $\mathcal{O}$-algebra, let M be an A-module, and let N and N' be two direct summands of M, corresponding to idempotents e and e' of* $\mathrm{End}_A(M)$ *respectively (that is, $N = eM$ and $N' = e'M$). Then N is isomorphic to N' if and only if e and e' are conjugate in* $\mathrm{End}_A(M)$.

Proof. If there exists $\phi \in \mathrm{End}_A(M)^*$ such that $\phi e \phi^{-1} = e'$, then the automorphism ϕ of M maps eM isomorphically onto $e'M$. Assume conversely that $eM \cong e'M$. Then we have two decompositions

$$M = eM \oplus (1-e)M = e'M \oplus (1-e')M$$

and by an easy application of the Krull–Schmidt theorem (Exercise 4.2), we also have an isomorphism $(1-e)M \cong (1-e')M$. The direct sum of the two isomorphisms yields an automorphism ϕ of M such that $\phi(eM) = e'M$ and $\phi((1-e)M) = (1-e')M$. Then $\phi e \phi^{-1}$ is an idempotent with kernel $(1-e')M$ and image $e'M$, which means that $\phi e \phi^{-1} = e'$. □

The next application of Theorem 3.1 tells us that the localization eAe is indeed a local ring when e is primitive.

(4.6) COROLLARY. *Let* A *be an* $\mathcal{O}$*-algebra and let* e *be an idempotent of* A. *Then* e *is primitive if and only if* eAe *is a local ring. In that case,* $J(eAe) = eJ(A)e$ *is the unique maximal ideal of* eAe, *with simple quotient* $eAe/eJ(A)e$ *isomorphic to* k.

Proof. Suppose first that eAe is a local ring. If $e = f + g$, where f and g are orthogonal idempotents of A, then f and g necessarily belong to eAe (because $f = efe$ and $g = ege$). But a local ring cannot have any non-trivial idempotent (because if i is an idempotent of a local ring, then either i or $1 - i$ must be invertible, hence equal to 1). It follows that either f or g is equal to e, which is the unity element of eAe.

Suppose now that e is primitive. Since every maximal ideal of eAe contains $J(eAe)$ and since $J(eAe) = eJ(A)e$ by Proposition 1.17, it suffices to prove that $eAe/eJ(A)e \cong k$. But $eAe/eJ(A)e$ is a semi-simple finite dimensional k-algebra and its unity element is primitive by part (d) of Theorem 3.1. This forces $eAe/eJ(A)e$ to be a division algebra and this can only be isomorphic to k since k is algebraically closed (Proposition 1.7). □

A useful consequence of Theorem 3.1 is Hensel's lemma. Since k is algebraically closed by assumption, any polynomial over k has all its roots in k and the lemma deals with the question of lifting these roots to $\mathcal{O}$.

(4.7) PROPOSITION (Hensel's lemma). *Let* $f \in \mathcal{O}[t]$ *be a polynomial in an indeterminate* t, *with leading coefficient 1, and let* $\overline{f} \in k[t]$ *be its image modulo* $\mathfrak{p}$. *If all the roots of* $\overline{f}$ *are distinct, then these roots lift uniquely to roots of* f *in* $\mathcal{O}$ *and* f *decomposes as a product of linear factors over* $\mathcal{O}$.

Proof. Let $A = \mathcal{O}[t]/(f)$ and $\overline{A} = A/\mathfrak{p}A = k[t]/(\overline{f})$. By assumption and by the Chinese remainder theorem, we have

$$\overline{A} \cong \prod_{i=1}^{n} k[t]/(t - \overline{\alpha}_i) \cong \prod_{i=1}^{n} k,$$

where n is the degree of f and $\{\overline{\alpha}_1, \ldots, \overline{\alpha}_n\}$ are the distinct roots of $\overline{f}$. Moreover the projection onto the i-th factor maps t to $\overline{\alpha}_i$. Let $\overline{e}_i$ be the primitive idempotent of $\overline{A}$ mapping to 1 in the i-th factor and to zero in the other factors, so that $\overline{A}\overline{e}_i \cong k$. By Theorem 3.1, $\overline{e}_i$ lifts to an idempotent $e_i \in A$ and $\sum_i e_i = 1$. Since $\overline{A}$ has dimension n, the primitive idempotents $\overline{e}_i$ form a k-basis of $\overline{A}$. Since f has leading coefficient 1, A is a free $\mathcal{O}$-module (with basis $\{1, t, t^2, \ldots, t^{n-1}\}$) and it follows from Proposition 1.3 that the idempotents e_i form an $\mathcal{O}$-basis of A. The decomposition $A = \bigoplus_i Ae_i$ now implies that $Ae_i \cong \mathcal{O}$ and therefore we have ring isomorphisms

$$A \cong \prod_{i=1}^{n} Ae_i \cong \prod_{i=1}^{n} \mathcal{O} .$$

Since t is a root of f in A, its image α_i in the i-th factor is a root of f in $\mathcal{O}$. Clearly α_i lifts $\overline{\alpha}_i$ and $f = \prod_{i=1}^{n}(t-\alpha_i)$. □

(4.8) COROLLARY. *Let $a \in \mathcal{O}^*$ and let n be a positive integer not divisible by p. Then a has n distinct n-th roots in $\mathcal{O}$.*

Proof. Let $\overline{a}$ be the image of a in k. Apply Hensel's lemma to the polynomial $f = t^n - a$. Its image $\overline{f} = t^n - \overline{a}$ has distinct roots in k because its derivative nt^{n-1} is non-zero (since n is prime to p) and has no root in common with $\overline{f}$ (because $\overline{a} \neq 0$ since a is invertible). □

Another application of Theorem 3.1 is Rosenberg's lemma. An alternative proof is given in Exercise 4.1.

(4.9) PROPOSITION (Rosenberg's lemma). *Let e be a primitive idempotent of an $\mathcal{O}$-algebra A and let $\mathcal{X}$ be a family of ideals of A. If we have $e \in \sum_{\mathfrak{a}\in\mathcal{X}} \mathfrak{a}$, then there exists $\mathfrak{a} \in \mathcal{X}$ such that $e \in \mathfrak{a}$.*

Proof. Part (h) of Theorem 3.1 allows us to replace A by its semi-simple quotient $A/J(A)$. In the semi-simple case, the result is trivial because an ideal is necessarily a direct sum of some of the simple factors, while a primitive idempotent lies in exactly one of the factors. □

(4.10) COROLLARY. *Let $\alpha \in \mathcal{P}(A)$ be a point of A, let $\mathfrak{m}_\alpha$ be the corresponding maximal ideal, let $e \in \alpha$, and let $\mathfrak{b}$ be an ideal of A. The following conditions are equivalent.*
(a) $e \notin \mathfrak{b}$.
(b) $\alpha \not\subseteq \mathfrak{b}$.
(c) $\mathfrak{b} \subseteq \mathfrak{m}_\alpha$.

Proof. Since $\mathfrak{b}$ is an ideal, it is clear that (a) and (b) are equivalent. Since $e \notin \mathfrak{m}_\alpha$, (c) implies (a). Finally if $e \notin \mathfrak{b}$, then Rosenberg's lemma implies that $e \notin \mathfrak{b}+\mathfrak{m}_\alpha$. Therefore $\mathfrak{b}+\mathfrak{m}_\alpha \neq A$ and by maximality of $\mathfrak{m}_\alpha$, it follows that $\mathfrak{b} \subseteq \mathfrak{m}_\alpha$. This proves that (a) implies (c). □

Another useful consequence of Rosenberg's lemma is the following.

(4.11) COROLLARY. *Let* $f : A \to B$ *be a homomorphism of* $\mathcal{O}$*-algebras, let* $\mathfrak{b}$ *be an ideal of* A *, and let* e *be a primitive idempotent of* A *which does not belong to* $\mathrm{Ker}(f)$ *. Then* $e \in \mathfrak{b}$ *if and only if* $f(e) \in f(\mathfrak{b})$ *.*

Proof. We have $f(e) \in f(\mathfrak{b})$ if and only if $e \in \mathfrak{b} + \mathrm{Ker}(f)$. By Rosenberg's lemma, this is equivalent to $e \in \mathfrak{b}$ because $e \notin \mathrm{Ker}(f)$. □

If $f : A \to B$ is a homomorphism of $\mathcal{O}$-algebras, the image of a primitive idempotent of A is in general not a primitive idempotent of B . The easiest example occurs when $A = \mathcal{O}$ and f is the natural map making B into an $\mathcal{O}$-algebra: the image of the primitive idempotent $1_{\mathcal{O}}$ is 1_B , which decomposes according to the points of B and their multiplicities (defined below). As a result, a homomorphism of $\mathcal{O}$-algebras may not induce a map between the points of A and the points of B . However, we prove here that if e is an idempotent of A , the inclusion $eAe \to A$ behaves very well with regard to points.

(4.12) PROPOSITION. *Let* A *be an* $\mathcal{O}$*-algebra, let* e *be an idempotent of* A *, and let* j *and* j' *be two idempotents of* eAe *.*

(a) *If* j *is primitive in* eAe *, then* j *is primitive in* A *(and conversely).*

(b) *If* j *and* j' *are conjugate in* A *, then they are conjugate in* eAe *(and conversely).*

(c) *The inclusion* $eAe \to A$ *induces an injection* $\mathcal{P}(eAe) \to \mathcal{P}(A)$ *.*

Proof. First note that (c) is a direct consequence of (a) and (b): the existence of a map $\mathcal{P}(eAe) \to \mathcal{P}(A)$ follows from (a) (and the converse of (b)), and (b) shows that this map is injective.

Let $B = eAe$. Recall that $J(B) = eJ(A)e$, that is, $J(B) = J(A) \cap B$. Therefore the inclusion $B \to A$ induces an injective homomorphism of semi-simple algebras $B/J(B) \to A/J(A)$. The image of this homomorphism is $\overline{e}\overline{A}\overline{e}$ (where $\overline{A} = A/J(A)$ and $\overline{e}$ is the image of e in $\overline{A}$). Since primitivity as well as conjugation of idempotents can be read in semi-simple quotients (Theorem 3.1), it follows that it suffices to prove (a) and (b) for semi-simple algebras.

If $A = S_1 \times \ldots \times S_r$ is semi-simple, then $e = (e_1, \ldots, e_r)$ where e_i is an idempotent of S_i , and $eAe = e_1S_1e_1 \times \ldots \times e_rS_re_r$ is the decomposition of eAe into simple algebras. Decomposing the idempotents j and j' into their r components, it is clear that it suffices to prove (a) and (b) for each simple algebra S_i . Thus we can assume that A is simple, hence isomorphic to $\mathrm{End}_k(V)$, where V is a finite dimensional k-vector space (thanks to our assumption that k is algebraically closed, see Proposition 1.7). Then e is a projection onto some subspace W and $eAe \cong \mathrm{End}_k(W)$.

Now (a) is obvious since, by Proposition 1.14, a primitive idempotent of either $\mathrm{End}_k(V)$ or $\mathrm{End}_k(W)$ is a projection onto some one-dimensional subspace. Proposition 1.14 also implies (b) since the conjugacy of idempotents comes down to the equality of their ranks. □

We note that (a) can be proved in a more direct fashion (Exercise 4.5).

With each point $\alpha \in \mathcal{P}(A)$, we associate an ideal which will be used extensively, namely the ideal $A\alpha A$ generated by α. An element of $A\alpha A$ is a finite sum of elements of the form aeb, where $e \in \alpha$ and $a, b \in A$. Note that since all elements of α are conjugate, we have $A\alpha A = AeA$ for every $e \in \alpha$. If $\beta \in \mathcal{P}(A)$ is a point of A, the image of $A\alpha A$ in the simple quotient $S(\beta)$ is equal to zero if $\beta \neq \alpha$ and to the whole of $S(\alpha)$ otherwise. Thus the image $\overline{A\alpha A}$ of $A\alpha A$ in $\overline{A} = A/J(A)$ is equal to the minimal ideal of $\overline{A}$ isomorphic to $S(\alpha)$. The ideal $A\alpha A$ is minimal with respect to the property that its image in $S(\alpha)$ is non-zero (that is, the whole of $S(\alpha)$). Indeed, since a primitive idempotent e in α has non-zero image in $S(\alpha)$, an ideal satisfying this property must contain e by Theorem 3.2, hence the whole of α since it is an ideal. Summarizing these remarks, we also express these properties in terms of maximal ideals.

(4.13) LEMMA. *Let A be an $\mathcal{O}$-algebra and let $\alpha \in \mathcal{P}(A)$ with corresponding maximal ideal $\mathfrak{m}_\alpha$ and simple quotient $S(\alpha)$.*

(a) The ideal $A\alpha A$ is the unique minimal element of the set of all ideals $\mathfrak{b}$ such that $\mathfrak{b} + \mathfrak{m}_\alpha = A$.

(b) The ideal $A\alpha A$ satisfies $A\alpha A \subseteq \mathfrak{m}_\beta$ for every $\beta \in \mathcal{P}(A)$ with $\beta \neq \alpha$.

(c) The image of $A\alpha A$ in the semi-simple quotient $\overline{A} = A/J(A)$ is equal to the minimal ideal of $\overline{A}$ isomorphic to $S(\alpha)$.

The ideals $A\alpha A$ are often used in the following context.

(4.14) PROPOSITION. *Let A be an $\mathcal{O}$-algebra and let $\mathfrak{b}$ be an ideal of A.*

(a) $\mathfrak{b} = \sum_{\alpha \in \mathcal{P}(A)} (A\alpha A \cap \mathfrak{b})$. *In particular* $A = \sum_{\alpha \in \mathcal{P}(A)} A\alpha A$.

(b) $\mathfrak{b} \subseteq \sum_{\substack{\alpha \in \mathcal{P}(A) \\ \alpha \subseteq \mathfrak{b}}} A\alpha A + J(A)$.

Proof. (a) Writing 1_A as a sum of primitive idempotents and multiplying (say on the left) by an arbitrary element of $\mathfrak{b}$, one obtains immediately $\mathfrak{b} = \sum_{\alpha\in\mathcal{P}(A)}(A\alpha\cap\mathfrak{b})$. The result follows from the obvious inclusion $A\alpha \subseteq A\alpha A$.

(b) It suffices to prove the result for the image of $\mathfrak{b}$ in $A/J(A)$. Thus we can assume that A is semi-simple. The result is trivial in that case because an ideal is necessarily a direct sum of some of the simple factors $S(\alpha)$, and $\alpha \subseteq \mathfrak{b}$ if and only if $S(\alpha) \subseteq \mathfrak{b}$. Here for simplicity we have identified $S(\alpha)$ with the minimal ideal of A isomorphic to $S(\alpha)$. □

Finally we introduce multiplicities. Let A be an $\mathcal{O}$-algebra and let I be a primitive decomposition of 1_A. For every point $\alpha \in \mathcal{P}(A)$, we consider the set $I_\alpha = I \cap \alpha$ of all idempotents in the decomposition which belong to α. Therefore we can write

$$1_A = \sum_{\alpha\in\mathcal{P}(A)} \sum_{i\in I_\alpha} i .$$

The number of elements of I_α is called the *multiplicity* of α in A and is written m_α (not to be confused with the maximal ideal $\mathfrak{m}_\alpha$). In other words m_α is the number of occurrences of idempotents of α in a primitive decomposition of 1_A. Since all primitive decompositions of 1_A are conjugate, m_α does not depend on the choice of I.

By Theorem 3.1, the image in $A/J(A)$ of the primitive decomposition above yields a primitive decomposition of the unity element of $A/J(A)$, so that the multiplicities of points can be read in $A/J(A)$. Moreover $A/J(A) \cong \prod_{\alpha\in\mathcal{P}(A)} S(\alpha)$ (where each $S(\alpha)$ is the simple quotient of A corresponding to α), and the primitive decomposition of 1 in $A/J(A)$ is the sum of primitive decompositions of the unity element of each $S(\alpha)$. Therefore the image in $S(\alpha)$ of the sum $\sum_{i\in I_\alpha} i$ is a primitive decomposition of the unity element of $S(\alpha) \cong \mathrm{End}_k(V(\alpha))$. Since a primitive idempotent of $S(\alpha)$ is a projection onto a one-dimensional summand of $V(\alpha)$ (Proposition 1.14), it follows that m_α is the dimension of $V(\alpha)$. In other words m_α is the size of the matrix algebra $S(\alpha)$, that is, $\dim_k(S(\alpha)) = m_\alpha^2$. We record these facts for later use.

(4.15) PROPOSITION. *Let A be an $\mathcal{O}$-algebra and let m_α be the multiplicity of a point $\alpha \in \mathcal{P}(A)$.*

(a) $m_\alpha = \dim_k(V(\alpha))$, where $V(\alpha)$ is a simple A-module corresponding to α.

(b) $m_\alpha^2 = \dim_k(S(\alpha))$, where $S(\alpha)$ is the simple quotient of A corresponding to α.

For the reasons above, the simple quotient $S(\alpha)$ corresponding to a point α is called the *multiplicity algebra* of the point α. Similarly, if we write $S(\alpha) \cong \mathrm{End}_k(V(\alpha))$, the simple A-module $V(\alpha)$ is also called the *multiplicity module* of the point α.

If e is an idempotent of A, one can also consider the *multiplicity of* α *in* e, namely the number of idempotents in α appearing in a primitive decomposition of e. This number is written $m_\alpha(e)$. It is not difficult to see that $m_\alpha(e)$ is either zero or is the multiplicity of a point of the algebra eAe (Exercise 4.3).

(4.16) PROPOSITION. *Let A be an $\mathcal{O}$-algebra and let e and f be two idempotents of A. Then e and f are conjugate if and only if we have $m_\alpha(e) = m_\alpha(f)$ for every $\alpha \in \mathcal{P}(A)$.*

Proof. If e and f are conjugate, it is clear that $m_\alpha(e) = m_\alpha(f)$ for every $\alpha \in \mathcal{P}(A)$. Assume conversely that these equalities hold. Since two idempotents are conjugate in A if and only if they are conjugate in $A/J(A)$ (by Theorem 3.1) and since the multiplicities do not change by passing to $A/J(A)$, we can assume that A is semi-simple. Then it suffices to consider the components of e and f in each simple factor of A, so we can assume that A is simple, thus with a single point α. The assumption on multiplicities now reduces to the fact that both e and f decompose as a sum of m primitive idempotents, where $m = m_\alpha(e) = m_\alpha(f)$. But $S \cong \mathrm{End}_k(V)$ for some k-vector space V and since a primitive idempotent is a projection onto a one-dimensional subspace, it is clear that e is a projection onto an m-dimensional subspace. The same holds for f and therefore e and f are conjugate (Proposition 1.14). □

Exercises

(4.1) Use Corollary 4.6 to give an alternative proof of Rosenberg's lemma.

(4.2) Let A be an $\mathcal{O}$-algebra. Let L, M and N be A-modules such that $L \oplus M \cong L \oplus N$. Prove that $M \cong N$.

(4.3) Let e be an idempotent of an $\mathcal{O}$-algebra A and let $\alpha \in \mathcal{P}(A)$.

(a) If α is not the image of a point of eAe (that is, $\alpha \cap eAe = \emptyset$), prove that $m_\alpha(e) = 0$.

(b) If α is the image of a point α' of eAe (that is, $\alpha' = \alpha \cap eAe = e\alpha e$), prove that $m_\alpha(e)$ is the multiplicity of α'.

(4.4) Let A be an $\mathcal{O}$-algebra and let B be a subalgebra of A such that $A = B + J(A)$. Prove that the inclusion map $B \to A$ induces a bijection $\mathcal{P}(B) \to \mathcal{P}(A)$. More precisely, prove that the image of a point $\beta \in \mathcal{P}(B)$ is the A^*-conjugacy closure of β. [Hint: Use Exercise 2.1.]

(4.5) Prove directly part (a) of Proposition 4.12. [Hint: Notice that we have $jAj = j(eAe)j$ and apply Corollary 4.6.]

(4.6) Let A be an $\mathcal{O}$-algebra, let n be a positive integer, and consider the homomorphism $f : A \to M_n(A)$ mapping a to the matrix having a as top left entry and zeros elsewhere. Prove that f induces a bijection $\mathcal{P}(A) \to \mathcal{P}(M_n(A))$. [Hint: Use Exercises 1.4 and 2.5.]

§ 5 PROJECTIVE MODULES

In this section, we review some basic properties of projective modules, projective covers and the Heller operator. Recall that throughout this book, all modules are assumed to be finitely generated and that $\mathcal{O}$ is a ring satisfying Assumption 2.1.

Let A be an $\mathcal{O}$-algebra. Recall that an A-module P is called *projective* if it is a direct summand of a free A-module, or equivalently, if for every surjective homomorphism $f : M \to N$, any homomorphism $g : P \to N$ lifts to a homomorphism $\widetilde{g} : P \to M$ such that $f\widetilde{g} = g$. In fact it is sufficient to assume this when $g = id$, that is, to require that any surjective homomorphism $f : M \to P$ splits.

Recall also that an A-module I is called *injective* if for every injective homomorphism $f : M \to N$, any homomorphism $g : M \to I$ extends to a homomorphism $\widetilde{g} : N \to I$ such that $\widetilde{g}f = g$. Again it is sufficient to assume this when $g = id$, that is, to require that any injective homomorphism $f : I \to N$ splits.

In the following proposition we review some of the main properties of projective A-modules. In particular we obtain that the set $\mathrm{Proj}(A)$ of isomorphism classes of indecomposable projective A-modules is in bijection with the set $\mathcal{P}(A)$, and also with the set $\mathrm{Irr}(A)$.

(5.1) PROPOSITION. *Let A be an $\mathcal{O}$-algebra.*

(a) Any projective A-module P decomposes as a finite direct sum of indecomposable projective A-modules. This decomposition is essentially unique in the sense that any other such decomposition of P is the image of the given one by an A-linear automorphism of P.

(b) A projective A-module is indecomposable if and only if it is isomorphic to Ae for some primitive idempotent e of A.

(c) Two indecomposable projective A-modules Ae and Af are isomorphic if and only if the primitive idempotents e and f are conjugate in A.

(d) The correspondence in (b) sets up a bijection between the sets $\mathrm{Proj}(A)$ and $\mathcal{P}(A)$.

(e) An indecomposable projective A-module Ae has a unique maximal submodule, namely $J(A)e$, hence a unique simple quotient $Ae/J(A)e$. Moreover $Ae \cong Af$ if and only if $Ae/J(A)e \cong Af/J(A)f$.

(f) The correspondence in (e) sets up a bijection between the sets $\mathrm{Proj}(A)$ and $\mathrm{Irr}(A)$.

Proof. (a) This is a direct application of the Krull–Schmidt theorem 4.4.

(b) By (a) it suffices to decompose a free A-module into indecomposable summands, and it suffices in turn to decompose the free module A of dimension one. The result now follows from Proposition 1.16.

(c) This is an application of Corollary 4.5, because $\mathrm{End}_A(A) \cong A^{\mathrm{op}}$, acting on A via right multiplication.

(d) This follows immediately from (b) and (c).

(e) For any maximal submodule M of Ae, we have $J(A)\cdot(Ae/M) = 0$ because $J(A)$ annihilates every simple A-module. Therefore $J(A)e \subseteq M$. But $Ae/J(A)e$ is simple by Theorem 4.3, so that $J(A)e$ is a maximal submodule. This proves the first claim. Now by Proposition 1.15, two simple A-modules $Ae/J(A)e$ and $Af/J(A)f$ are isomorphic if and only if $\overline{e}$ is conjugate to $\overline{f}$ in $A/J(A)$. By part (c) of Theorem 3.1, this holds if and only if e and f are conjugate in A, and the result follows by (c).

(f) This is immediate by (e). □

(5.2) COROLLARY. *Let A be an $\mathcal{O}$-algebra and let $\overline{A} = A/\mathfrak{p}A$. Then reduction modulo $\mathfrak{p}$ induces a bijection between the sets $\mathrm{Proj}(A)$ and $\mathrm{Proj}(\overline{A})$.*

Proof. This follows immediately from Proposition 5.1 and Theorem 3.1 on lifting idempotents, because $\mathfrak{p}A \subseteq J(A)$ (see also Exercise 5.3). □

For every point $\alpha \in \mathcal{P}(A)$, we write $V(\alpha)$ for a simple A-module corresponding to α (see Theorem 4.3), and $P(\alpha)$ for an indecomposable projective A-module corresponding to α. These are uniquely determined by α up to isomorphism. Explicitly $P(\alpha) \cong Ae$ and $V(\alpha) \cong Ae/J(A)e$ where $e \in \alpha$.

(5.3) COROLLARY. *Let A be an $\mathcal{O}$-algebra.*

(a) Let $\alpha \in \mathcal{P}(A)$. In a decomposition of A as direct sum of indecomposable projective A-modules, the number of occurences of modules isomorphic to $P(\alpha)$ is equal to $m_\alpha = \dim_k(V(\alpha))$.

(b) If A is free as an $\mathcal{O}$-module, then we have

$$\dim_{\mathcal{O}}(A) = \sum_{\alpha \in \mathcal{P}(A)} \dim_{\mathcal{O}}(P(\alpha)) \dim_k(V(\alpha)).$$

Proof. (a) By Proposition 1.16, a decomposition of A as in the statement corresponds to a primitive decomposition of 1_A. By Proposition 5.1, isomorphic summands correspond to conjugate idempotents. Therefore the number of occurrences of $P(\alpha)$ is equal to the multiplicity m_α of the point α, which is known to be equal to $\dim_k(V(\alpha))$ (Proposition 4.15).

(b) This follows immediately from (a). Note that $P(\alpha)$ is free as an $\mathcal{O}$-module because any direct summand of a free $\mathcal{O}$-module is free (Corollary 1.4). □

With our strong assumptions on $\mathcal{O}$, we also have the useful property that an arbitrary (finitely generated) A-module can be covered in a unique minimal fashion by a projective module. This is the notion of projective cover which we now define. First we define a *projective cap* of an A-module M to be a pair (P, f) where P is a projective A-module and $f : P \to M$ is a homomorphism of A-modules which is surjective. A projective cap of M is called a *projective cover* of M if the restriction of f to any proper submodule of P is not surjective. Instead of (P, f) we shall often abusively call P a projective cover of M. Before examining the question of the existence of projective covers, we first prove their minimality property and their uniqueness.

(5.4) PROPOSITION. *Let A be an $\mathcal{O}$-algebra and let (P, f) be a projective cover of an A-module M.*

(a) If $g : Q \to M$ is a projective cap of M, there exists a split surjective homomorphism $h : Q \to P$ such that $f h = g$. In other words g is isomorphic to the direct sum

$$(Q \xrightarrow{g} M) \cong (P \xrightarrow{f} M) \oplus (Q' \longrightarrow 0),$$

where $Q' = \mathrm{Ker}(h)$. In particular $\mathrm{Ker}(g) \cong \mathrm{Ker}(f) \oplus Q'$.

(b) If (P', f') is another projective cover of M, there exists an isomorphism $h : P' \to P$ such that $f h = f'$.

Proof. (a) Since Q is projective and f surjective, the map g lifts to a homomorphism $h : Q \to P$ such that $f\,h = g$. The image of h is a submodule of P, which maps surjectively onto M via f because $f(\mathrm{Im}(h)) = \mathrm{Im}(g) = M$. Therefore $\mathrm{Im}(h) = P$ by definition of a projective cover and so h is surjective. Since P is projective, there exists a homomorphism $s : P \to Q$ such that $h\,s = id$, that is, h is split.

(b) By part (a), there exists a surjective homomorphism $h : P' \to P$ which is split by a homomorphism $s : P \to P'$ and such that $f\,h = f'$. The image of s is a submodule of P', which maps surjectively onto M via f' because $f'\,s = f\,h\,s = f$. Therefore $\mathrm{Im}(s) = P'$ by definition of a projective cover and so s is surjective. It follows that h and s are mutual inverses. □

Note that since the homomorphism h constructed in the proposition is in general not unique, property (a) is not universal (but might be called "versal"). In our next result, we assume the existence of a projective cover of M, but we note that this is always satisfied, as we shall prove below.

(5.5) PROPOSITION. *Let A be an $\mathcal{O}$-algebra, let $f : Q \to M$ be a projective cap of an A-module M, and assume that a projective cover of M exists. The following conditions are equivalent.*

(a) (Q, f) is a projective cover of M.

(b) Every A-linear endomorphism $g : Q \to Q$ such that $f\,g = f$ is an isomorphism.

Proof. If (Q, f) is a projective cover of M and $g : Q \to Q$ satisfies $f\,g = f$, then $\mathrm{Im}(g)$ maps onto M via f, and therefore $\mathrm{Im}(g) = Q$. The result follows from the fact that any surjective endomorphism of a noetherian module is injective. Indeed the increasing sequence of submodules $\mathrm{Ker}(g^k)$ must stop, that is, $\mathrm{Ker}(g^n) = \mathrm{Ker}(g^{n+1})$ for some n, and if $g(x) = 0$, then $x = g^n(y)$ by surjectivity, and $g^{n+1}(y) = 0$ implies $g^n(y) = 0$, that is $x = 0$.

Conversely assume that (b) holds. Since a projective cover of M exists by assumption, we can apply Proposition 5.4. Thus there is a direct sum decomposition $(Q \xrightarrow{f} M) = (P \xrightarrow{f'} M) \oplus (Q' \to 0)$ where (P, f') is a projective cover of M (and f' is the restriction of f to the direct summand P). Since the idempotent projection $g : Q \to Q$ with image P satisfies $f\,g = f$, it must be an isomorphism, and so $P = Q$. □

Turning to the question of the existence of projective covers, we first mention that they do not exist for arbitrary rings (Exercise 5.1). Recall that the *radical* $J(M)$ of an A-module M is the intersection of all maximal submodules of M.

(5.6) LEMMA. *Let A be an $\mathcal{O}$-algebra and let M be an A-module. Suppose that (P, f) is a projective cover of $M/J(M)$. Then f lifts to a homomorphism $\widetilde{f} : P \to M$ and $(P, \widetilde{f})$ is a projective cover of M.*

Proof. Since the canonical map $q : M \to M/J(M)$ is surjective, the surjection $f : P \to M/J(M)$ lifts to a homomorphism $\widetilde{f} : P \to M$ such that $q\widetilde{f} = f$. Let N be any proper submodule of M. Then N is contained in some maximal submodule of M (because M is noetherian) and so $q(N) \neq M/J(M)$. Applying this argument with $N = \mathrm{Im}(\widetilde{f})$ and noting that $\mathrm{Im}(\widetilde{f})$ maps surjectively onto $M/J(M)$ (because f is surjective), we deduce that $\mathrm{Im}(\widetilde{f}) = M$, proving the surjectivity of $\widetilde{f}$. If now Q is a proper submodule of P, then we know that $f(Q) \neq M/J(M)$, and it follows immediately that $\widetilde{f}(Q) \neq M$. Thus $(P, \widetilde{f})$ is a projective cover of M. □

It follows from the lemma that it suffices to prove the existence of projective covers for a module M such that $J(M) = 0$. Our assumptions on $\mathcal{O}$ imply that such a module is semi-simple.

(5.7) LEMMA. *Let A be an $\mathcal{O}$-algebra and let M be an A-module.*
(a) $J(M) = J(A)\cdot M$.
(b) $M/J(M)$ *is semi-simple.*

Proof. We have $J(A)\cdot(M/N) = 0$ for every maximal submodule N of M, because $J(A)$ annihilates every simple A-module. It follows that $J(A)\cdot M \subseteq N$ and therefore $J(A)\cdot M \subseteq J(M)$.

The module $M/J(A)\cdot M$ is a module over the ring $A/J(A)$, which is a semi-simple k-algebra (Theorem 2.7). It follows that $M/J(A)\cdot M$ is a semi-simple module (Theorem 1.10). In particular $J(M/J(A)\cdot M) = 0$, so that $J(M) \subseteq J(A)\cdot M$. Therefore $J(M) = J(A)\cdot M$ and it follows that $M/J(M)$ is semi-simple. □

Since we are dealing with finitely generated modules, a semi-simple module is a *finite* direct sum of simple modules. Our next lemma deals with direct sums.

(5.8) LEMMA. *Let A be an $\mathcal{O}$-algebra, let $M_1, \ldots, M_n$ be A-modules, and let (P_i, f_i) be a projective cover of M_i. Then $(\bigoplus_{i=1}^{n} P_i, \bigoplus_{i=1}^{n} f_i)$ is a projective cover of $\bigoplus_{i=1}^{n} M_i$.*

Proof. This is an easy exercise which is left to the reader. □

We are left with the case of a simple A-module.

(5.9) LEMMA. *Let A be an $\mathcal{O}$-algebra and let V be a simple A-module. There exists a primitive idempotent e of A such that $V \cong Ae/J(A)e$. Moreover the canonical surjection $Ae \to Ae/J(A)e$ is a projective cover of $Ae/J(A)e$.*

Proof. The first assertion follows from Theorem 4.3. Moreover by Proposition 5.1, $J(A)e$ is the unique maximal submodule of the projective module Ae and therefore the surjection $Ae \to Ae/J(A)e$ must be a projective cover. □

Combining all the preceding lemmas, we obtain the existence of projective covers.

(5.10) THEOREM. *Let A be an $\mathcal{O}$-algebra and let M be an A-module. Then a projective cover of M exists and is unique up to isomorphism.*

The *Heller operator* Ω is a map from the set of isomorphism classes of A-modules to itself, defined as follows. Let M be an A-module and choose a projective cover (P, f) of M. Then $\Omega M = \mathrm{Ker}(f)$ is an A-module which is uniquely defined up to isomorphism, because (P, f) is unique up to isomorphism by Proposition 5.4. We also say that ΩM is the *Heller translate* of M. Thus there is an exact sequence

$$0 \longrightarrow \Omega M \longrightarrow P \stackrel{f}{\longrightarrow} M \longrightarrow 0\,.$$

Clearly $\Omega P = 0$ if and only if P is projective (because (P, id) is a projective cover of a projective module P). Lemma 5.8 implies that $\Omega(\bigoplus_i M_i) \cong \bigoplus_i \Omega M_i$. Moreover if $g : Q \to M$ is an arbitrary projective cap of M, then by Proposition 5.4, $\mathrm{Ker}(g) \cong \Omega M \oplus Q'$ for some projective A-module Q'.

The module of all homomorphisms from an indecomposable projective A-module Ae to another module can be described in the following way. Recall that the *opposite* algebra A^{op} of an $\mathcal{O}$-algebra A is the same $\mathcal{O}$-module A, but endowed with the product $*$ defined by $a * b = ba$.

(5.11) PROPOSITION. *Let A be an $\mathcal{O}$-algebra, let e be an idempotent of A, and let M be an A-module.*

(a) $\mathrm{Hom}_A(Ae, M) \cong eM$ *as $\mathcal{O}$-modules, via evaluation at e.*

(b) In particular if f is an idempotent in A, then $\mathrm{Hom}_A(Ae, Af) \cong eAf$ *and the inverse isomorphism maps $a \in eAf$ to the right multiplication by a.*

(c) $\mathrm{End}_A(Ae)^{op} \cong eAe$ *as $\mathcal{O}$-algebras.*

Proof. (a) Let $\phi : \mathrm{Hom}_A(Ae, M) \to eM$ given by $\phi(h) = h(e)$. It is clear that ϕ is an $\mathcal{O}$-linear map. Given an element $m \in eM$, one defines $h : Ae \to M$ by $h(a) = am$, and this provides the inverse of ϕ, using the fact that $h(a) = h(ae) = ah(e)$. Now (b) follows immediately.

(c) Let $\phi : \mathrm{End}_A(Ae) \xrightarrow{\sim} eAe$ be the isomorphism of part (b). If $g, h \in \mathrm{End}_A(Ae)$, then

$$\phi(gh) = gh(e) = g(h(e)e) = h(e)g(e) = \phi(h)\phi(g)\,.$$

Therefore ϕ is an isomorphism of algebras, provided one of the algebras is considered with the opposite multiplication. □

We now consider the special case of an algebra over the field k. By our convention 2.4, every A-module M is a finite dimensional k-vector space. In particular M has a *composition series*, that is, a sequence of submodules

$$0 = M_0 \subset M_1 \subset \ldots \subset M_n = M$$

such that each successive quotient M_i/M_{i-1} is a simple A-module. Every such quotient is called a *composition factor* of M. By the Jordan–Hölder theorem, the set of isomorphism classes of composition factors of M is independent of the choice of a composition series (but of course the simple factors may appear in another order). In particular the number of composition factors of M isomorphic to some given simple A-module V is independent of the composition series and is called the *multiplicity of V as a composition factor* of M.

Since both $\mathrm{Irr}(A)$ and $\mathrm{Proj}(A)$ are in bijection with $\mathcal{P}(A)$, with each point α are associated an indecomposable projective A-module $P(\alpha)$ and a simple A-module $V(\alpha)$, which are uniquely determined up to isomorphism. Explicitly $P(\alpha) \cong Ae$ and $V(\alpha) \cong Ae/J(A)e$ if $e \in \alpha$. We define the *Cartan integer* $c_{\alpha,\beta}$ to be the multiplicity of $V(\alpha)$ as a composition factor of $P(\beta)$. Thus $(c_{\alpha,\beta})$ is a square matrix indexed by the points, called the *Cartan matrix* of A. It has a very natural interpretation as the matrix of a linear map between two Grothendieck groups (see Serre [1971] or Curtis–Reiner [1981] for details).

As an example, we mention that the Cartan matrix of the group algebra kG of a finite group G is symmetric (see Exercise 6.5 of the next section). Moreover it is non-singular, with determinant a power of p. We shall return in Section 42 to this basic result of modular representation theory.

We now give another characterization of the Cartan integers in terms of homomorphisms.

(5.12) PROPOSITION. *Let A be a k-algebra, let $\alpha, \beta \in \mathcal{P}(A)$, and let $e \in \alpha$, $f \in \beta$. Then*

$$c_{\alpha,\beta} = \dim(\mathrm{Hom}_A(P(\alpha), P(\beta))) = \dim(eAf)\,.$$

Proof. Since $P(\alpha) \cong Ae$ and $P(\beta) \cong Af$, the second equality is an immediate consequence of the isomorphism $\mathrm{Hom}_A(Ae, Af) \cong eAf$ of Proposition 5.11. If N is a submodule of an A-module M, then since $P(\alpha)$ is projective, the sequence

$$0 \longrightarrow \mathrm{Hom}_A(P(\alpha), N) \longrightarrow \mathrm{Hom}_A(P(\alpha), M) \longrightarrow \mathrm{Hom}_A(P(\alpha), M/N) \longrightarrow 0$$

is exact. Therefore we have

$$\dim(\mathrm{Hom}_A(P(\alpha), N)) + \dim(\mathrm{Hom}_A(P(\alpha), M/N)) = \dim(\mathrm{Hom}_A(P(\alpha), M))$$

and if $0 = M_0 \subset M_1 \subset \ldots \subset M_n = P(\beta)$ is a composition series of $P(\beta)$, it follows by induction on the length that

$$\dim(\mathrm{Hom}_A(P(\alpha), P(\beta))) = \sum_{i=1}^{n} \dim(\mathrm{Hom}_A(P(\alpha), M_i/M_{i-1}))\,.$$

Since $P(\alpha)$ has a unique maximal submodule $J(P(\alpha))$, with simple quotient $V(\alpha) = P(\alpha)/J(P(\alpha))$, any homomorphism $P(\alpha) \to M_i/M_{i-1}$ factorizes through $V(\alpha)$ because M_i/M_{i-1} is simple. Therefore

$$\mathrm{Hom}_A(P(\alpha), M_i/M_{i-1}) \cong \mathrm{Hom}_A(V(\alpha), M_i/M_{i-1})$$

and by Schur's lemma 1.8 we have

$$\dim(\mathrm{Hom}_A(P(\alpha), M_i/M_{i-1})) = \begin{cases} 1 & \text{if } V(\alpha) \cong M_i/M_{i-1}, \\ 0 & \text{if } V(\alpha) \not\cong M_i/M_{i-1}. \end{cases}$$

This proves that $\dim(\mathrm{Hom}_A(P(\alpha), P(\beta)))$ is the multiplicity of $V(\alpha)$ as a composition factor of $P(\beta)$, which is $c_{\alpha,\beta}$ by definition. □

A very useful way of decomposing a k-algebra A as a direct product is provided by the following result. It says essentially that if the Cartan matrix of A can be decomposed into diagonal blocks (with off-diagonal blocks zero), then A decomposes accordingly as a direct product.

(5.13) PROPOSITION. *Let A be a k-algebra. Assume that there exists a disjoint union decomposition $\mathcal{P}(A) = \mathcal{P}_1 \cup \mathcal{P}_2$ such that $c_{\alpha,\beta} = 0$ and $c_{\beta,\alpha} = 0$ for all $\alpha \in \mathcal{P}_1$ and $\beta \in \mathcal{P}_2$. Let I be a primitive decomposition of 1_A and, for $r = 1, 2$, let e_r be the sum of all idempotents in I belonging to points in $\mathcal{P}_r$, so that $1_A = e_1 + e_2$.*

(a) e_1 and e_2 are central idempotents. In particular Ae_r is a k-algebra with unity element e_r.

(b) $A \cong Ae_1 \times Ae_2$.

(c) The surjection $A \to Ae_r$ induces a bijection $\mathcal{P}_r \cong \mathcal{P}(Ae_r)$.

Proof. (a) By Proposition 5.12, the assumption implies that $iAj = 0$ and $jAi = 0$ if i belongs to a point in $\mathcal{P}_1$ and j belongs to a point in $\mathcal{P}_2$. Therefore $e_1Ae_2 = 0$ and $e_2Ae_1 = 0$. It follows that if $a \in A$, we have

$$a = (e_1 + e_2)a(e_1 + e_2) = e_1ae_1 + e_2ae_2 ,$$

so that $e_1a = e_1ae_1 = ae_1$, and similarly $e_2a = ae_2$.

(b) Every $a \in A$ can be written uniquely $a = a_1 + a_2$ with $a_r \in Ae_r$. Indeed the existence follows from the decomposition $a = ae_1 + ae_2$, and we have uniqueness because $a_r = ae_r$ (after right multiplication by e_r). Moreover $a_1a_2 = a_1e_1a_2e_2 = a_1a_2e_1e_2 = 0$, and similarly $a_2a_1 = 0$ (where $a_r \in Ae_r$). Therefore we obtain an isomorphism $Ae_1 \times Ae_2 \to A$ mapping (a_1, a_2) to $a_1 + a_2$.

(c) If $i \in I$ belongs to a point $\alpha \in \mathcal{P}_1$, then $ie_1 = i$ and $ie_2 = 0$. Thus $\alpha \in \mathcal{P}_1$ if and only if $\alpha \not\subseteq Ae_2 = \mathrm{Ker}(A \to Ae_1)$. By Theorem 3.2, this implies that the surjection $A \to Ae_1$ induces a bijection $\mathcal{P}_1 \cong \mathcal{P}(Ae_1)$. □

An important special case is the following.

(5.14) COROLLARY. *Let A be a k-algebra and assume that there exists a simple A-module V which is projective and injective.*

(a) $A \cong \mathrm{End}_k(V) \times A'$ for some k-algebra A'.

(b) If A has no non-trivial central idempotent, then $A \cong \mathrm{End}_k(V)$ and A is a simple k-algebra.

Proof. (a) We have $V = V(\alpha)$ for some point $\alpha \in \mathcal{P}(A)$. Since $V(\alpha)$ is projective, it coincides with its projective cover $P(\alpha)$. Therefore $V(\alpha)$ is the only composition factor of $P(\alpha)$ and so $c_{\beta,\alpha} = 0$ for every point $\beta \neq \alpha$. If now $c_{\alpha,\beta} \neq 0$ for some point β , then there exists a non-zero homomorphism $f : V(\alpha) = P(\alpha) \to P(\beta)$ by Proposition 5.12. As $V(\alpha)$ is simple, the submodule $\mathrm{Ker}(f)$ is zero, so that f is injective. Since $V(\alpha)$ is an injective A-module, f splits and therefore $V(\alpha)$ is isomorphic to a direct summand of $P(\beta)$. But as $P(\beta)$ is indecomposable, it follows that $V(\alpha) \cong P(\beta)$, forcing $\alpha = \beta$. This proves that $c_{\alpha,\beta} = 0$ for every point $\beta \neq \alpha$. Thus the assumptions of Proposition 5.13 are satisfied with $\mathcal{P}_1 = \{\alpha\}$ and $\mathcal{P}_2 = \mathcal{P}(A) - \{\alpha\}$.

By Proposition 5.13, $A \cong Ae_1 \times Ae_2$ where e_r is defined as in the proposition. Moreover Ae_1 is a k-algebra with a single point α , and the unique simple Ae_1-module $V(\alpha)$ is projective. This forces the semi-simplicity of all Ae_1-modules, so that Ae_1 is a semi-simple k-algebra, hence a simple algebra since there is a single point. Therefore we have $Ae_1 \cong \mathrm{End}_k(V(\alpha))$, as required.

(b) This follows immediately from (a). □

Exercises

(5.1) Let p be a prime number. Prove that $\mathbb{Z}/p\mathbb{Z}$ does not have a projective cover as a $\mathbb{Z}$-module. Prove that $J(\mathbb{Z}) = 0$ but that $\mathbb{Z}$ is not semi-simple as a $\mathbb{Z}$-module.

(5.2) Prove Lemma 5.8.

(5.3) Let A be an $\mathcal{O}$-algebra and let $\overline{A} = A/\mathfrak{p}A \cong k \otimes_{\mathcal{O}} A$. For any indecomposable projective A-module P , show that $\overline{P} = P/\mathfrak{p}P$ is an indecomposable projective $\overline{A}$-module, and that P is the projective cover of $\overline{P}$ as an A-module. Prove that this provides a bijection between $\mathrm{Proj}(A)$ and $\mathrm{Proj}(\overline{A})$ such that the following two diagrams of bijections commute (where the bijections are defined by Proposition 5.1).

$$\begin{array}{ccccc}
\mathcal{P}(A) & \xrightarrow{\sim} & \mathrm{Proj}(A) & \xrightarrow{\sim} & \mathrm{Irr}(A) \\
\downarrow\wr & & \downarrow\wr & & \downarrow\wr \\
\mathcal{P}(\overline{A}) & \xrightarrow{\sim} & \mathrm{Proj}(\overline{A}) & \xrightarrow{\sim} & \mathrm{Irr}(\overline{A})
\end{array}$$

(5.4) Let $A = k[X]/(X^m)$. Prove that the modules $k[X]/(X^r)$ (for $1 \leq r \leq m$) form a complete list of indecomposable A-modules. Show that the Heller operator is periodic on non-projective indecomposable modules, by showing that its square Ω^2 is the identity.

§ 6 SYMMETRIC ALGEBRAS

In this section we examine the special case of symmetric algebras where more information on projective modules, projective covers and the Heller operator is available. As usual $\mathcal{O}$ denotes a ring satisfying Assumption 2.1.

Let A be an $\mathcal{O}$-algebra and let M be an A-module. We define the *dual* of M to be the right A-module $M^* = \mathrm{Hom}_{\mathcal{O}}(M, \mathcal{O})$. The right A-module structure on M^* is given by $(fa)(m) = f(am)$, for $a \in A$, $f \in M^*$, and $m \in M$. Similarly if M is a right A-module, then M^* is a left A-module via $(af)(m) = f(ma)$. If M is free as an $\mathcal{O}$-module, then so is M^* , but without any assumption on M or $\mathcal{O}$ it may happen that $M^* = 0$ (for instance if $\mathcal{O}$ is a discrete valuation ring and M is a torsion module).

Let M and N be two $\mathcal{O}$-modules and let $\phi : M \times N \to \mathcal{O}$ be an $\mathcal{O}$-bilinear form. The form ϕ corresponds to an $\mathcal{O}$-linear map $\theta : M \to N^*$ defined by $\theta(x)(y) = \phi(x, y)$ for all $x \in M$ and $y \in N$, and similarly to a map $\theta' : N \to M^*$ defined by $\theta'(y)(x) = \phi(x, y)$. The $\mathcal{O}$-bilinear form ϕ is called *non-degenerate* if the corresponding linear maps θ and θ' are injective, and ϕ is called *unimodular* if θ and θ' are isomorphisms. When $\mathcal{O} = k$ is a field, then both notions coincide, because the injectivity of θ and θ' forces the vector spaces M and N to have the same dimension and an injective linear map between two vector spaces of the same dimension is necessarily an isomorphism. However, this is not the case when $\mathcal{O}$ is a complete discrete valuation ring, and the distinction between the two notions will turn out to be quite important.

We shall often work with the case where M and N are equal. A bilinear form $\phi : M \times M \to \mathcal{O}$ is called *symmetric* if $\phi(x, y) = \phi(y, x)$ for all $x, y \in M$. In that case the corresponding maps θ and θ' coincide, so that the non-degeneracy or unimodularity of ϕ is a condition on the single map θ .

If now M is a right A-module and N is a left A-module, then $\theta : M \to N^*$ is an $\mathcal{O}$-linear map between two right A-modules. The requirement that θ be A-linear is equivalent to the condition that $\phi(xa, y) = \phi(x, ay)$ for all $x \in M$, $y \in N$, and $a \in A$. Applying all this to A , we let

A_ℓ (respectively A_r) denote A with its left (respectively right) A-module structure.

(6.1) PROPOSITION. *Let A be an $\mathcal{O}$-algebra. The following three conditions are equivalent.*

(a) There exists an isomorphism of right A-modules $\theta : A_r \to A_\ell^*$ which is symmetric (that is, $\theta(a)(b) = \theta(b)(a)$ for all $a, b \in A$).

(b) There exists a unimodular symmetric $\mathcal{O}$-bilinear form $\phi : A \times A \to \mathcal{O}$ which is associative (that is, $\phi(ab, c) = \phi(a, bc)$ for all $a, b, c \in A$).

(c) There exists an $\mathcal{O}$-linear map $\lambda : A \to \mathcal{O}$ with the following three properties:

(i) λ is symmetric (that is, $\lambda(ab) = \lambda(ba)$ for all $a, b \in A$).

(ii) $\mathrm{Ker}(\lambda)$ does not contain any non-zero right ideal of A .

(iii) For any $\mathcal{O}$-linear map $f : A \to \mathcal{O}$, there exists $a \in A$ such that $f(b) = \lambda(ab)$ for all $b \in A$.

Proof. The connection between θ and ϕ is given by the formula $\theta(a)(b) = \phi(a, b)$. The fact that θ is A-linear corresponds to the requirement that ϕ be associative. The equivalence between (a) and (b) follows.

The connection between ϕ and λ is given by the formula $\phi(a, b) = \lambda(ab)$. The associativity of ϕ corresponds to the associativity of the multiplication in A . Moreover if $\theta : A_r \to A_\ell^*$ is the map corresponding to ϕ , then θ is injective if and only if $\mathrm{Ker}(\lambda)$ does not contain any non-zero right ideal of the form aA , that is, if and only if $\mathrm{Ker}(\lambda)$ does not contain any non-zero right ideal of A . Finally θ is surjective if and only if any linear map $f : A \to \mathcal{O}$ has the form $f(b) = \lambda(ab)$ for some a . □

An $\mathcal{O}$-algebra A satisfying the equivalent conditions of the proposition is called a *symmetric algebra* and any linear form $\lambda : A \to \mathcal{O}$ satisfying condition (c) is called a *symmetrizing form* for A . Instead of calling λ symmetric, one often says that λ is *central* if $\lambda(ab) = \lambda(ba)$ for all $a, b \in A$.

Note that condition (ii) on $\mathrm{Ker}(\lambda)$ guarantees the non-degeneracy of ϕ , while the additional condition (iii) guarantees the unimodularity of ϕ . Thus over a field k , (iii) is a consequence of (ii). Note also that (iii) implies (ii) if A is free as an $\mathcal{O}$-module. Indeed the dual A^* is then also free of the same dimension and the surjectivity of θ implies its injectivity (because A is noetherian).

By the symmetry condition, one can also view θ as an isomorphism of left A-modules $A_\ell \to A_r^*$. For the same reason, one can require equivalently that $\mathrm{Ker}(\lambda)$ does not contain any non-zero left ideal of A , and also that ϕ satisfies $\phi(ab, c) = \phi(b, ca)$ for all $a, b, c \in A$.

Let A be a symmetric algebra and let λ be a symmetrizing form for A. If I is an ideal of A, we define the *orthogonal* $I^\perp$ of I to be

$$I^\perp = \{ a \in A \mid \lambda(ab) = 0 \text{ for all } b \in I \}.$$

The map $I \mapsto I^\perp$ is order reversing, and we have $I \subseteq I^{\perp\perp}$. Equality holds over a field but fails to hold in general (Exercise 6.1). A basic property of symmetric algebras is that the (left or right) annihilator of an ideal I coincides with $I^\perp$. The proof of this is left to the reader (see Exercise 6.2).

(6.2) EXAMPLE. The group algebra $\mathcal{O}G$ of a finite group G is a symmetric algebra. A symmetrizing form for $\mathcal{O}G$ is the form $\lambda : \mathcal{O}G \to \mathcal{O}$ mapping a basis element g to zero if $g \neq 1$ and to 1 if $g = 1$. The symmetry condition follows from a straightforward computation. By considering the dual basis $\{ g^{-1} \mid g \in G \}$, it is easy to check the unimodularity condition.

(6.3) EXAMPLE. The matrix algebra $A = M_n(\mathcal{O})$ is a symmetric algebra. Indeed the trace map $\mathrm{tr} : M_n(\mathcal{O}) \to \mathcal{O}$ is a symmetrizing form, because it satisfies $\mathrm{tr}(ab) = \mathrm{tr}(ba)$ and the canonical basis (e_{ij}) has a dual basis, namely (e_{ji}). More generally any finite direct product of matrix algebras is a symmetric algebra, using the sum of the trace maps of the factors.

If A is a symmetric algebra and $e \in A$ is an idempotent, it is often useful to know that eAe is again a symmetric algebra. We now prove a slightly more general result.

(6.4) PROPOSITION. *Let A be a symmetric $\mathcal{O}$-algebra and let λ be a symmetrizing form for A. If e and f are idempotents of A, then λ induces by restriction a unimodular bilinear form*

$$eAf \times fAe \longrightarrow \mathcal{O}.$$

In particular eAe is a symmetric algebra.

Proof. Let $a \in eAf$ and suppose that $\lambda(ab) = 0$ for every $b \in fAe$. Since $a = eaf$, we have for every $c \in A$

$$\lambda(ac) = \lambda(eafc) = \lambda(a(fce)) = 0.$$

Therefore $a = 0$ by non-degeneracy of λ. Suppose now that $h : fAe \to \mathcal{O}$ is a linear form. Then h extends to a linear form $h : A \to \mathcal{O}$ by setting $h(x) = h(fxe)$. By unimodularity of λ, there exists $a \in A$ such that $h(c) = \lambda(ac)$ for all $c \in A$. Then for every $b \in fAe$, we have $b = fbe$ and therefore

$$\lambda((eaf)b) = \lambda(afbe) = \lambda(ab) = h(b).$$

This proves that the linear form h is the image of eaf under the map $eAf \to (fAe)^*$, proving unimodularity. The special case follows by taking $e = f$. □

We shall see in Section 33 a natural example of a symmetric algebra which is not free as an $\mathcal{O}$-module. However, the notion of symmetric algebra is particularly useful when the algebra is free as an $\mathcal{O}$-module and we make this assumption for the rest of this section. Over an $\mathcal{O}$-algebra A which is free as an $\mathcal{O}$-module, it is natural to consider the category of A-lattices. An *A-lattice* is an A-module which is free as an $\mathcal{O}$-module (and finitely generated, as usual). Any direct summand of an A-lattice is again an A-lattice, because a direct summand of a free $\mathcal{O}$-module is again free (Corollary 1.4). In particular, since a free A-module is free over $\mathcal{O}$, all projective A-modules are A-lattices, and we shall call them projective A-lattices in the sequel. Clearly the dual M^* of a (left) A-lattice M is a (right) A-lattice. Moreover the evaluation map $M^{**} \cong M$ is an isomorphism of (left) A-lattices. We are going to use this for the dualization of the notions of the previous section. This would not be possible for arbitrary A-modules since for instance the dual of an A-module may be zero.

An A-lattice I is called *injective relative to* $\mathcal{O}$, or simply *$\mathcal{O}$-injective*, if the following condition holds: for any given injective homomorphism of A-modules $f : N \to M$ and any homomorphism $g : N \to I$ having an $\mathcal{O}$-linear extension $h : M \to I$ (that is, $hf = g$), there exists an A-linear extension $\widetilde{h} : M \to I$ (that is, $\widetilde{h}f = g$). Taking in particular $g = id_I$, one obtains that any injective homomorphism $f : I \to M$ having an $\mathcal{O}$-linear retraction $h : M \to I$ has an A-linear retraction $\widetilde{h} : M \to I$. In other words, if we let $M' = \text{Coker}(f)$, then the short exact sequence of A-modules $0 \to I \to M \to M' \to 0$ splits provided it splits as a sequence of $\mathcal{O}$-modules. Taking now M to be an A-lattice, the splitting of the sequence over $\mathcal{O}$ is equivalent to the condition that M' be again a lattice (because on the one hand a direct summand of a free $\mathcal{O}$-module is a free $\mathcal{O}$-module and on the other hand a short exact sequence of A-lattices necessarily splits over $\mathcal{O}$). Thus we obtain in particular that if I is $\mathcal{O}$-injective, then every short exact sequence of A-lattices $0 \to I \to M \to M' \to 0$ splits. It can be shown that this condition is in fact equivalent to the $\mathcal{O}$-injectivity of I, but we shall not need this.

An $\mathcal{O}$-injective A-lattice is not necessarily an injective A-module because, in the definition, an $\mathcal{O}$-linear extension may not exist. For instance if $\mathcal{O}$ is a domain with $\mathfrak{p} \neq 0$, then for any A-lattice M, the endomorphism of M equal to the multiplication by an element $\lambda \in \mathfrak{p}$ is injective but has no retraction. However, if $\mathcal{O} = k$ is a field (in which case the notion of lattice coincides with that of module), then a k-injective A-module is an injective A-module, because any k-linear map can always be extended to a larger k-vector space (alternatively any injective map of k-vector spaces always has a k-linear retraction).

Similarly an A-lattice P is called *$\mathcal{O}$-projective* if the following condition holds: given a surjective homomorphism $f : M \to N$ of A-modules and a homomorphism $g : P \to N$ which has an $\mathcal{O}$-linear lift $h : P \to M$ (that is, $f\,h = g$), then there exists an A-linear lift $\widetilde{h} : P \to M$ (that is, $\widetilde{f}\,h = g$). Taking in particular $g = id_P$ and M to be an A-lattice, we obtain in particular that if P is $\mathcal{O}$-projective, then every short exact sequence of A-lattices terminating in P splits. But we now show that the notion of $\mathcal{O}$-projectivity is in fact equivalent to projectivity.

(6.5) LEMMA. *Let A be an $\mathcal{O}$-algebra which is free as an $\mathcal{O}$-module and let P be a (left) A-lattice. The following conditions are equivalent.*
(a) P is a projective left A-lattice.
(b) P is an $\mathcal{O}$-projective left A-lattice.
(c) The dual P^* is an $\mathcal{O}$-injective right A-lattice.

Proof. The equivalence between (b) and (c) follows immediately from the definitions and duality. It is clear that (a) implies (b). Finally, to show that (b) implies (a), assume that P is an $\mathcal{O}$-projective A-lattice and let $f : Q \to P$ be a projective cap of P. Since P is free over $\mathcal{O}$, the surjection $f : Q \to P$ splits over $\mathcal{O}$, hence over A by $\mathcal{O}$-projectivity. Therefore P is isomorphic to a direct summand of Q, so is projective. □

In order to define the notion of $\mathcal{O}$-injective hull, we dualize the characterization of projective covers given in Proposition 5.5. An *$\mathcal{O}$-injective hull* of an A-lattice M is a pair (I, f), where I is an $\mathcal{O}$-injective A-lattice and $f : M \to I$ is an injective homomorphism of A-modules, such that f has an $\mathcal{O}$-linear retraction and any endomorphism $g : I \to I$ with $g\,f = f$ is an isomorphism. Instead of (I, f) we shall often abusively call I an $\mathcal{O}$-injective hull of M. We emphasize that an $\mathcal{O}$-injective hull of a lattice is in general not its injective hull as a module (unless $\mathcal{O} = k$ is a field). We also define the Heller operator Ω^{-1} by setting $\Omega^{-1}(M) = \mathrm{Coker}(f)$ where (I, f) is an $\mathcal{O}$-injective hull of M. Since f has an $\mathcal{O}$-linear retraction by definition, the exact sequence

$$0 \longrightarrow M \xrightarrow{\ f\ } I \longrightarrow \Omega^{-1}(M) \longrightarrow 0$$

splits over $\mathcal{O}$ and therefore $\Omega^{-1}(M)$ is again an A-lattice. The properties of $\mathcal{O}$-injective hulls are similar to those of projective covers. In particular we show that they exist.

(6.6) PROPOSITION. *Let A be an $\mathcal{O}$-algebra which is free as an $\mathcal{O}$-module and let M be an A-lattice. Then an $\mathcal{O}$-injective hull of M exists and is unique up to isomorphism.*

Proof. Let (P, f) be a projective cover of the right A-lattice M^*, which exists by Proposition 5.10. Since M^* is free over $\mathcal{O}$, there exists an $\mathcal{O}$-linear section $s : M^* \to P$ of f. Then clearly (P^*, f^*) is an $\mathcal{O}$-injective hull of $M^{**} \cong M$ with $\mathcal{O}$-linear retraction s^*. The proof of uniqueness is left to the reader. □

Let A be an $\mathcal{O}$-algebra which is free as an $\mathcal{O}$-module. Then A is called *self-injective* if the left A-module A_ℓ is an $\mathcal{O}$-injective A-lattice. If A is symmetric, then it is self-injective since, by Proposition 6.1, A_ℓ is isomorphic to the dual of a free right lattice and is therefore $\mathcal{O}$-injective by Lemma 6.5. For self-injective algebras, we have the following result.

(6.7) PROPOSITION. *Let A be a self-injective $\mathcal{O}$-algebra (free as an $\mathcal{O}$-module).*

(a) An A-lattice is projective if and only if it is $\mathcal{O}$-injective.

(b) If M is an A-lattice with no non-zero projective direct summand, then we have $\Omega\Omega^{-1}M \cong M$ and $\Omega^{-1}\Omega M \cong M$.

(c) If M is an indecomposable non-projective A-lattice, then ΩM and $\Omega^{-1}M$ are indecomposable non-projective A-lattices.

Proof. (a) Since A_ℓ is $\mathcal{O}$-injective, so is any direct summand of a free A-lattice. Thus a projective A-lattice is $\mathcal{O}$-injective. In particular $\mathrm{Proj}(A) \subseteq \mathrm{Inj}(A)$, where $\mathrm{Inj}(A)$ denotes the set of isomorphism classes of indecomposable $\mathcal{O}$-injective (left) A-lattices. By the duality of Lemma 6.5, $\mathrm{Inj}(A)$ is in bijection with the set $\mathrm{Proj}_r(A)$ of isomorphism classes of indecomposable projective right A-lattices. By Proposition 5.1 both sets $\mathrm{Proj}(A)$ and $\mathrm{Proj}_r(A)$ are in bijection with $\mathcal{P}(A)$ (which is intrinsically defined without any one-sided condition). Since all these sets are finite, it follows that $\mathrm{Proj}(A) = \mathrm{Inj}(A)$, and consequently any $\mathcal{O}$-injective A-lattice is projective.

(b) Since Ω and Ω^{-1} are additive, we can assume that M is indecomposable non-projective. Let $j : M \to P$ be an $\mathcal{O}$-injective hull of M , with cokernel $\Omega^{-1}M$. Since P is a projective A-lattice by (a), one can apply Proposition 5.4 to the surjective map $f : P \to \Omega^{-1}M$. Thus P is the direct sum of a projective cover of $\Omega^{-1}M$ and some projective A-lattice Q , and we have $f(Q) = 0$. Therefore $M = \mathrm{Ker}(f)$ is the direct sum of $\Omega\Omega^{-1}M$ and Q . Since M is indecomposable non-projective, we must have $Q = 0$ and $M = \Omega\Omega^{-1}M$. Dualizing the whole argument, we obtain $M = \Omega^{-1}\Omega M$.

(c) Let M be an indecomposable non-projective A-lattice and let $f : P \to M$ be a projective cover of M . If Q is an $\mathcal{O}$-injective direct summand of ΩM , then the projection $\Omega M \to Q$ extends to a homomorphism $g : P \to Q$, which is the identity on Q . Thus $P = Q \oplus \mathrm{Ker}(g)$ and since $Q \subseteq \mathrm{Ker}(f)$, we have $f(\mathrm{Ker}(g)) = M$ and hence $\mathrm{Ker}(g) = P$ by definition of a projective cover. Therefore $Q = 0$ and ΩM has no non-zero $\mathcal{O}$-injective direct summand. If $\Omega M = N \oplus N'$, then by (b) $M = \Omega^{-1}\Omega M = \Omega^{-1}N \oplus \Omega^{-1}N'$ and by indecomposability of M it follows that $\Omega^{-1}N = M$ and $\Omega^{-1}N' = 0$ (or vice versa). This implies that $N' = 0$ because the Heller operator Ω^{-1} is non-zero on a non-zero non- $\mathcal{O}$-injective A-lattice. This shows that ΩM is indecomposable, and non- $\mathcal{O}$-injective, that is, non-projective by (a). The dual of this argument implies similarly that $\Omega^{-1}M$ is indecomposable non-projective. □

Returning to the special case of symmetric algebras, we show some of their most important properties, which hold over a field k . We need the notion of socle. For any k-algebra A , the *socle* $\mathrm{Soc}(M)$ of an A-module M is the sum of all simple submodules of M . In other words $\mathrm{Soc}(M)$ is the largest semi-simple submodule of M . Since a module is semi-simple precisely when it is annihilated by $J(A)$, the socle is the largest submodule of M annihilated by $J(A)$. Applying this to the left A-module A_ℓ , we have the *left socle* $\mathrm{Soc}(A_\ell)$, which is easily seen to be a two-sided ideal of A . Similarly $\mathrm{Soc}(A_r)$ is the *right socle* of A . In case A is symmetric, then $\mathrm{Soc}(A_\ell) = \mathrm{Soc}(A_r)$ by Exercise 6.2, and this ideal is simply called the *socle* of A , written $\mathrm{Soc}(A)$.

Let A be a symmetric k-algebra. In particular A is self-injective, so that projective and injective A-modules coincide (Proposition 6.7). Dualizing the fact that every indecomposable projective A-module P has a unique simple quotient $P/J(P)$, we see that every indecomposable projective A-module P has a unique simple submodule $\mathrm{Soc}(P)$. For an arbitrary k-algebra, the socle of an indecomposable projective module need not be simple, but this is the case for any self-injective k-algebra. This argument does not apply over an arbitrary complete local ring $\mathcal{O}$, because the simple A-module $P/J(P)$ is in general not an A-lattice; this is why we have to work over a field k . The extra property of the socle in the symmetric case is the following.

(6.8) PROPOSITION. *Let A be a symmetric k-algebra and let P be an indecomposable projective A-module. Then* $\mathrm{Soc}(P) \cong P/J(P)$.

Proof. Since P is isomorphic to Ae for some primitive idempotent e of A , we can assume that $P = Ae$. Then $\mathrm{Soc}(P)$ is a left ideal of A and therefore $\lambda(\mathrm{Soc}(P)) \neq 0$ by definition of a symmetric algebra, where λ denotes a symmetrizing form for A . Thus there exists $a \in \mathrm{Soc}(P)$ such that $\lambda(a) \neq 0$ and, by symmetry, we have $\lambda(ea) = \lambda(ae) = \lambda(a) \neq 0$ (notice that $a = ae$ since $a \in P$). This shows that $e\,\mathrm{Soc}(P) \neq 0$ and so $\mathrm{Hom}_A(Ae, \mathrm{Soc}(P)) \neq 0$ by Proposition 5.11. Since $\mathrm{Soc}(P)$ is simple, a non-zero homomorphism $Ae \to \mathrm{Soc}(P)$ factorizes through the unique simple quotient $Ae/J(A)e$ of Ae . Then the non-zero homomorphism $Ae/J(A)e \to \mathrm{Soc}(P)$ must be an isomorphism since both modules are simple. □

There is another useful property of socles for symmetric algebras.

(6.9) PROPOSITION. *Let* A *be a symmetric* k*-algebra and let* P *be an indecomposable projective* A*-module.*

(a) $\mathrm{End}_A(P)$ *is a symmetric algebra.*

(b) Let $f \in \mathrm{End}_A(P)$. *Then* $f \in \mathrm{Soc}(\mathrm{End}_A(P))$ *if and only if we have* $\mathrm{Im}(f) \subseteq \mathrm{Soc}(P)$.

Proof. (a) We have $P \cong Ae$ for some primitive idempotent e of A and there is an isomorphism $\mathrm{End}_A(P) \cong (eAe)^{op}$ by Proposition 5.11. By Proposition 6.4, eAe is a symmetric algebra, and therefore so is $(eAe)^{op}$, by just taking the same symmetrizing form.

(b) Since P is indecomposable, id_P is a primitive idempotent of the algebra $\mathrm{End}_A(P)$, so that $\mathrm{End}_A(P)$ is a local ring (Corollary 4.6). Therefore $J(\mathrm{End}_A(P))$ consists exactly of the non-invertible endomorphisms of P . Since P is a finite dimensional k-vector space, any non-invertible endomorphism has a non-zero kernel and a proper image. But as P is projective indecomposable, $J(P)$ is its unique maximal submodule (Proposition 5.1) and $\mathrm{Soc}(P)$ is its unique minimal submodule (Proposition 6.8). Thus any $f \in J(\mathrm{End}_A(P))$ has a kernel containing $\mathrm{Soc}(P)$ and an image contained in $J(P)$.

By Proposition 6.8, there exists an isomorphism $\overline{h} : P/J(P) \xrightarrow{\sim} \mathrm{Soc}(P)$ and $\overline{h}$ lifts to an endomorphism $h \in \mathrm{End}_A(P)$ such that $\mathrm{Ker}(h) = J(P)$ and $\mathrm{Im}(h) = \mathrm{Soc}(P)$. It follows that for any $f \in J(\mathrm{End}_A(P))$, we have $\mathrm{Im}(h) \subseteq \mathrm{Ker}(f)$ and $\mathrm{Im}(f) \subseteq \mathrm{Ker}(h)$, and therefore $fh = 0$ and $hf = 0$. This shows that h belongs to the annihilator of $J(\mathrm{End}_A(P))$, which is equal to $\mathrm{Soc}(\mathrm{End}_A(P))$.

Since $\mathrm{End}_A(P)$ is a local ring, $\mathrm{End}_A(P)/J(\mathrm{End}_A(P)) \cong k$, and therefore $\mathrm{Soc}(\mathrm{End}_A(P)) \cong k$ as $\mathrm{End}_A(P)$-modules by Proposition 6.8. Thus $\mathrm{Soc}(\mathrm{End}_A(P))$ consists exactly of the scalar multiples of h . Finally we show that the endomorphisms f satisfying $\mathrm{Im}(f) \subseteq \mathrm{Soc}(P)$ are also exactly the scalar multiples of h . Indeed if $\mathrm{Im}(f) \subseteq \mathrm{Soc}(P)$ and $f \neq 0$, then $\mathrm{Im}(f) = \mathrm{Soc}(P)$ by simplicity of $\mathrm{Soc}(P)$, and therefore $\mathrm{Ker}(f) = J(P)$ since $P/J(P)$ is the only simple quotient of P . In other words f induces an isomorphism $\overline{f} : P/J(P) \xrightarrow{\sim} \mathrm{Soc}(P)$. By Schur's lemma $\mathrm{End}_A(P/J(P)) \cong \mathrm{End}_A(\mathrm{Soc}(P)) \cong k$ and so any endomorphism $P/J(P) \to \mathrm{Soc}(P)$ is a scalar multiple of $\overline{h}$. Thus f is a scalar multiple of h . □

(6.10) REMARK. With a little bit more work, it can be shown that this proposition holds more generally for an arbitrary projective module over a symmetric k-algebra A .

Exercises

(6.1) Let A be a symmetric $\mathcal{O}$-algebra and let I and J be ideals of A.
(a) Prove that if $I \subseteq J$, then $J^{\perp} \subseteq I^{\perp}$.
(b) Prove that $I \subseteq I^{\perp\perp}$ and that $I = I^{\perp\perp}$ if $\mathcal{O} = k$. [Hint: Over k, we have $\dim(I^{\perp}) + \dim(I) = \dim(A)$ and $\dim(I^{\perp\perp}) = \dim(I)$.]
(c) Construct an example for which $I \neq I^{\perp\perp}$. [Hint: Choose a domain $\mathcal{O}$ with $\mathfrak{p} \neq 0$ and a symmetric algebra A which is free as an $\mathcal{O}$-module. Consider the ideal $\mathfrak{p}A$.]

(6.2) Let A be a symmetric $\mathcal{O}$-algebra.
(a) Let I be an ideal of A, let $\ell(I) = \{ a \in A \mid aI = 0 \}$ be the left annihilator of I, and let $r(I) = \{ a \in A \mid Ia = 0 \}$ be the right annihilator of I. Prove that $r(I)$ is a two-sided ideal and that it is equal to the orthogonal $I^{\perp}$ of I. Similarly prove that $\ell(I) = I^{\perp}$ and deduce that $r(I) = \ell(I)$.
(b) Assume that $\mathcal{O} = k$. Prove that $\mathrm{Soc}(A_{\ell}) = \mathrm{Soc}(A_r) = J(A)^{\perp}$, where $\mathrm{Soc}(A_{\ell})$ is the left socle of A and $\mathrm{Soc}(A_r)$ is the right socle of A.

(6.3) Let A be a symmetric $\mathcal{O}$-algebra and let $\lambda : A \to \mathcal{O}$ be a symmetrizing form for A. Let $\mu : A \to \mathcal{O}$ be a linear form, so that by Proposition 6.1 there exists $u \in A$ such that $\mu(a) = \lambda(au)$ for all $a \in A$. Prove that μ is a symmetrizing form for A if and only if u is central and invertible. In particular describe all symmetrizing forms for a matrix algebra.

(6.4) Prove the uniqueness of $\mathcal{O}$-injective hulls up to isomorphism (Proposition 6.6).

(6.5) Let A be a symmetric k-algebra. Prove that the Cartan matrix of A is symmetric. [Hint: Use Proposition 6.4.]

§ 7 SIMPLE ALGEBRAS AND SUBALGEBRAS

In this section, we introduce the important class of $\mathcal{O}$-simple algebras, and show their crucial properties as subalgebras of arbitrary algebras. We continue with a ring $\mathcal{O}$ satisfying Assumption 2.1.

An $\mathcal{O}$-algebra S is called *$\mathcal{O}$-simple* if S is isomorphic to $\mathrm{End}_{\mathcal{O}}(V)$ for some free $\mathcal{O}$-module V, or in other words if S is isomorphic to a matrix algebra $M_n(\mathcal{O})$ over $\mathcal{O}$ (where n is the dimension of V). In that case $J(S) = \mathfrak{p}S$ and $S/J(S)$ is a simple algebra isomorphic to $M_n(k)$. Thus S has only one point, with multiplicity n. An $\mathcal{O}$-algebra S is called *$\mathcal{O}$-semi-simple* if S is isomorphic to a direct product of $\mathcal{O}$-simple algebras. Note that an $\mathcal{O}$-semi-simple algebra is always free as an $\mathcal{O}$-module. We first prove that the Skolem–Noether theorem 1.9 holds for $\mathcal{O}$-simple algebras, starting with a useful lemma.

(7.1) LEMMA. *Let S be an $\mathcal{O}$-simple algebra, so that we can write $S \cong \mathrm{End}_{\mathcal{O}}(V)$ for some free $\mathcal{O}$-module V.*

(a) V is an indecomposable projective S-module.

(b) V is the unique indecomposable S-lattice up to isomorphism.

Proof. (a) Choose an $\mathcal{O}$-basis (v_i) of V and let e be the projection onto $\mathcal{O}v_1$, with kernel containing all the other basis elements. By the theorem on lifting idempotents, e is a primitive idempotent of S, because its image in $S/\mathfrak{p}S \cong \mathrm{End}_k(V/\mathfrak{p}V)$ is a projection onto a one-dimensional k-subspace of the k-vector space $V/\mathfrak{p}V$. Therefore Se is an indecomposable projective S-module (Proposition 5.1). Informally, Se is isomorphic to the first column of the matrix algebra S, hence is isomorphic to V. More explicitly, the map $f : Se \to V$ mapping s to $s(v_1)$ is clearly S-linear. Moreover f is surjective by elementary linear algebra, and is therefore an isomorphism since both Se and V are free $\mathcal{O}$-modules of the same dimension (Proposition 1.3).

(b) Let M be an S-lattice. Since $S/\mathfrak{p}S \cong \mathrm{End}_k(V/\mathfrak{p}V)$ is a simple k-algebra with unique simple module $V/\mathfrak{p}V$, the $(S/\mathfrak{p}S)$-module $M/\mathfrak{p}M$ is isomorphic to $(V/\mathfrak{p}V)^n$ for some n (Theorem 1.10). Since V^n is projective by (a), the map $V^n \to (V/\mathfrak{p}V)^n \cong M/\mathfrak{p}M$ lifts to a homomorphism $f : V^n \to M$. Then f must be an isomorphism since its reduction modulo $\mathfrak{p}$ is an isomorphism (Proposition 1.3). Thus $M \cong V^n$ and so, by the Krull–Schmidt theorem, V is the unique indecomposable S-lattice up to isomorphism. □

(7.2) THEOREM (Skolem–Noether). *Let S be an $\mathcal{O}$-simple algebra. Then every $\mathcal{O}$-algebra automorphism of S is an inner automorphism.*

Proof. By assumption $S \cong \mathrm{End}_{\mathcal{O}}(V)$ for some free $\mathcal{O}$-module V and we identify S with $\mathrm{End}_{\mathcal{O}}(V)$. By Lemma 7.1, V is the unique indecomposable S-lattice up to isomorphism. Now let g be an automorphism of S. Then V carries another S-module structure, defined by $s * v = g(s)(v)$ (where $s \in S$ and $v \in V$), and this is again indecomposable. By uniqueness of V, the new module structure on V is isomorphic to the original one. Therefore there exists an $\mathcal{O}$-linear automorphism h of V such that $h(s * v) = s(h(v))$ for all $s \in S$ and $v \in V$. But $h \in \mathrm{End}_{\mathcal{O}}(V) = S$ and h is invertible, so that we obtain $g(s)(v) = s * v = h^{-1}sh(v)$, or in other words $g(s) = h^{-1}sh$ for all $s \in S$. □

Now we consider $\mathcal{O}$-semi-simple subalgebras. Given an $\mathcal{O}$-algebra A and an $\mathcal{O}$-semi-simple subalgebra S of A, it follows from Exercise 2.1 that $J(A) \cap S = J(S)$ because $J(S) = \mathfrak{p}S \subseteq J(A)$. Therefore the semi-simple k-algebra $S/J(S)$ embeds into the semi-simple k-algebra $A/J(A)$. There are many possible such embeddings since on the one hand any matrix algebra $M_n(k)$ has subalgebras of the form $M_{a_1}(k) \times \ldots \times M_{a_r}(k)$ (provided $a_1 + \ldots a_r \leq n$) and on the other hand $M_a(k)$ can be embedded diagonally in $M_n(k) \times M_m(k)$ (provided $a \leq n$ and $a \leq m$). We are particularly interested in the extreme case where $S/J(S) = A/J(A)$, or in other words $S + J(A) = A$; this means that S is an $\mathcal{O}$-semi-simple lift in A of the k-semi-simple quotient $A/J(A)$. In that case S turns out to be a *maximal* $\mathcal{O}$-semi-simple subalgebra of A and any maximal $\mathcal{O}$-semi-simple subalgebra is of that type, as we now prove.

(7.3) THEOREM. *Let A be an $\mathcal{O}$-algebra which is free as an $\mathcal{O}$-module.*

(a) There exists an $\mathcal{O}$-semi-simple subalgebra S such that $S+J(A) = A$.

(b) An $\mathcal{O}$-semi-simple subalgebra S of A is maximal if and only if we have $S + J(A) = A$. In particular any $\mathcal{O}$-semi-simple subalgebra T of A is contained in an $\mathcal{O}$-semi-simple subalgebra S of A such that $S + J(A) = A$.

(c) Any two maximal $\mathcal{O}$-semi-simple subalgebras of A are conjugate by an element of A^*.

Proof. (a) In a primitive decomposition of 1_A, one can choose one idempotent e_α for each point α of A and write the others as conjugates of those. Thus we have

$$1_A = \sum_{\alpha \in \mathcal{P}(A)} \sum_{u \in U_\alpha} e_\alpha^u ,$$

where U_α is a finite set of invertible elements of A (whose cardinality is necessarily the multiplicity of α). Now consider the elements $u^{-1}e_\alpha v$ where $\alpha \in \mathcal{P}(A)$ and $u, v \in U_\alpha$. They satisfy the following orthogonality relations:

$$(7.4) \qquad t^{-1}e_\alpha u \cdot v^{-1}e_\beta w = \begin{cases} t^{-1}e_\alpha w & \text{if } \alpha = \beta \text{ and } u = v, \\ 0 & \text{otherwise.} \end{cases}$$

Indeed $t^{-1}e_\alpha u \cdot v^{-1}e_\beta w = t^{-1}ue_\alpha^u \cdot e_\beta^v v^{-1}w$ and we know that the two middle idempotents are orthogonal if they are not equal.

The first consequence of the relations 7.4 is that the elements $u^{-1}e_\alpha v$ are $\mathcal{O}$-linearly independent, and are even part of an $\mathcal{O}$-basis of A. Indeed by Proposition 1.3 (and because A is free as an $\mathcal{O}$-module by assumption), it suffices to prove this in the k-algebra $\overline{A} = A/\mathfrak{p}A$. But since $\mathfrak{p}A \subseteq J(A)$, the images $\overline{u}^{-1}\overline{e}_\alpha\overline{v}$ of the elements $u^{-1}e_\alpha v$ are non-zero in $\overline{A}$ (by the theorem on lifting idempotents). If $\sum_{\alpha,u,v} \lambda_{\alpha,u,v}\overline{u}^{-1}\overline{e}_\alpha\overline{v} = 0$ (where $\lambda_{\alpha,u,v} \in k$), it suffices to multiply this relation by $\overline{u}^{-1}\overline{e}_\alpha\overline{v}$ to obtain $\lambda_{\alpha,u,v}\overline{u}^{-1}\overline{e}_\alpha\overline{v} = 0$ and therefore $\lambda_{\alpha,u,v} = 0$. This proves the required linear independence.

The next observation is that the relations 7.4 correspond exactly to the multiplication rules for the standard basis of a matrix algebra. Thus for each point α, we see that $S(\alpha) = \bigoplus_{u,v\in U_\alpha} \mathcal{O} \cdot u^{-1}e_\alpha v$ is isomorphic to a matrix algebra over $\mathcal{O}$ (of size $|U_\alpha|$) and therefore

$$S = \bigoplus_{\substack{\alpha\in\mathcal{P}(A) \\ u,v\in U_\alpha}} \mathcal{O} \cdot u^{-1}e_\alpha v \cong \prod_{\alpha\in\mathcal{P}(A)} S(\alpha)$$

is an $\mathcal{O}$-semi-simple subalgebra of A. Since the images in $A/J(A)$ of the elements $u^{-1}e_\alpha v$ are non-zero (by the theorem on lifting idempotents), they generate a semi-simple k-algebra which is the whole of $A/J(A)$ by construction (or by comparison of dimensions). Therefore $S + J(A) = A$, as required.

(b) Assume that $S + J(A) = A$ and that S is contained in some maximal $\mathcal{O}$-semi-simple subalgebra S'. Then we also have $S' + J(A) = A$ and both S and S' lift the semi-simple k-algebra $A/J(A)$. It follows that $S' = S + \mathfrak{p}S'$ and therefore $S' = S$ by Nakayama's lemma. This shows that S is maximal.

Conversely let T be an $\mathcal{O}$-semi-simple subalgebra of A. We have to show that $T \subseteq S$ where S is $\mathcal{O}$-semi-simple and $S + J(A) = A$. The element 1_T is an idempotent of A, and T is a subalgebra of the $\mathcal{O}$-semi-simple algebra $T' = T \times \mathcal{O}(1_A - 1_T)$. Replacing T by T', we can assume that $1_T = 1_A$. Either by the argument of part (a) applied to T or by direct inspection of the standard basis of a matrix algebra (see Exercise 7.1), we can write

$$T = \bigoplus_{\substack{\alpha\in\mathcal{P}(T)\\ u,u'\in U_\alpha}} \mathcal{O}\cdot u^{-1}e_\alpha u' \,,$$

where e_α is a primitive idempotent of T belonging to α, where all $u,u'\in U_\alpha$ are invertible elements of T, and where $1=\sum_\alpha\sum_{u\in U_\alpha} e_\alpha^u$ is a primitive decomposition of 1 in T. Each e_α is primitive in T, but not necessarily in A. So choose a primitive decomposition in A of each e_α,

$$e_\alpha = \sum_{\beta\in\mathcal{P}(A)} \sum_{v\in V_{\alpha,\beta}} f_{\alpha,\beta}^v$$

where $f_{\alpha,\beta}\in\beta$ or $f_{\alpha,\beta}=0$, and $V_{\alpha,\beta}$ is a finite subset of A^*. For every $\beta\in\mathcal{P}(A)$, fix some primitive idempotent g_β in β and write $f_{\alpha,\beta} = g_\beta^{w(\alpha,\beta)}$ whenever it is non-zero. Then we obtain a primitive decomposition of 1 in A

$$1=\sum_{\beta\in\mathcal{P}(A)}\Big(\sum_{\substack{\alpha\in\mathcal{P}(T)\\ f_{\alpha,\beta}\neq 0}}\sum_{u\in U_\alpha}\sum_{v\in V_{\alpha,\beta}} g_\beta^{w(\alpha,\beta)vu}\Big).$$

Therefore, as in the proof of part (a), we have an $\mathcal{O}$-semi-simple subalgebra S of A having an $\mathcal{O}$-basis $\{\,(w(\alpha,\beta)vu)^{-1}g_\beta\,(w(\alpha,\beta)v'u')\,\}$ and such that $S+J(A)=A$. By construction it is clear that each element $u^{-1}e_\alpha u'$ belongs to S and this proves that T is contained in S.

(c) Let S and T be two maximal $\mathcal{O}$-semi-simple subalgebras of A. As above we can write

$$S = \bigoplus_{\substack{\alpha\in\mathcal{P}(S)\\ u,u'\in U_\alpha}} \mathcal{O}\cdot u^{-1}e_\alpha u' \qquad\text{and}\qquad T = \bigoplus_{\substack{\alpha\in\mathcal{P}(T)\\ v,v'\in V_\alpha}} \mathcal{O}\cdot v^{-1}f_\alpha v' \,,$$

where $1_S=\sum_\alpha\sum_{u\in U_\alpha} e_\alpha^u$ is a primitive decomposition of 1_S (and similarly for T). We can assume that the sets U_α are disjoint: with respect to the decomposition $S=\prod_\alpha S(\alpha)$ into simple $\mathcal{O}$-algebras, it suffices to choose the elements of U_α with all components equal to 1, except in $S(\alpha)$ where they can be taken different from 1 (using a central element of $S(\alpha)$ instead of 1 if necessary). Similarly we can assume that the sets V_α are disjoint.

Since S is maximal, it maps onto $A/J(A)$ (because by (b) we have $S+J(A)=A$) and therefore each idempotent e_α remains primitive in $A/J(A)$, hence also in A. Thus it is clear that the inclusion $S\to A$

induces a bijection between $\mathcal{P}(S)$ and $\mathcal{P}(A)$, and consequently we can index both sets of points of S and T by $\alpha \in \mathcal{P}(A)$. Moreover the primitive idempotents e_α and f_α belong to the same point of A, so are conjugate in A; we write $f_\alpha = e_\alpha^{c_\alpha}$ for some $c_\alpha \in A^*$.

Since the cardinalities of U_α and V_α are equal (they are both the multiplicity of α), there exists a bijection $g : \bigcup_\alpha U_\alpha \to \bigcup_\alpha V_\alpha$ mapping U_α onto V_α, using the fact that the sets U_α (respectively V_α) are disjoint. Now consider the element of A

$$a = \sum_{\beta \in \mathcal{P}(A)} \sum_{w \in U_\beta} w^{-1} e_\beta \, c_\beta \, g(w) .$$

We have orthogonality relations similar to the relations 7.4 (because the idempotents $f_\alpha^{g(u)} = g(u)^{-1} c_\alpha^{-1} e_\alpha \, c_\alpha \, g(u)$ are orthogonal). Therefore

$$\Big(\sum_{\substack{\beta \in \mathcal{P}(A) \\ w \in U_\beta}} w^{-1} e_\beta \, c_\beta \, g(w) \Big) \Big(\sum_{\substack{\gamma \in \mathcal{P}(A) \\ x \in U_\gamma}} g(x)^{-1} c_\gamma^{-1} e_\gamma \, x \Big) = \sum_{\substack{\beta \in \mathcal{P}(A) \\ w \in U_\beta}} w^{-1} e_\beta \, w = 1 ,$$

and similarly for the product in the other order (or use Exercise 3.3). Thus a is invertible. Now the orthogonality relations also imply that

$$(u^{-1} e_\alpha \, u') \cdot a = u^{-1} e_\alpha \, c_\alpha \, g(u') = a \cdot (g(u)^{-1} c_\alpha^{-1} e_\alpha \, c_\alpha \, g(u')) .$$

It follows that

$$a^{-1} (u^{-1} e_\alpha \, u') a = g(u)^{-1} c_\alpha^{-1} e_\alpha \, c_\alpha \, g(u') = g(u)^{-1} f_\alpha \, g(u') .$$

Thus conjugation by a maps S onto T, as required. □

Let B be a non-zero $\mathcal{O}$-algebra and assume that $\mathcal{O}$ maps injectively into B (via $\lambda \mapsto \lambda \cdot 1_B$). This condition is satisfied for instance if B is free as an $\mathcal{O}$-module, and this always holds if $\mathcal{O} = k$. Then it is clear that the algebra $A = M_n(B)$ has an $\mathcal{O}$-simple subalgebra S isomorphic to $M_n(\mathcal{O})$. Moreover there is an isomorphism of algebras $S \otimes_{\mathcal{O}} B \cong A$. Recall that the *centralizer* of a subalgebra S in A is the subalgebra

$$C_A(S) = \{ a \in A \mid as = sa \text{ for all } s \in S \} .$$

It is easy to see here that $C_A(S)$ consists of the diagonal matrices with all diagonal entries equal to some $b \in B$. Thus $C_A(S) \cong B$ and the isomorphism maps $a \in C_A(S)$ to its top left entry, which can also be viewed as the matrix $eae = ea = ae$, where e is the idempotent matrix having a single non-zero entry equal to 1 in the top left corner. Note that e is a primitive idempotent of S (but not necessarily of A). Therefore A is isomorphic to $S \otimes_{\mathcal{O}} C_A(S)$ and $C_A(S) \cong eAe \cong B$. The proofs of all these assertions are easy and are left to the reader (Exercise 7.3).

We now wish to prove that if an arbitrary $\mathcal{O}$-algebra A merely has an $\mathcal{O}$-simple subalgebra S with the same unity element as A, then we are necessarily in the situation described above, so that A decomposes as the tensor product of S and its centralizer.

(7.5) PROPOSITION. *Let A be an $\mathcal{O}$-algebra and let S be an $\mathcal{O}$-simple subalgebra of A with $1_S = 1_A$. Let $C_A(S)$ be the centralizer of S and let e be a primitive idempotent of S.*
(a) *There is an isomorphism of $\mathcal{O}$-algebras*

$$\phi : S \otimes_{\mathcal{O}} C_A(S) \xrightarrow{\sim} A\,, \quad s \otimes a \mapsto sa\,.$$

In other words $A \cong M_n(C_A(S))$ if $S \cong M_n(\mathcal{O})$.
(b) *There is an isomorphism of $\mathcal{O}$-algebras*

$$C_A(S) \xrightarrow{\sim} eAe\,, \quad a \mapsto ea = ae = eae\,.$$

Proof. (a) It is clear that ϕ is well-defined and is an $\mathcal{O}$-linear map. It is a homomorphism of algebras because S and $C_A(S)$ commute by definition:

$$\phi((s\otimes a)(s'\otimes a')) = \phi(ss'\otimes aa') = ss'aa' = sas'a' = \phi(s\otimes a)\phi(s'\otimes a')\,.$$

Since S is $\mathcal{O}$-simple, all primitive idempotents of S are conjugate and so there is a primitive decomposition

$$1_S = \sum_{u\in U} e^u\,,$$

where U is a finite set of invertible elements of S. As in the proof of Theorem 7.3, the elements $u^{-1}ev$ (for $u,v\in U$) form an $\mathcal{O}$-basis of S and satisfy orthogonality relations as in 7.4. This implies in particular that for any $eae \in eAe$, the element $\sum_{w\in U}(eae)^w$ commutes with S, because its product on either side with the basis element $u^{-1}ev$ yields $u^{-1}eaev$. Thus $\sum_{w\in U}(eae)^w \in C_A(S)$ and this allows us to define the following $\mathcal{O}$-linear map:

$$\psi : A \longrightarrow S\otimes_{\mathcal{O}} C_A(S)\,, \quad a \mapsto \sum_{u,v\in U}\Big(u^{-1}ev \otimes \sum_{w\in U}(euav^{-1}e)^w\Big)\,.$$

We now show that ψ is the inverse of ϕ. First we have

$$\begin{aligned}\phi\psi(a) &= \sum_{u,v\in U} u^{-1}ev \sum_{w\in U}(euav^{-1}e)^w = \sum_{u,v\in U} u^{-1}euav^{-1}ev\\ &= 1_S\, a\, 1_S = a\,,\end{aligned}$$

because $1_S = 1_A$. On the other hand let $b\in C_A(S)$ and let $s^{-1}et$ be a basis element of S (with $s,t\in U$). Then

$$\psi\phi(s^{-1}et\otimes b) = \sum_{u,v\in U}\Big(u^{-1}ev\otimes \sum_{w\in U}(eus^{-1}etbv^{-1}e)^w\Big)\,.$$

We have $eus^{-1}e = ue^ue^ss^{-1} = 0$ if $u \neq s$, while for $u = s$ the term in the inner sum is equal to $etbv^{-1}e = betv^{-1}e$, using the fact that b centralizes S. This is again zero by orthogonality unless $t = v$. For $u = s$ and $t = v$, the inner sum is equal to

$$\sum_{w \in U} (be)^w = \sum_{w \in U} be^w = b\,1_S = b\,,$$

using the fact that $b^w = b$ since b centralizes $w \in S$. Therefore we have $\psi\phi(s^{-1}et \otimes b) = s^{-1}et \otimes b$.

(b) Let $C = C_A(S)$. Clearly $S \otimes 1$ corresponds to S under the isomorphism ϕ of part (a), and $1 \otimes C$ corresponds to C. The definition of the inverse map ψ constructed above shows that an arbitrary element of C can be written $c = \sum_{w \in U} (eae)^w$ where $eae \in eAe$. We can assume that e is one of the idempotents in the decomposition $1_S = \sum_w e^w$ and, by orthogonality, we have $ece = eae$. It is then clear that $c \mapsto ece$ and $eae \mapsto \sum_{w \in U} (eae)^w$ are inverse isomorphisms between C and eAe. □

In the situation of the proposition, for any A-module M, it is clear that eM is a C-submodule of M, where $C = C_A(S)$. On the other hand Se is an S-module (which is indecomposable projective). Thus $Se \otimes_{\mathcal{O}} eM$ is an $S \otimes_{\mathcal{O}} C$-module, which can be viewed as an A-module via the isomorphism ϕ.

(7.6) PROPOSITION. *With the notation of the previous proposition, let M be an A-module. Then there is an isomorphism of A-modules*

$$Se \otimes_{\mathcal{O}} eM \xrightarrow{\sim} M\,, \quad s \otimes m \mapsto sm\,.$$

Proof. It is easy to see that the map is a homomorphism of A-modules. Letting $1 = \sum_u e^u$ be a primitive decomposition in S as in the proof of the previous proposition, we define the inverse map by $m \mapsto \sum_u u^{-1}e \otimes eum$. The details of the proof are left to the reader. □

(7.7) REMARK. In the situation of the proposition above, the correspondence $M \mapsto eM$ is in fact a functor from the category of A-modules to the category of C-modules, and this functor is an equivalence of categories. Thus A and C are Morita equivalent in the sense of Section 9.

Exercises

(7.1) Let e be the matrix in $M_n(\mathcal{O})$ with a single non-zero entry $e_{11} = 1$. Find a set $\{u_1, \ldots, u_n\}$ of invertible elements such that $(u_i^{-1} e\, u_j)_{1 \leq i,j \leq n}$ is the canonical basis of $M_n(\mathcal{O})$.

(7.2) Let A be an $\mathcal{O}$-algebra and let B be a subalgebra of A such that $A = B + J(A)$. Prove that any maximal $\mathcal{O}$-semi-simple subalgebra of B is also a maximal $\mathcal{O}$-semi-simple subalgebra of A.

(7.3) Prove that a commutative $\mathcal{O}$-semi-simple algebra is isomorphic to a direct product of copies of $\mathcal{O}$. Prove that the commutative $\mathcal{O}$-semi-simple subalgebras of an $\mathcal{O}$-algebra A are in bijection with the decompositions of 1_A into orthogonal idempotents, and that the maximal ones correspond to the primitive decompositions. For commutative $\mathcal{O}$-semi-simple subalgebras, state and prove a theorem analogous to Theorem 7.3.

(7.4) Let B be an $\mathcal{O}$-algebra and assume that $\mathcal{O}$ maps injectively into B. Let $S = M_n(\mathcal{O})$ be the $\mathcal{O}$-simple subalgebra of $A = M_n(B)$ and let e be the primitve idempotent of S with a single non-zero entry $e_{11} = 1$. Prove directly all the facts mentioned before Proposition 7.5, namely that $S \otimes_{\mathcal{O}} B \cong A$, that $C_A(S)$ consists of diagonal matrices, and that we have $C_A(S) \cong eAe \cong B$.

(7.5) Provide the details of the proof of Proposition 7.6.

(7.6) Let A be an $\mathcal{O}$-algebra which is free as an $\mathcal{O}$-module. Assume that $A/\mathfrak{p}A$ is a semi-simple k-algebra. Prove that A is $\mathcal{O}$-semi-simple. [Hint: Use Proposition 1.3.]

§ 8 EXOMORPHISMS AND EMBEDDINGS

One of the prominent features of non-commutative algebra is the use of concepts which are only defined up to conjugation. We have already seen it with the definition of points, but this applies to homomorphisms as well and leads to the fundamental concepts of exomorphism and embedding. We prove in this section some of the main properties of embeddings, in particular two cancellation results which will be often used in the sequel. As usual $\mathcal{O}$ is a ring satisfying Assumption 2.1.

Let A and B be two $\mathcal{O}$-algebras. For many purposes, the composition of a homomorphism $f : A \to B$ with an inner automorphism of either A or B (or both) has to be considered as equivalent to f. It is clear that this defines an equivalence relation on the set of homomorphisms from A to B and an equivalence class is called an *exomorphism* from A to B (or also *exterior homomorphism*). If $a \in A^*$, write $\mathrm{Inn}(a)$ for the inner automorphism defined by a, that is $\mathrm{Inn}(a)(x) = {}^a x$ (using the notation ${}^a x = axa^{-1}$). Then for any homomorphism $f : A \to B$, we have

(8.1) $$f \cdot \mathrm{Inn}(a) = \mathrm{Inn}\big(f(a) + 1_B - f(1_A)\big) \cdot f$$

using the invertibility of $f(a) + 1_B - f(1_A)$ which we noticed at the end of Section 2. It follows that the exomorphism containing f is also simply the set

$$\mathcal{F} = \{\mathrm{Inn}(b) \cdot f \mid b \in B^*\}.$$

We shall use freely the notation $\mathcal{F} : A \to B$ for an exomorphism $\mathcal{F}$ from A to B. Equation 8.1 also implies immediately the following lemma which shows that exomorphisms can be composed.

(8.2) LEMMA. *Let A, B and C be $\mathcal{O}$-algebras. Let $\mathcal{F} : A \to B$ and $\mathcal{G} : B \to C$ be two exomorphisms. Then the set*

$$\mathcal{G} \cdot \mathcal{F} = \{g \cdot f \mid g \in \mathcal{G}, f \in \mathcal{F}\}$$

is an exomorphism from A to C.

The exomorphism containing the identity map $id_A : A \to A$ consists of all inner automorphisms of A and deserves the name of *identity exomorphism*. Thus the category of $\mathcal{O}$-algebras and exomorphisms is perfectly well-defined. An isomorphism in this category consists of ordinary isomorphisms and will be called an *exo-isomorphism* (or also an *exterior* isomorphism). An exomorphism containing an automorphism is called an *exo-automorphism* or also an *outer automorphism* (which is a more classical terminology).

The next important definition is that of an embedding. An exomorphism $\mathcal{F}$ from A to B is called an *embedding* if some $f \in \mathcal{F}$ is injective and has for image the whole of $f(1_A)Bf(1_A)$. Since conjugation in B is harmless, it is clear that any $f \in \mathcal{F}$ has the same two properties. If e is an idempotent in B and $j : eBe \to B$ is the inclusion, then the exomorphism $\mathcal{J}$ containing j is an embedding. This is in fact essentially the only example since any embedding is clearly the composition of an exo-isomorphism followed by an embedding of this special type.

If α is a point of A and e belongs to α, the subalgebra eAe depends on the choice of e. But we wish to have a concept which only depends on the point α and which is unique in some natural sense. Thus we define an *embedding associated* with the point α to be an embedding $\mathcal{F} : B \to A$ such that $f(1_B) \in \alpha$ for some $f \in \mathcal{F}$ (and thus for each $f \in \mathcal{F}$). To show the existence of such an embedding, it suffices to choose some $e \in \alpha$ and take the exomorphism containing the inclusion $f : eAe \to A$. We now prove that associated embeddings are unique up to a unique exo-isomorphism.

(8.3) LEMMA. *Let $\mathcal{F} : B \to A$ and $\mathcal{F}' : B' \to A$ be two embeddings associated with a point α of A. Then there exists a unique exo-isomorphism $\mathcal{H} : B' \to B$ such that $\mathcal{F}' = \mathcal{F} \cdot \mathcal{H}$.*

Proof. Let $f \in \mathcal{F}$ and $e = f(1_B)$. By definition of embedding, one can factorize f as the composition of an isomorphism $f_0 : B \to eAe$ followed by the inclusion $eAe \to A$. For $f' \in \mathcal{F}'$, the idempotent $f'(1_{B'})$ belongs by assumption to the same point α as $e = f(1_B)$. After conjugation, one can choose f' such that $f'(1_{B'}) = e$ and so f' factorizes as the composition of an isomorphism $f'_0 : B' \to eAe$ followed by the inclusion $eAe \to A$. Then the isomorphism $h = (f_0)^{-1}f'_0$ is the unique isomorphism satisfying $f' = fh$ and it follows that the exomorphism $\mathcal{H}$ containing h is the required exo-isomorphism. The uniqueness of $\mathcal{H}$ is an easy consequence of the uniqueness of h. □

We emphasize that this crucial result is a uniqueness property of the pair $(B, \mathcal{F})$. If we only consider the algebra B (for instance if we choose $B = eAe$), then we obtain an object which is unique up to isomorphism, but not necessarily up to a *unique* exo-isomorphism (because an exo-isomorphism can always be composed with an arbitrary exo-automorphism of B). Note also that both the definition of associated embeddings and their uniqueness property show the relevance of the concept of exomorphism, as opposed to homomorphisms.

(8.4) EXAMPLE. Consider the matrix algebra $A = M_n(\mathcal{O})$ and its unique point α. For each $e \in \alpha$ (for instance the matrix with a single non-zero entry equal to 1 at the top left corner), eAe is isomorphic to $\mathcal{O}$. There is in this case a canonical choice for an embedding associated with α, namely the exomorphism $\mathcal{O} \to A$ containing the map defined by $1_{\mathcal{O}} \mapsto e$. Another choice of e yields the same exomorphism.

We now consider the behaviour of points with respect to embeddings and we give a version of Proposition 4.12 which takes into account exomorphisms. Let $\mathcal{F} : A \to B$ be an embedding of $\mathcal{O}$-algebras and let $f \in \mathcal{F}$. By Proposition 4.12, f induces an injective map $\mathcal{P}(A) \to \mathcal{P}(B)$ which maps $\alpha \in \mathcal{P}(A)$ to the point $\beta \in \mathcal{P}(B)$ such that $f(\alpha) \subseteq \beta$. In other words β is the conjugacy closure of $f(\alpha)$. If $f' = \mathrm{Inn}(b)f$ is another representative of the exomorphism $\mathcal{F}$ and if $i \in \alpha$, then $f'(i) = bf(i)b^{-1}$. Thus $f'(i)$ belongs to the same point β and this proves that the map $\mathcal{P}(A) \to \mathcal{P}(B)$ is independent of the choice of $f \in \mathcal{F}$. Moreover the image of α is the set

$$\beta = \mathcal{F}(\alpha) = \{\, f(i) \mid f \in \mathcal{F}, i \in \alpha \,\},$$

because this is now closed under conjugation.

The first part of the next result summarizes this discussion.

(8.5) PROPOSITION. *Let $\mathcal{F} : A \to B$ be an embedding of $\mathcal{O}$-algebras.*
(a) $\mathcal{F}$ induces an injective map $\mathcal{P}(A) \to \mathcal{P}(B)$, $\alpha \mapsto \mathcal{F}(\alpha)$.
(b) $\mathcal{F}$ induces an embedding $\overline{\mathcal{F}} : \overline{A} \to \overline{B}$, where $\overline{A} = A/J(A)$ and $\overline{B} = B/J(B)$.

Proof. The first statement was proved above, so we consider the second. Let $f \in \mathcal{F}$ and $e = f(1_A)$. Denote by a bar the images of elements of B in $\overline{B}$. Since $\mathcal{F}$ is an embedding, f induces an isomorphism $A \cong f(A) = eBe$. By Proposition 1.17 we have

$$f(J(A)) = J(f(A)) = J(eBe) = eJ(B)e = J(B) \cap eBe = J(B) \cap f(A).$$

It follows that on the one hand f induces $\overline{f} : \overline{A} \to \overline{B}$ and on the other hand $\overline{f}$ is injective. If $f' = \mathrm{Inn}(b)f$ is another representative of $\mathcal{F}$, then obviously $\overline{f}' = \mathrm{Inn}(\overline{b})\overline{f}$ and it follows that the exomorphism $\overline{\mathcal{F}}$ containing $\overline{f}$ is well-defined. Finally consider the commutative diagram

$$\begin{array}{ccc} A & \xrightarrow{f} & eBe \\ \downarrow & & \downarrow \\ \overline{A} & \xrightarrow{\overline{f}} & \overline{e}\overline{B}\overline{e}. \end{array}$$

Since f and the vertical maps are surjective, we have $\overline{f}(\overline{A}) = \overline{e}\overline{B}\overline{e}$ and this shows that $\overline{\mathcal{F}}$ is an embedding. □

If g is an injective map, it is clear that $gf = gf'$ implies $f = f'$. This property does not hold for exomorphisms: if $f, f' : \mathcal{O} \to \mathcal{O} \times \mathcal{O}$ are the two distinct embeddings and if $g : \mathcal{O} \times \mathcal{O} \to M_2(\mathcal{O})$ is the injection onto the diagonal, then gf and gf' belong to the same exomorphism, but f and f' do not differ by an inner automorphism (since $\mathcal{O} \times \mathcal{O}$ is commutative). In other words an injective exomorphism is not necessarily a monomorphism in the category of $\mathcal{O}$-algebras and exomorphisms. However, we now prove that an embedding is a monomorphism.

(8.6) PROPOSITION. *Let $\mathcal{F}, \mathcal{F}' : A \to B$ be two exomorphisms of $\mathcal{O}$-algebras and let $\mathcal{G} : B \to C$ be an embedding of $\mathcal{O}$-algebras.*
(a) If $\mathcal{G}\mathcal{F} = \mathcal{G}\mathcal{F}'$, then $\mathcal{F} = \mathcal{F}'$. In other words $\mathcal{G}$ is a monomorphism.
(b) $\mathcal{F}$ is an embedding if and only if $\mathcal{G}\mathcal{F}$ is an embedding.

Proof. (a) Let $f \in \mathcal{F}$, $f' \in \mathcal{F}'$ and $g \in \mathcal{G}$. Then by assumption there exists $c \in C^*$ such that

$$gf'(a) = c \cdot gf(a) \cdot c^{-1} \qquad \text{for all } a \in A \; .$$

Let $j = f(1_A)$ and $j' = f'(1_A)$. Then $g(j)$ and $g(j')$ are conjugate in C, but since $\mathcal{G}$ is an embedding, it follows from Proposition 4.12 that j and j' are already conjugate in B. Changing the choice of $f' \in \mathcal{F}'$, we can therefore assume that $f(1_A) = f'(1_A) = j$.

We deduce from the equation above that the idempotent $g(j)$ commutes with c (and with c^{-1}). Since $\mathcal{G}$ is an embedding, g is injective and its image is $g(1_B)C\,g(1_B)$, which contains $g(j)C\,g(j)$. Therefore the element $g(j)c = c\,g(j) = g(j)c\,g(j)$ is the image under g of a unique element $b \in B$. Similarly there is a unique $b' \in B$ with $g(b') = g(j)c^{-1}$. Moreover $jb = b = bj$, $jb' = b' = b'j$ and $bb' = j$ because these equalities hold after applying the injective map g. It follows that $b_0 = b + (1_B - j)$ is invertible in B with inverse $b_0^{-1} = b' + (1_B - j)$, because j and $(1_B - j)$ are orthogonal. Now for all $a \in A$, we have

$$f'(a) = b_0 \cdot f(a) \cdot b_0^{-1}$$

because by applying g to the right hand side, we obtain

$$\begin{aligned} &\big(g(j)c + g(1_B) - g(j)\big)\; gf(1_A a\, 1_A)\; \big(g(j)c^{-1} + g(1_B) - g(j)\big) \\ =&\big(g(j)c + g(1_B) - g(j)\big)\; g(j)gf(a)g(j)\; \big(g(j)c^{-1} + g(1_B) - g(j)\big) \\ =&c\, g(j)gf(a)g(j)\, c^{-1} = c\, gf(a)\, c^{-1} = gf'(a) \, . \end{aligned}$$

This proves that $f' = \mathrm{Inn}(b_0)\, f$ and $\mathcal{F} = \mathcal{F}'$.

(b) It is straightforward to see that the composite of two embeddings is an embedding. Conversely, if $\mathcal{G}\mathcal{F}$ and $\mathcal{G}$ are embeddings, let $f \in \mathcal{F}$ and $g \in \mathcal{G}$. It is clear that f is injective since gf is. Moreover if $b \in f(1_A)Bf(1_A)$, then $g(b) \in gf(1_A)C\,gf(1_A)$ and so there exists $a \in A$ such that $g(b) = gf(a)$. By injectivity of g, we obtain $b = f(a)$, and this completes the proof that $\mathcal{F}$ is an embedding. □

With an extra assumption on the embedding $\mathcal{G}$, we prove that it is also an epimorphism in the category of $\mathcal{O}$-algebras and exomorphisms. Thus it is both a monomorphism and an epimorphism (without being an isomorphism).

(8.7) PROPOSITION. *Let* $\mathcal{F}, \mathcal{F}' : A \to B$ *be two exomorphisms of* $\mathcal{O}$*-algebras and let* $\mathcal{G} : C \to A$ *be an embedding of* $\mathcal{O}$*-algebras. Assume that* C *and* A *have the same number of points.*
(a) If $\mathcal{F}\mathcal{G} = \mathcal{F}'\mathcal{G}$, *then* $\mathcal{F} = \mathcal{F}'$. *In other words* $\mathcal{G}$ *is an epimorphism.*
(b) $\mathcal{F}$ *is an embedding if and only if* $\mathcal{F}\mathcal{G}$ *is an embedding.*

Proof. Without loss of generality we can assume that $C = eAe$ and that $\mathcal{G}$ is the embedding containing the inclusion $g : eAe \to A$, where e is an idempotent of A. By Proposition 8.5, $\mathcal{G}$ induces an injection $\mathcal{G}_* : \mathcal{P}(C) \to \mathcal{P}(A)$ and since these two sets have the same cardinality by assumption, the map $\mathcal{G}_*$ is a bijection. This means that for every point $\alpha \in \mathcal{P}(A)$, there exists $e_\alpha \in \alpha$ with $e_\alpha \in C$. Then, as in the proof of Theorem 7.3, we can write a primitive decomposition of the unity element

$$1_A = \sum_{\alpha \in \mathcal{P}(A)} \sum_{u \in U_\alpha} u^{-1} e_\alpha u \, ,$$

where U_α is a finite set of invertible elements of A (whose cardinality is necessarily the multiplicity of α). Then for $\alpha, \beta \in \mathcal{P}(A)$ and $u \in U_\alpha$, $v \in U_\beta$, we have the orthogonality relations

$$\text{(8.8)} \qquad e_\alpha u \cdot v^{-1} e_\beta = \begin{cases} e_\alpha & \text{if } \alpha = \beta \text{ and } u = v, \\ 0 & \text{otherwise.} \end{cases}$$

(a) Let $f \in \mathcal{F}$ and $f' \in \mathcal{F}'$. By assumption $fg = \mathrm{Inn}(b) f' g$ for some $b \in B^*$. Thus changing the choice of $f' \in \mathcal{F}'$, we can assume that $fg = f'g$. In other words f and f' coincide on the subalgebra $C = eAe$ and we have to show that they belong to same exomorphism. Since each e_α belongs to C, we can define

$$j_\alpha = f(e_\alpha) = f'(e_\alpha) \, .$$

Then we have

$$f(1_A) = \sum_{\alpha,u} f(u^{-1}) j_\alpha f(u) = \sum_{\alpha,u} f_*(u)^{-1} j_\alpha f_*(u) \, ,$$
$$f'(1_A) = \sum_{\alpha,u} f'(u^{-1}) j_\alpha f'(u) = \sum_{\alpha,u} f'_*(u)^{-1} j_\alpha f'_*(u) \, ,$$

where $f_*(u) = f(u) + (1_B - f(1_A))$ and $f'_*(u) = f'(u) + (1_B - f'(1_A))$. Here $1_B - f(1_A)$ and $1_B - f'(1_A)$ are added in order to make $f_*(u)$ and $f'_*(u)$ invertible, but they cancel since

$$(1_B - f(1_A))j_\alpha = (1_B - f(1_A))f(e_\alpha) = (1_B - f(1_A))f(1_A)f(e_\alpha) = 0\,,$$

and similarly with f'. The above decompositions of $f(1_A)$ and $f'(1_A)$ are orthogonal and they involve conjugates of the same idempotents j_α. Therefore $f(1_A)$ and $f'(1_A)$ have the same multiplicities and, by Proposition 4.16, they are conjugate:

$$f'(1_A) = b^{-1}f(1_A)b \text{ for some } b \in B^*\,.$$

Now define

$$c = \Big(\sum_{\alpha\in\mathcal{P}(A)}\ \sum_{u\in U_\alpha} f(u^{-1})j_\alpha f'(u)\Big) + (1_B - f(1_A))\,b\,(1_B - f'(1_A))\,,$$

$$c' = \Big(\sum_{\beta\in\mathcal{P}(A)}\ \sum_{v\in U_\beta} f'(v^{-1})j_\beta f(v)\Big) + (1_B - f'(1_A))\,b^{-1}(1_B - f(1_A))\,.$$

Using the images under f of the orthogonality relations 8.8, as well as the fact that $(1_B - f(1_A))f(u^{-1}) = (1_B - f(1_A))f(1_A)f(u^{-1}) = 0$ and $f(v)(1_B - f(1_A)) = 0$, we have

$$\begin{aligned} c'c &= \Big(\sum_{\alpha\in\mathcal{P}(A)}\ \sum_{u\in U_\alpha} f'(u^{-1})j_\alpha f'(u)\Big) \\ &\qquad + (1_B - f'(1_A))\,b^{-1}(1_B - f(1_A))\,b\,(1_B - f'(1_A)) \\ &= f'\Big(\sum_{\alpha\in\mathcal{P}(A)}\ \sum_{u\in U_\alpha} u^{-1}e_\alpha u\Big) + (1_B - f'(1_A))^3 \\ &= f'(1_A) + (1_B - f'(1_A)) = 1_B\,. \end{aligned}$$

By a similar computation (or by Exercise 3.3), $cc' = 1_B$. Now we prove that $\mathrm{Inn}(c)f = f'$, which will establish the result. For $a \in A$, we compute $c^{-1}f(a)c = c^{-1}f(1_A)f(a)f(1_A)c$. In the expressions for c and c^{-1}, the terms $(1_B - f(1_A))\,b\,(1_B - f'(1_A))$ and $(1_B - f'(1_A))\,b^{-1}(1_B - f(1_A))$ cancel with $f(1_A)$. Moreover by the orthogonality relations 8.8, we obtain

$$\begin{aligned} c^{-1}f(a)c &= \Big(\sum_{\substack{\alpha\in\mathcal{P}(A)\\ u\in U_\alpha}} f'(u^{-1})j_\alpha f(u)\Big)\, f(a)\,\Big(\sum_{\substack{\beta\in\mathcal{P}(A)\\ v\in U_\beta}} f(v^{-1})j_\beta f'(v)\Big) \\ &= \sum_{\alpha,u}\sum_{\beta,v} f'(u^{-1})f(e_\alpha uav^{-1}e_\beta)f'(v) \\ &= \sum_{\alpha,u}\sum_{\beta,v} f'(u^{-1})f'(e_\alpha uav^{-1}e_\beta)f'(v) \\ &= \Big(\sum_{\alpha,u} f'(u^{-1})j_\alpha f'(u)\Big)\, f'(a)\,\Big(\sum_{\beta,v} f'(v^{-1})j_\beta f'(v)\Big) \\ &= f'(1_A)f'(a)f'(1_A) = f'(a)\,. \end{aligned}$$

We use that $e_\alpha uav^{-1}e_\beta = ee_\alpha uav^{-1}e_\beta e \in eAe = C$, so that f and f' coincide on this element. This completes the proof of (a).

(b) It is clear that $\mathcal{F}\mathcal{G}$ is an embedding if $\mathcal{F}$ is an embedding. Assume now that $\mathcal{F}\mathcal{G}$ is an embedding. Let $f \in \mathcal{F}$ and assume that $f(a) = 0$ for some $a \in A$. As in the proof of the first part, we have

$$0 = f(a) = f(1_A)f(a)f(1_A) = \sum_{\alpha,u}\sum_{\beta,v} f(u^{-1})f(e_\alpha uav^{-1}e_\beta)f(v)\,.$$

Multiplying by $f(e_\alpha u)$ on the left and by $f(v^{-1}e_\beta)$ on the right, and using the orthogonality relations 8.8, we obtain $f(e_\alpha uav^{-1}e_\beta) = 0$. Since $e_\alpha uav^{-1}e_\beta$ belongs to C and since fg (that is, the restriction of f to C) is injective, it follows that $e_\alpha uav^{-1}e_\beta = 0$ and so

$$a = 1_A\, a\, 1_A = \sum_{\alpha,u}\sum_{\beta,v} u^{-1}e_\alpha uav^{-1}e_\beta v = 0\,,$$

proving the injectivity of f. Now for $b \in B$, we have

$$\begin{aligned} f(1_A)b\,f(1_A) &= \sum_{\alpha,u}\sum_{\beta,v} f(u^{-1}e_\alpha u)\,b\,f(v^{-1}e_\beta v) \\ &= \sum_{\alpha,u}\sum_{\beta,v} f(u^{-1})f(e)f(e_\alpha u)\,b\,f(v^{-1}e_\beta)f(e)f(v)\,. \end{aligned}$$

Since $\mathcal{F}\mathcal{G}$ is an embedding, any element of $f(e)Bf(e)$ is in the image of the restriction of f to $eAe = C$. Thus we obtain that $f(1_A)b\,f(1_A)$ is in the image of f, and this completes the proof that $\mathcal{F}$ is an embedding. □

A practical way of verifying the assumption of the last proposition is the following.

(8.9) LEMMA. *Let $\mathcal{F} : A \to B$ be an embedding of $\mathcal{O}$-algebras. If there exists an embedding of B into a matrix algebra $M_n(A)$ over A (for some integer n), then A and B have the same number of points.*

Proof. By Proposition 8.5, $\mathcal{F}$ induces an injection $\mathcal{P}(A) \to \mathcal{P}(B)$. Similarly the other embedding induces an injection $\mathcal{P}(B) \to \mathcal{P}(M_n(A))$. Thus it suffices to prove that A and $M_n(A)$ have the same number of points. This follows either from Exercise 4.6 or from the Morita equivalence between A and $M_n(A)$ (see the next section and Exercise 9.4). □

Exercises

(8.1) Let A be an $\mathcal{O}$-algebra which is free as an $\mathcal{O}$-module and denote by $\pi : A \to A/J(A)$ the quotient map. Prove that there exists a unique exomorphism $\mathcal{F} : S \to A$ with the following properties:
(a) S is $\mathcal{O}$-semi-simple.
(b) f is injective for some $f \in \mathcal{F}$ (or equivalently for every $f \in \mathcal{F}$).
(c) πf is surjective for some $f \in \mathcal{F}$ (or equivalently for every $f \in \mathcal{F}$).

(8.2) Let m and n be two integers such that $m \leq n < 2m$.
(a) Prove that there is a unique non-zero exomorphism of $\mathcal{O}$-algebras $M_m(\mathcal{O}) \to M_n(\mathcal{O})$ and that it is an embedding.
(b) Prove that there are exactly two distinct non-zero exomorphisms of $\mathcal{O}$-algebras $M_m(\mathcal{O}) \to M_{2m}(\mathcal{O})$, that both are injective and that one of them is an embedding.
(c) Generalize to arbitrary integers.

(8.3) Let $\mathcal{F} : A \to B$ be an embedding of $\mathcal{O}$-algebras, let $\alpha \in \mathcal{P}(A)$ and let $\alpha' \in \mathcal{P}(B)$ be its image under the injection $\mathcal{P}(A) \to \mathcal{P}(B)$ of Proposition 8.5. Prove that for any $f \in \mathcal{F}$, we have $\mathfrak{m}_\alpha = f^{-1}(\mathfrak{m}_{\alpha'})$. Deduce that $\mathcal{F}$ induces an embedding of simple k-algebras $S(\alpha) \to S(\alpha')$, where $S(\alpha) = A/\mathfrak{m}_\alpha$ and $S(\alpha') = B/\mathfrak{m}_{\alpha'}$.

(8.4) Let $\mathcal{F} : A \to B$ be an embedding of k-algebras, let $\alpha, \beta \in \mathcal{P}(A)$ and let $\alpha', \beta' \in \mathcal{P}(B)$ be their images under the injection $\mathcal{P}(A) \to \mathcal{P}(B)$ of Proposition 8.5. Prove that the Cartan integers $c_{\alpha,\beta}$ and $c_{\alpha',\beta'}$ are equal. [Hint: Use Proposition 5.12.]

§ 9 MORITA EQUIVALENCE

We discuss in this section the basic properties of Morita equivalences and prove a simple criterion for the existence of a Morita equivalence. Recall that $\mathcal{O}$ is a ring satisfying Assumption 2.1 and that all modules are assumed to be finitely generated (left) modules. This assumption also applies to bimodules.

Let A and B be two $\mathcal{O}$-algebras. An (A,B)-*bimodule* is an abelian group M endowed with a left A-module structure and a right B-module structure, which coincide on restriction to $\mathcal{O}$ (that is, $(\lambda{\cdot}1_A)m = m(\lambda{\cdot}1_B)$ for every $\lambda \in \mathcal{O}$ and $m \in M$), and such that $(am)b = a(mb)$ for every $a \in A$, $b \in B$, $m \in M$.

Two $\mathcal{O}$-algebras A and B are said to be *Morita equivalent* if there exist a (B,A)-bimodule M, an (A,B)-bimodule N, an isomorphism of (A,A)-bimodules $\varepsilon : N \otimes_B M \to A$, and an isomorphism of (B,B)-bimodules $\eta : M \otimes_A N \to B$, such that the following two diagrams of isomorphisms commute.

$$\begin{array}{ccc} M \otimes_A N \otimes_B M & \xrightarrow{id_M \otimes \varepsilon} & M \otimes_A A \\ {\scriptstyle \eta\otimes id_M}\big\downarrow & & \big\downarrow{\scriptstyle \sim} \\ B \otimes_B M & \xrightarrow{\ \sim\ } & M \end{array}$$

(9.1)

$$\begin{array}{ccc} N \otimes_B M \otimes_A N & \xrightarrow{id_N \otimes \eta} & N \otimes_B B \\ {\scriptstyle \varepsilon\otimes id_N}\big\downarrow & & \big\downarrow{\scriptstyle \sim} \\ A \otimes_A N & \xrightarrow{\ \sim\ } & N \end{array}$$

In this situation there is an equivalence of categories between the category $\mathrm{mod}(A)$ of (left) A-modules and the category $\mathrm{mod}(B)$ of (left) B-modules, as follows. There are two functors

$$M \otimes_A - : \mathrm{mod}(A) \longrightarrow \mathrm{mod}(B)\,, \qquad V \mapsto M \otimes_A V\,,$$
$$N \otimes_B - : \mathrm{mod}(B) \longrightarrow \mathrm{mod}(A)\,, \qquad W \mapsto N \otimes_B W\,,$$

and for every A-module V and B-module W, there are natural isomorphisms

$$N \otimes_B M \otimes_A V \xrightarrow{\varepsilon\otimes id_V} A \otimes_A V \cong V\,,$$
$$M \otimes_A N \otimes_B W \xrightarrow{\eta\otimes id_W} B \otimes_B W \cong W\,.$$

These data show that the two functors $M \otimes_A -$ and $N \otimes_B -$ are inverse equivalences of categories. The detailed proof is left to the reader (Exercise 9.1). Note also that it follows easily from the definition that the Morita equivalence is an equivalence relation.

(9.2) REMARK. It is not necessary to assume that the additional condition 9.1 holds in order to get an equivalence of categories, but the condition can in fact always be realized for a suitable choice of the two isomorphisms ε and η (which are not unique). Indeed the two functors in an equivalence of categories are always left and right adjoint of each other (see Mac Lane [1971], § IV.4), and one can take ε and η to be the units and counits of the adjunctions. More precisely $\eta^{-1} \otimes id_W$ and $\varepsilon \otimes id_V$ are the unit and counit of one adjunction, and $\varepsilon^{-1} \otimes id_V$ and $\eta \otimes id_W$ are the unit and counit of the other adjunction. Any one of the two adjunction properties is then equivalent to the condition 9.1 (see Mac Lane [1971], § IV.1). Note also that the Morita theorem asserts that an equivalence between two module categories can be chosen to be of the above type; thus there is no limitation in defining a Morita equivalence in this way. The advantage of introducing the extra condition 9.1 lies in the next lemma. The lemma asserts that one can in fact suppress some redundancy in the definition.

(9.3) LEMMA. *Let A and B be two $\mathcal{O}$-algebras, let M be a (B,A)-bimodule, let N be an (A,B)-bimodule, let $\varepsilon : N \otimes_B M \to A$ be a homomorphism of (A,A)-bimodules, and let $\eta : M \otimes_A N \to B$ be a homomorphism of (B,B)-bimodules. Assume that ε and η are surjective and that the two diagrams 9.1 commute. Then ε and η are isomorphisms (so that A and B are Morita equivalent).*

Proof. By surjectivity of ε, we can write $1_A = \varepsilon(\sum_i n_i \otimes m_i)$, where $n_i \in N$ and $m_i \in M$. Let $\sum_j x_j \otimes y_j \in \mathrm{Ker}(\varepsilon)$, where $x_j \in N$ and $y_j \in M$. Multiplying this by 1_A, and using 9.1, we obtain:

$$\begin{aligned}
\sum_j x_j \otimes y_j &= (\sum_j x_j \otimes y_j)\, \varepsilon(\sum_i n_i \otimes m_i) \\
&= \sum_{i,j} x_j \otimes (y_j{\cdot}\varepsilon(n_i \otimes m_i)) = \sum_{i,j} x_j \otimes (\eta(y_j \otimes n_i){\cdot}m_i) \\
&= \sum_{i,j} (x_j{\cdot}\eta(y_j \otimes n_i)) \otimes m_i = \sum_{i,j} (\varepsilon(x_j \otimes y_j){\cdot}n_i) \otimes m_i \\
&= \varepsilon(\sum_j x_j \otimes y_j)\,(\sum_i n_i \otimes m_i) \;= 0\,.
\end{aligned}$$

This proves the injectivity of ε. The proof for η is similar. □

An equivalence of categories preserves all properties which are defined in categorical terms. For instance we mention the following results.

(9.4) PROPOSITION. *Let A and B be two Morita equivalent $\mathcal{O}$-algebras and assume that the equivalence is realized by a (B,A)-bimodule M and an (A,B)-bimodule N. Let V be an A-module and let $M \otimes_A V$ be the corresponding B-module.*

(a) V is zero if and only if $M \otimes_A V$ is zero.

(b) Let $S : 0 \to V \to V' \to V'' \to 0$ be a sequence of A-modules and let $M \otimes_A S : 0 \to M \otimes_A V \to M \otimes_A V' \to M \otimes_A V'' \to 0$ be the corresponding sequence of B-modules. Then S is exact if and only if $M \otimes_A S$ is exact. Moreover S splits if and only if $M \otimes_A S$ splits.

(c) V is simple if and only if $M \otimes_A V$ is simple.

(d) V is projective if and only if $M \otimes_A V$ is projective.

(e) V is indecomposable if and only if $M \otimes_A V$ is indecomposable.

(f) The partially ordered set of A-submodules of V is isomorphic to the partially ordered set of B-submodules of $M \otimes_A V$.

(g) The $\mathcal{O}$-algebras $\mathrm{End}_A(V)$ and $\mathrm{End}_B(M \otimes_A V)$ are isomorphic.

Proof. (a) If $M \otimes_A V = 0$, then $0 = N \otimes_B M \otimes_A V \cong A \otimes_A V \cong V$.

(b) We first show that the functor $M \otimes_A -$ preserves injections. Let $f : V \to V'$ be injective and let

$$W = \mathrm{Ker}(id_M \otimes f : M \otimes_A V \longrightarrow M \otimes_A V').$$

If $i : W \to M \otimes_A V$ denotes the inclusion, then $(id_M \otimes f)i = 0$. Applying $N \otimes_B -$, we see that the composite map $f(\varepsilon \otimes id_V)(id_N \otimes i)$ in the following diagram is zero.

$$\begin{array}{ccccc} N \otimes_B W & \xrightarrow{id_N \otimes i} & N \otimes_B M \otimes_A V & \xrightarrow{id_N \otimes id_M \otimes f} & N \otimes_B M \otimes_A V' \\ & & \downarrow{\scriptstyle \varepsilon \otimes id_V} & & \downarrow{\scriptstyle \varepsilon \otimes id_{V'}} \\ & & V & \xrightarrow{f} & V' \end{array}$$

But since f is injective and $\varepsilon \otimes id_V$ is an isomorphism, this implies that $id_N \otimes i = 0$. Applying now $M \otimes_A -$, we have a commutative diagram

$$\begin{array}{ccc} M \otimes_A N \otimes_B W & \xrightarrow{id_M \otimes id_N \otimes i} & M \otimes_A N \otimes_B M \otimes_A V \\ \downarrow{\scriptstyle \eta \otimes id_W} & & \downarrow{\scriptstyle \eta \otimes id_M \otimes id_V} \\ W & \xrightarrow{i} & M \otimes_A V \end{array}$$

with the top map equal to zero. Since $\eta \otimes id_W$ is an isomorphism, it follows that $i = 0$. This means that $W = 0$, proving the injectivity of $id_M \otimes f$.

Using cokernels instead of kernels, one can prove in a analogous fashion that the functor $M\otimes_A -$ preserves surjections. Similarly the functor $N\otimes_B -$ preserves injections and surjections.

Now assume that the sequence $0\to V\xrightarrow{f} V'\xrightarrow{g} V''\to 0$ is exact. Then $id_M\otimes f$ is injective by the above argument, and the composite in the sequence

$$M\otimes_A V\xrightarrow{id_M\otimes f} M\otimes_A V'\xrightarrow{id_M\otimes g} M\otimes_A V''$$

is zero, so that $\mathrm{Im}(id_M\otimes f)\subseteq K=\mathrm{Ker}(id_M\otimes g)$. Thus we have a sequence of maps

$$M\otimes_A V\xrightarrow{\ \overline{f}\ } K\xrightarrow{\ j\ } M\otimes_A V'\xrightarrow{id_M\otimes g} M\otimes_A V''$$

where $\overline{f}$ is the injection induced by $id_M\otimes f$ and j is the inclusion. Applying $N\otimes_B -$, which preserves injections, we have a sequence of maps

$$\begin{array}{ccccc} N\otimes_B M\otimes_A V & \xrightarrow{id_N\otimes\overline{f}} & N\otimes_B K & \xrightarrow{id_N\otimes j} & N\otimes_B M\otimes_A V' \\ & & & & \Big\downarrow{\scriptstyle id_N\otimes id_M\otimes g} \\ & & & & N\otimes_B M\otimes_A V'' \end{array}$$

the first two being injective, and the composite of the last two being zero. But the sequence

$$N\otimes_B M\otimes_A V\longrightarrow N\otimes_B M\otimes_A V'\longrightarrow N\otimes_B M\otimes_A V''$$

is exact (because it is isomorphic to $V\to V'\to V''$ via $\varepsilon\otimes -$). It follows that the image of $id_N\otimes j$ must be contained in the image of $id_{N\otimes M}\otimes f=(id_N\otimes j)(id_N\otimes\overline{f})$, or in other words that $id_N\otimes\overline{f}$ must be an isomorphism. Then $\overline{f}$ is an isomorphism too (because we recover $\overline{f}$ from $id_N\otimes\overline{f}$ by tensoring with M and applying the isomorphism $\eta\otimes -$). Since $\overline{f}$ is induced by $id_M\otimes f$, it follows that the image of $id_M\otimes f$ is equal to $K=\mathrm{Ker}(id_M\otimes g)$. This proves that the sequence

$$M\otimes_A V\to M\otimes_A V'\to M\otimes_A V''$$

is exact, as required.

The converse implication follows in a similar way by applying the functor $N\otimes_B -$, and then the isomorphism $\varepsilon\otimes -$. The proof of the additional statement about splitting is elementary and is left to the reader.

(c) V is not simple if and only if there exists a short exact sequence $0\to V'\to V\to V''\to 0$ with V' and V'' non-zero. Thus the statement is an immediate consequence of (a) and (b).

(d) V is projective if and only if every short exact sequence terminating in V splits. Thus the statement is an immediate consequence of (b).

(e) If $V = V' \oplus V''$, then $M \otimes_A V = (M \otimes_A V') \oplus (M \otimes_A V'')$. Moreover by (a), $M \otimes_A V'$ and $M \otimes_A V''$ are non-zero if V' and V'' are non-zero. The converse follows similarly by applying $N \otimes_B -$ and the isomorphism $\varepsilon \otimes -$.

The proof of (f) and (g) is left as an exercise for the reader. □

(9.5) COROLLARY. *A Morita equivalence between two $\mathcal{O}$-algebras A and B induces bijections* $\mathrm{Irr}(A) \xrightarrow{\sim} \mathrm{Irr}(B)$ *and* $\mathrm{Proj}(A) \xrightarrow{\sim} \mathrm{Proj}(B)$.

If M and N are bimodules realizing a Morita equivalence between two $\mathcal{O}$-algebras A and B, then it is elementary to check that $\overline{M} = M/\mathfrak{p}M$ and $\overline{N} = N/\mathfrak{p}N$ realize a Morita equivalence between the k-algebras $\overline{A} = A/\mathfrak{p}A$ and $\overline{B} = B/\mathfrak{p}B$ (by tensoring everything with k and using the isomorphism $k \otimes_{\mathcal{O}} M \cong M/\mathfrak{p}M$, and similarly with N, A and B). Now $\overline{A}$ and $\overline{B}$ are finite dimensional k-algebras (by our Convention 2.4), so that all finitely generated modules have finite composition lengths. By Proposition 9.4, the Morita equivalence preserves simple modules as well as short exact sequences. Thus by induction on the length of a composition series, we deduce that the composition factors of an $\overline{A}$-module V are mapped by the equivalence to the composition factors of the $\overline{B}$-module $\overline{M} \otimes_{\overline{A}} V$.

We now apply this fact to the multiplicities of composition factors of indecomposable projective modules and we obtain that the Cartan integer $c_{\alpha,\beta}$, associated with two simple $\overline{A}$-modules $V(\alpha)$ and $V(\beta)$, is equal to the Cartan integer associated with the corresponding simple $\overline{B}$-modules $\overline{M} \otimes_{\overline{A}} V(\alpha)$ and $\overline{M} \otimes_{\overline{A}} V(\beta)$. The Cartan matrix of $\overline{A}$ is indexed by $\mathrm{Irr}(\overline{A}) \times \mathrm{Irr}(\overline{A})$ and similarly for $\overline{B}$. In the following result, we use the implicit convention that the index set for the Cartan matrix of $\overline{A}$ corresponds to the index set for the Cartan matrix of $\overline{B}$ under the bijection induced by the Morita equivalence.

(9.6) COROLLARY. *If two $\mathcal{O}$-algebras A and B are Morita equivalent, then $A/\mathfrak{p}A$ and $B/\mathfrak{p}A$ are Morita equivalent and the Cartan matrices of $A/\mathfrak{p}A$ and $B/\mathfrak{p}A$ are equal.*

Another important property is that a Morita equivalence preserves centres.

(9.7) PROPOSITION. *If two $\mathcal{O}$-algebras A and B are Morita equivalent, then the centres $Z(A)$ and $Z(B)$ are isomorphic $\mathcal{O}$-algebras.*

Proof. We first show that $Z(A)$ is isomorphic to the ring $\mathrm{Nat}(A)$ of natural transformations between the identity functor $id_{\mathrm{mod}(A)}$ and itself. If $a \in Z(A)$, then multiplication by a is a natural transformation between $id_{\mathrm{mod}(A)}$ and itself. Indeed it is elementary to check that for any A-module V, the map $v \mapsto a{\cdot}v$ is a homomorphism of A-modules (because a is central), and that it is a natural transformation. Conversely let ϕ be any natural transformation between $id_{\mathrm{mod}(A)}$ and itself, given by maps $\phi_V : V \to V$ for each A-module V. Choosing $V = A$, we define $a = \phi_A(1_A) \in A$. Then for any A-module V and $v \in V$, consider the homomorphism of A-modules $f : A \to V$ mapping 1_A to v. By naturality of ϕ, we have

$$\phi_V(v) = \phi_V(f(1_A)) = f(\phi_A(1_A)) = f(a) = a{\cdot}v\,.$$

It follows that ϕ coincides with the multiplication by a. In particular a is central because for any $b \in A$, we have

$$ab = \phi_A(b) = \phi_A(b{\cdot}1_A) = b\,\phi_A(1_A) = ba\,.$$

This completes the proof that $Z(A) \cong \mathrm{Nat}(A)$. In particular $\mathrm{Nat}(A)$ is endowed with an $\mathcal{O}$-algebra structure.

Now since A and B are Morita equivalent, there exist bimodules M and N such that the functors $M \otimes_A -$ and $N \otimes_B -$ are inverse equivalences. We use these functors to construct an isomorphism between $\mathrm{Nat}(A)$ and $\mathrm{Nat}(B)$. If $\phi \in \mathrm{Nat}(A)$, then we define $\psi \in \mathrm{Nat}(B)$ by setting

$$\psi_W = (\eta \otimes id_W)(id_M \otimes \phi_{N\otimes W})(\eta^{-1} \otimes id_W)\,.$$

We clearly obtain an $\mathcal{O}$-algebra homomorphism

$$\mathrm{Nat}(A) \longrightarrow \mathrm{Nat}(B)\,, \quad \phi \mapsto \psi\,.$$

It is an easy exercise to check that this is an isomorphism. In fact one can use condition 9.1 to check that the inverse isomorphism maps ψ to ϕ, where ϕ is defined by $\phi_V = (\varepsilon \otimes id_V)(id_N \otimes \psi_{M\otimes V})(\varepsilon^{-1} \otimes id_V)$. Details are left to the reader. □

(9.8) COROLLARY. *If two commutative $\mathcal{O}$-algebras are Morita equivalent, then they are isomorphic.*

Having discussed properties of Morita equivalences, we now come to the question of the existence of a Morita equivalence. A very simple and useful condition is provided by the following result.

(9.9) THEOREM. *Let* A *be an* $\mathcal{O}$*-algebra and let* e *be an idempotent of* A *. The following conditions are equivalent.*
(a) eAe *and* A *are Morita equivalent.*
(b) eAe *and* A *have the same number of points.*
(c) $AeA = A$ *, where* AeA *denotes the ideal generated by* e *.*

Proof. (a) $\Rightarrow$ (b). By Corollary 9.5, $\mathrm{Irr}(eAe)$ and $\mathrm{Irr}(A)$ are in bijection. By Theorem 4.3, $\mathcal{P}(A)$ is in bijection with $\mathrm{Irr}(A)$ (and similarly with eAe). Therefore eAe and A have the same number of points.

(b) $\Rightarrow$ (c). By Proposition 4.12, the inclusion $eAe \to A$ induces an injection $\mathcal{P}(eAe) \to \mathcal{P}(A)$. Since both sets are finite, (b) means that the map is bijective. Thus if $\alpha \in \mathcal{P}(A)$, there exists $i \in \alpha$ such that $i \in eAe$, so that i belongs to the ideal AeA . Thus AeA is not contained in the maximal ideal $\mathfrak{m}_\alpha$ (Corollary 4.10). Since this holds for every maximal ideal $\mathfrak{m}_\alpha$ of A , we have $AeA = A$.

(c) $\Rightarrow$ (a). Consider the (eAe, A)-bimodule eA and similarly the (A, eAe)-bimodule Ae . There is an isomorphism of (eAe, eAe)-bimodules (which does not depend on the assumption)

$$\eta : eA \otimes_A Ae \longrightarrow eAe \,, \qquad \eta(a \otimes a') = aa'$$

whose inverse maps $b \in eAe$ to $b \otimes e$ (note that we have $b \otimes e = eb \otimes e = e \otimes be = e \otimes b$). Consider the (A, A)-linear map

$$\varepsilon : Ae \otimes_{eAe} eA \longrightarrow A \,, \qquad \varepsilon(a \otimes a') = aa' \,.$$

The image of ε is equal to the ideal AeA , which is the whole of A by assumption. Thus ε is surjective. Finally condition 9.1 is trivially satisfied, for it comes down to the associativity of multiplication in A . By Lemma 9.3, eAe and A are Morita equivalent. □

One can construct explicitly the inverse of the map ε in the above proof, using the fact that eAe and A have the same number of points (Exercise 9.6). This provides in fact a direct proof that (b) implies (a).

It should be noted that, in the above theorem, the Morita equivalence between A and eAe maps an A-module V to the eAe-module eV , which is a direct summand of V . Indeed the equivalence is realized by the (eAe, A)-bimodule eA , and we have an isomorphism $eA \otimes_A V \cong eV$.

We have seen before that an embedding which preserves the number of points is not far from an isomorphism in the sense that it is both a monomorphism and an epimorphism. Theorem 9.9 shows that it is not far from an isomorphism in another sense: it induces a Morita equivalence.

(9.10) COROLLARY. *Let* $\mathcal{F}: B \to A$ *be an embedding of* $\mathcal{O}$*-algebras and assume that* A *and* B *have the same number of points. Then* A *and* B *are Morita equivalent.*

Proof. By definition of an embedding, $B \cong eAe$ for some idempotent e of A. □

Any $\mathcal{O}$-algebra A clearly embeds in $M_n(A)$ and they have the same number of points (Exercise 4.6). Thus Corollary 9.10 shows in particular that A and $M_n(A)$ are always Morita equivalent. However, this can be shown more directly (Exercise 9.4). More generally we have the following useful characterization of Morita equivalences.

(9.11) THEOREM. *Let* A *and* B *be two* $\mathcal{O}$*-algebras. The following conditions are equivalent.*

(a) A *and* B *are Morita equivalent.*

(b) There exist embeddings $A \to M_m(B)$ *and* $B \to M_n(A)$ *for some positive integers* m *and* n *.*

Proof. (a) $\Rightarrow$ (b). Suppose that A and B are Morita equivalent and that the equivalence is realized by a (B, A)-bimodule M and an (A, B)-bimodule N. As a B-module, M is isomorphic to the image $M \otimes_A A$ of the A-module A under the equivalence. It follows that $\mathrm{End}_B(M) \cong \mathrm{End}_A(A)$ and this is isomorphic to A^{op} (Proposition 5.11). On the other hand M is a projective B-module (because A is a projective A-module), so that $M \oplus Q = B^m$ for some B-module Q and some integer m. Therefore the $\mathcal{O}$-algebra $\mathrm{End}_B(M) \cong A^{op}$ embeds into $\mathrm{End}_B(B^m)$, which is isomorphic to $M_m(\mathrm{End}_B(B)) \cong M_m(B^{op})$. Consequently A^{op} embeds into $M_m(B^{op})$ and so A embeds into $M_m(B)$. The same argument using the other bimodule N shows that B embeds into $M_n(A)$ for some n.

(b) $\Rightarrow$ (a). The embedding $A \to M_m(B)$ induces an injective map $\mathcal{P}(A) \to \mathcal{P}(M_m(B))$. Therefore, since B and $M_m(B)$ have the same number of points (Exercise 4.6), we have $|\mathcal{P}(A)| \leq |\mathcal{P}(B)|$. Similarly $|\mathcal{P}(B)| \leq |\mathcal{P}(A)|$, so that $|\mathcal{P}(A)| = |\mathcal{P}(B)| = |\mathcal{P}(M_m(B))|$. We now have an embedding $A \to M_m(B)$ with the same number of points, so that A is Morita equivalent to $M_m(B)$ by Corollary 9.10. It follows that A is Morita equivalent to B since B is always Morita equivalent to $M_m(B)$. □

Exercises

(9.1) Provide the details of the proof that if A and B are Morita equivalent, then the categories $\mathrm{mod}(A)$ and $\mathrm{mod}(B)$ are equivalent.

(9.2) Complete the proof of Proposition 9.4.

(9.3) If A is an $\mathcal{O}$-algebra, let $\mathrm{Nat}(A)$ be the ring of natural transformations between the identity functor $id_{\mathrm{mod}(A)} : \mathrm{mod}(A) \to \mathrm{mod}(A)$ and itself. Complete the proof of Proposition 9.7 by showing that if A and B are Morita equivalent, then $\mathrm{Nat}(A)$ and $\mathrm{Nat}(B)$ are isomorphic.

(9.4) For any $\mathcal{O}$-algebra A, prove directly that A and $M_n(A)$ are Morita equivalent by constructing suitable bimodules.

(9.5) Let A be an $\mathcal{O}$-algebra and let $S \cong \mathrm{End}_{\mathcal{O}}(L)$ be an $\mathcal{O}$-simple algebra.

(a) Prove that $S \otimes_{\mathcal{O}} A$ is Morita equivalent to A, via the functor mapping an A-module M to the $S \otimes_{\mathcal{O}} A$-module $L \otimes_{\mathcal{O}} M$. [Hint: Remember that $L \cong Se$ where e is a primitive idempotent of S, and use the idempotent $e \otimes 1_A$. Compare with Proposition 7.6.]

(b) Prove the assertions made in Remark 7.7.

(9.6) The purpose of this exercise is to construct the inverse of the map ε appearing in the proof of Theorem 9.9, providing a direct proof that (b) implies (a). We assume that eAe and A have the same number of points.

(a) Prove that there exists a primitive decomposition of the unity element

$$1_A = \sum_{\alpha \in \mathcal{P}(A)} \sum_{u \in U_\alpha} u^{-1} i_\alpha u ,$$

where $i_\alpha \in \alpha \cap eAe$, and U_α is a finite set of invertible elements of A (for each point $\alpha \in \mathcal{P}(A)$). Moreover the elements $u^{-1} i_\alpha u$ satisfy the orthogonality relations 8.8. [Hint: Use the argument of the beginning of the proof of Proposition 8.7.]

(b) Consider the map

$$A \longrightarrow Ae \otimes_{eAe} eA , \qquad a \mapsto \sum_{\alpha \in \mathcal{P}(A)} \sum_{u \in U_\alpha} u^{-1} i_\alpha \otimes i_\alpha u a .$$

Prove that this is the inverse of the map ε of Theorem 9.9.

(9.7) Let A and B be two Morita equivalent $\mathcal{O}$-algebras.

(a) Provide the details of the proof that $k \otimes_{\mathcal{O}} A$ and $k \otimes_{\mathcal{O}} B$ are Morita equivalent.

(b) Suppose that $\mathcal{O}$ is a domain and let K be the field of fractions of $\mathcal{O}$. Prove that $K \otimes_{\mathcal{O}} A$ and $K \otimes_{\mathcal{O}} B$ are Morita equivalent.

(c) Generalize to an arbitrary ring homomorphism $\mathcal{O} \to \mathcal{O}'$.

Notes on Chapter 1

As most of the results of this chapter are standard, we leave to the historian the task of attributing them to the right mathematicians. We just mention a few facts. The idea of working systematically with points rather than primitive idempotents, and with exomorphisms and embeddings rather than homomorphisms, is due to Puig [1981]. Our treatment is also inspired by Puig [1984]. The existence of maximal $\mathcal{O}$-semi-simple algebras (Theorem 7.3) is a version of the Wedderburn–Malcev theorem, but our approach is taken from Puig [1981]. For the Morita theorem (mentioned in Remark 9.2), a short proof can be found in Benson [1991], and a detailed discussion appears in Curtis–Reiner [1981].

CHAPTER 2

G-algebras and pointed groups

We introduce in this chapter a finite group G acting on an $\mathcal{O}$-algebra and we develop the main concepts and their properties: G-algebras, interior G-algebras, the Brauer homomorphism, pointed groups, local pointed groups, associated embeddings, the containment relation between pointed groups, and relative projectivity. We continue with our assumption that $\mathcal{O}$ is a commutative complete local noetherian ring with an algebraically closed residue field k of characteristic p. We postpone until Chapter 8 the task of dropping hypotheses and generalizing some of the notions. Throughout this chapter and for the rest of this book, G denotes a finite group.

§ 10 EXAMPLES OF G-ALGEBRAS AND INTERIOR G-ALGEBRAS

The main concept of this book is introduced in this section, together with important examples.

A *G-algebra* (or more precisely a G-algebra over $\mathcal{O}$) is a pair (A, ψ) where A is an $\mathcal{O}$-algebra and $\psi : G \to \mathrm{Aut}(A)$ is a group homomorphism. Here $\mathrm{Aut}(A)$ denotes the group of $\mathcal{O}$-algebra automorphisms of A. As usual we only write A instead of (A, ψ) to denote a G-algebra. Equivalently one can define a G-algebra to be an $\mathcal{O}$-algebra endowed with an action of G by algebra automorphisms. The (left) action $\psi(g)$ of $g \in G$ on A will always be written $\psi(g)(a) = {}^g a$ for $a \in A$. Thus the temporary notation ψ will never be used. If A and B are G-algebras, a map $f : A \to B$ is called a *homomorphism of G-algebras* if it is a homomorphism of $\mathcal{O}$-algebras such that $f({}^g a) = {}^g(f(a))$ for all $g \in G$ and $a \in A$. We recall that we do not require f to be unitary.

The following definition will turn out to be even more important than the previous one. An *interior G-algebra* is a pair (A, ϕ) where A is an $\mathcal{O}$-algebra and $\phi : G \to A^*$ is a group homomorphism. Since there is a canonical group homomorphism $A^* \to \mathrm{Aut}(A)$ mapping a to the inner automorphism $\mathrm{Inn}(a)$, any interior G-algebra is in particular a G-algebra. In other words $g \in G$ acts on A via the inner automorphism $\mathrm{Inn}(\phi(a))$ (and this is the origin of the terminology). Note that a G-algebra may have several different interior G-algebra structures, or no such structure (Exercise 10.1). Again the notation ϕ is never used and is replaced by the following one: for every $a \in A$ and $g \in G$, we define

$$g \cdot a = \phi(g)a \qquad \text{and} \qquad a \cdot g = a\phi(g) .$$

Thus we see that we obtain a left $\mathcal{O}$-linear action as well as a right $\mathcal{O}$-linear action of G on A and the associativity of the multiplication in A implies that these two actions commute. The G-algebra structure then corresponds to the conjugation action ${}^g a = g \cdot a \cdot g^{-1}$. The group homomorphism ϕ is recovered from the latter notation via $\phi(g) = g \cdot 1_A = 1_A \cdot g$. Note that we do not require ϕ to be injective so that $g \cdot 1_A$ can be equal to 1_A. Thus g should not be identified with its image $g \cdot 1_A$ in A (despite the fact that the terminology may suggest that the group G can be found in the interior of A). We shall always use a dot to denote the left and the right action of G on A, but we shall usually not write a dot for the multiplication in A. It is clear that for all $g, h \in G$ and $a, b \in A$, we have

$$(10.1) \qquad \begin{array}{ll} (g \cdot a) \cdot h = g \cdot (a \cdot h) , & g \cdot 1_A = 1_A \cdot g , \\ g \cdot (ab) = (g \cdot a)b , & (ab) \cdot g = a(b \cdot g) , \end{array}$$

and also simply

$$(a \cdot g)b = a(g \cdot b)\,. \tag{10.2}$$

Conversely, given an $\mathcal{O}$-algebra A endowed with a left $\mathcal{O}$-linear action and a right $\mathcal{O}$-linear action of G which satisfy either the relations 10.1 or the relations 10.2, then the map $g \mapsto g \cdot 1_A = 1_A \cdot g$ defines an interior G-algebra structure on A (see Exercise 10.2).

If A and B are interior G-algebras, a map $f : A \to B$ is called a *homomorphism of interior G-algebras* if it is a homomorphism of $\mathcal{O}$-algebras such that $f(g \cdot a) = g \cdot f(a)$ and $f(a \cdot g) = f(a) \cdot g$ for all $g \in G$ and $a \in A$. Note that this is equivalent to requiring that $f(1_A)$ is fixed under the conjugation action of G and that $f(g \cdot 1_A) = g \cdot f(1_A)$ for all $g \in G$ (Exercise 10.3). However, since we do not require algebra homomorphisms to preserve unity elements, we emphasize that the composite map $G \to A \xrightarrow{f} B$ is not the structural map of the interior G-algebra B (unless f is unitary). Of course any homomorphism of interior G-algebras is in particular a homomorphism of G-algebras.

The relevance of the concept of interior G-algebra as opposed to that of G-algebra will become clear later. For the time being, we shall work with arbitrary G-algebras. If H is a subgroup of G, then any G-algebra A can be viewed as an H-algebra by restriction. This H-algebra will be written $\mathrm{Res}^G_H(A)$, in order to always make clear which group is considered as acting on the algebra. The same notation will be used for the restriction of interior G-algebras. Given two G-algebras A and B, the tensor product $A \otimes_{\mathcal{O}} B$ is an $\mathcal{O}$-algebra which carries a G-algebra structure: the action of $g \in G$ is given by ${}^g(a \otimes b) = {}^g a \otimes {}^g b$. In case A and B are interior G-algebras, then so is $A \otimes_{\mathcal{O}} B$, via the map $G \to (A \otimes B)^*$, $g \mapsto (g \cdot 1_A) \otimes (g \cdot 1_B)$. The opposite algebra A^{op} of a G-algebra A is clearly again a G-algebra, and is interior if A is interior.

If H is a subgroup of G, if A is an H-algebra, and if $g \in G$, we define the *conjugate* algebra ${}^g A$ to be the ${}^g H$-algebra which is equal to A as an $\mathcal{O}$-algebra and which is endowed with the action of ${}^g H$ defined by $(x, a) \mapsto {}^{(g^{-1}xg)}a$ (where $x \in {}^g H$ and $a \in A$). In other words the structural group homomorphism ${}^g H \to \mathrm{Aut}({}^g A)$ is obtained by composing the conjugation by g^{-1} with the structural homomorphism $H \to \mathrm{Aut}(A)$. Note that if H is a normal subgroup of G (or more precisely if g normalizes H), then ${}^g A$ is again an H-algebra. Similarly, if A is an interior H-algebra, the *conjugate* algebra ${}^g A$ is the interior ${}^g H$-algebra obtained by composing the conjugation by g^{-1} with the structural homomorphism $H \to A^*$.

(10.3) EXAMPLE: Group algebras.
Consider the group algebra $A = \mathcal{O}G$, namely the free $\mathcal{O}$-module on the basis G, endowed with the product which extends $\mathcal{O}$-bilinearly the product of group elements. We identify the group G with the basis of $\mathcal{O}G$. The canonical inclusion $G \to (\mathcal{O}G)^*$ obviously makes $\mathcal{O}G$ into an interior G-algebra. For an arbitrary interior G-algebra A, the structural map $G \to A^*$ extends uniquely by $\mathcal{O}$-linearity to a homomorphism of interior G-algebras $\phi : \mathcal{O}G \to A$. In fact an interior G-algebra can be defined to be an $\mathcal{O}$-algebra A endowed with a unitary algebra homomorphism $\phi : \mathcal{O}G \to A$. Then ϕ is obviously a unitary homomorphism of interior G-algebras and is unique with this property. Thus interior G-algebras can be viewed as those algebras which are directly connected with the group algebra via a homomorphism. An important property of group algebras is Maschke's theorem, which asserts that the group algebra kG is semi-simple if and only if p does not divide the order of the group G. If one works over $\mathcal{O}$ rather than k, one has to replace semi-simplicity by $\mathcal{O}$-semi-simplicity. We shall return to this in Section 17. We emphasize however that the purpose of modular representation theory is to study the case where p divides $|G|$.

(10.4) EXAMPLE: Twisted group algebras.
These algebras arise when a central extension is given as follows:

$$1 \longrightarrow \mathcal{O}^* \xrightarrow{\phi} \widehat{G} \xrightarrow{\pi} G \longrightarrow 1 .$$

Thus $\widehat{G}$ is a group having a central subgroup $\phi(\mathcal{O}^*)$ isomorphic to the multiplicative group $\mathcal{O}^*$ of the ring $\mathcal{O}$, and the quotient $\widehat{G}/\phi(\mathcal{O}^*)$ is isomorphic to G. We define the *twisted group algebra* $\mathcal{O}_\sharp\widehat{G}$ to be

$$\mathcal{O}_\sharp\widehat{G} = \mathcal{O} \otimes_{\mathcal{O}[\mathcal{O}^*]} \mathcal{O}\widehat{G} ,$$

where $\mathcal{O}\widehat{G}$ denotes the group algebra of the infinite group $\widehat{G}$ and $\mathcal{O}[\mathcal{O}^*]$ is the group algebra of the group $\mathcal{O}^*$. Here $\mathcal{O}[\mathcal{O}^*]$ acts on the left on $\mathcal{O}\widehat{G}$ via ϕ and acts on the right on $\mathcal{O}$ via the inclusion $\mathcal{O}^* \to \mathcal{O}$. More explicitly, $\mathcal{O}_\sharp\widehat{G}$ is isomorphic to the quotient of $\mathcal{O}\widehat{G}$ by the ideal I generated by the elements $\phi(\lambda) - \lambda \cdot 1$, where $\lambda \in \mathcal{O}^*$. Thus the central subgroup $\phi(\mathcal{O}^*) \cong \mathcal{O}^*$ is identified with the scalars $\mathcal{O}^*$ of the group algebra. Multiplying the generators of I by arbitrary elements $x \in \widehat{G}$, we see that I is the $\mathcal{O}$-linear span of the elements $\phi(\lambda)\, x - \lambda \cdot x$, where $\lambda \in \mathcal{O}^*$ and $x \in \widehat{G}$. Thus if $\sigma : G \to \widehat{G}$ is a map such that $\sigma\pi = id_G$ (so that $\{\sigma(x) \mid x \in G\}$ is a set of representatives of the cosets $\widehat{G}/\phi(\mathcal{O}^*)$), then the images of the elements $\sigma(x)$, for $x \in G$, form a basis of the algebra $\mathcal{O}_\sharp\widehat{G}$. Therefore

$\mathcal{O}_\sharp\widehat{G}$ has a basis indexed by the elements of G. The product of two basis elements is not (in general) the corresponding product of group elements, but is modified by a scalar in $\mathcal{O}^*$; indeed $\sigma(xy) = \lambda(x,y)\,\sigma(x)\sigma(y)$ for some $\lambda(x,y) \in \mathcal{O}^*$. In particular we see that $\mathcal{O}_\sharp\widehat{G}$ is an $\mathcal{O}$-algebra satisfying our convention 2.4 (that is, it is finitely generated over $\mathcal{O}$), and moreover it is a G-algebra: the action of $g \in G$ is by definition the conjugation by $\sigma(g)$. This is well-defined since $\sigma(g)$ is defined up to a central element of $\widehat{G}$ (which is mapped to a scalar in $\mathcal{O}_\sharp\widehat{G}$). When the central extension above splits (so that $\widehat{G} \cong \mathcal{O}^* \times G$), then we can choose σ to be a group homomorphism and it follows that $\mathcal{O}_\sharp\widehat{G}$ is isomorphic to the ordinary group algebra $\mathcal{O}G$ (but there are in general several such isomorphisms, unless G is perfect or G is a p-group and $\mathcal{O} = k$). As in the case of group algebras, one can show that $\mathcal{O}_\sharp\widehat{G}$ is semi-simple if p does not divide $|G|$ (see Section 17).

Note that $\mathcal{O}_\sharp\widehat{G}$ is in general not an interior G-algebra, unless the algebra happens to be isomorphic to the ordinary group algebra. However, $\mathcal{O}_\sharp\widehat{G}$ can be given an interior structure over $\widehat{G}$ since $\widehat{G}$ maps to $(\mathcal{O}_\sharp\widehat{G})^*$. This is an obvious extension of the definition of an interior algebra to the case of infinite groups. More generally, whenever there is a unitary algebra homomorphism $\mathcal{O}_\sharp\widehat{G} \to A$, then A is an interior $\widehat{G}$-algebra. This structure is not arbitrary since the subgroup $\mathcal{O}^*$ of $\widehat{G}$ maps to the scalars of A^* by the identity. We shall only occasionally refer to interior $\widehat{G}$-algebras, but they will always be of this special type.

Finally we show that $\mathcal{O}_\sharp\widehat{G}$ is a symmetric algebra. As above, let $\{\,\sigma(x) \mid x \in G\,\}$ be an $\mathcal{O}$-basis of $\mathcal{O}_\sharp\widehat{G}$, with $\sigma(xy) = \lambda(x,y)\sigma(x)\sigma(y)$ for some $\lambda(x,y) \in \mathcal{O}^*$. We choose $\sigma(1) = 1$, from which it follows that $\lambda(x,x^{-1}) = \lambda(x^{-1},x)$ (by computing $\sigma(x)\sigma(x^{-1})\sigma(x)$). Define an $\mathcal{O}$-linear map

$$\mu : \mathcal{O}_\sharp\widehat{G} \longrightarrow \mathcal{O}\,, \qquad \mu(\sigma(x)) = \begin{cases} 1 & \text{if } x = 1, \\ 0 & \text{if } x \neq 1. \end{cases}$$

Then $\mu(\sigma(x)\sigma(y)) = 0 = \mu(\sigma(y)\sigma(x))$ if $y \neq x^{-1}$ and

$$\mu(\sigma(x)\sigma(x^{-1})) = \lambda(x,x^{-1}) = \lambda(x^{-1},x) = \mu(\sigma(x^{-1})\sigma(x))\,.$$

Thus μ is symmetric. The unimodularity condition follows from the fact that $\{\,\sigma(x)^{-1} \mid x \in G\,\}$ is the dual basis of the above basis (note that $\sigma(x)^{-1} = \lambda(x,x^{-1})^{-1}\sigma(x^{-1})$).

We now show that any twisted group algebra over k is in fact a quotient of the ordinary group algebra of a finite group.

(10.5) PROPOSITION. *Let* $\widehat{G}$ *be a central extension of* G *by* k^* *and let* $k_\sharp\widehat{G}$ *be the corresponding twisted group algebra. Then there exists a central extension of finite groups* $1 \to Z \to F \to G \to 1$, *with* Z *cyclic of order prime to* p, *such that* $k_\sharp\widehat{G}$ *is isomorphic to a quotient of the group algebra* kF. *More precisely* $k_\sharp\widehat{G} \cong kFe$ *for some central idempotent* e *of* kF.

Proof. Let $n = |G|$ be the order of the group G, and consider the map $\phi : k^* \to k^*$ defined by $\phi(\lambda) = \lambda^n$. This is a surjective group homomorphism because k is algebraically closed by Assumption 2.1. The kernel Z of ϕ consists of all n-th roots of unity in k^*, but since a field of characteristic p has no non-trivial p^r-th root of unity (for any $r \geq 1$), Z consists of m-th roots of unity where m is the part of n of order prime to p (that is, $n = mp^r$ where m is not divisible by p). Thus Z is cyclic of order m.

We use some standards facts from the cohomology theory of groups, which are recalled in Proposition 1.18. Consider k^* as a trivial G-module. For every positive integer q, the automorphism ϕ induces an automorphism ϕ_* of the cohomology group $H^q(G, k^*)$, and ϕ_* is multiplication by n in this abelian group (in additive notation). Therefore $\phi_* = 0$ since the order of the group annihilates $H^q(G, k^*)$. Associated with the exact sequence $1 \to Z \xrightarrow{\eta} k^* \xrightarrow{\phi} k^* \to 1$, there is a long exact sequence of group cohomology, and a portion of this sequence is

$$H^2(G, Z) \xrightarrow{\eta_*} H^2(G, k^*) \xrightarrow{0} H^2(G, k^*),$$

so that the map $\eta_* : H^2(G, Z) \to H^2(G, k^*)$ is surjective.

Now $H^2(G, k^*)$ classifies the central extensions with kernel k^* and quotient group G (the extensions are central because we consider the trivial action of G on k^*). Let $c \in H^2(G, k^*)$ be the cohomology class associated with the given central extension $\widehat{G}$. By surjectivity of η_*, there exists a class $d \in H^2(G, Z)$ such that $\eta_*(d) = c$, and d corresponds in turn to a central extension $1 \to Z \to F \to G \to 1$. As both Z and G are finite, F is finite too. From the construction of a central extension associated with a cohomology class, the equation $\eta_*(d) = c$ means that there is a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & Z & \longrightarrow & F & \longrightarrow & G & \longrightarrow & 1 \\ & & {\scriptstyle\eta}\big\downarrow & & {\scriptstyle\tau}\big\downarrow & & {\scriptstyle id}\big\downarrow & & \\ 1 & \longrightarrow & k^* & \longrightarrow & \widehat{G} & \longrightarrow & G & \longrightarrow & 1. \end{array}$$

The group homomorphism $\tau : F \to \widehat{G}$ induces an algebra homomorphism $\tau : kF \to k\widehat{G}$, and since by construction $k_\sharp\widehat{G}$ is a quotient of $k\widehat{G}$, we obtain by composition an algebra homomorphism $\overline{\tau} : kF \to k_\sharp\widehat{G}$. If $\{\sigma(g) \mid g \in G\}$ is a set of representatives of $F/Z \cong G$ in F, then $\{\tau(\sigma(g)) \mid g \in G\}$ is a set of representatives of G in $\widehat{G}$, and therefore $\{\overline{\tau}(\sigma(g)) \mid g \in G\}$ is a basis of the twisted group algebra $k_\sharp\widehat{G}$. This shows that $\overline{\tau}$ is surjective and completes the proof of the first statement.

We only sketch the proof of the second more precise statement and leave the details to the reader. The element

$$e = \frac{1}{|Z|} \sum_{z \in Z} \eta(z^{-1}) z$$

is a central idempotent of kF, so that $kF \cong kFe \times kF(1-e)$. Moreover $\overline{\tau}(e) = 1$ (by construction of $k_\sharp\widehat{G}$ as a quotient of $k\widehat{G}$) and we obtain by restriction a surjection $\overline{\tau} : kFe \to k_\sharp\widehat{G}$. In order to show that this is an isomorphism, it suffices to note that $\{\sigma(g)e \mid g \in G\}$ is a basis of kFe (because for every $z \in Z$ we have $ze = \lambda e$ for some $\lambda \in k^*$). $\square$

Note that the group homomorphism $\tau : F \to \widehat{G}$ is injective, so that F can be identified with a finite subgroup of $\widehat{G}$. The above result is in fact a consequence of the much more precise theory of the Schur multiplier, but only this special case will be used in this text.

(10.6) EXAMPLE: Modules over group algebras.
We recall our convention that an $\mathcal{O}G$-module is always finitely generated. Since G is finite, it is equivalent to require that the module is finitely generated as an $\mathcal{O}$-module (because the set of all translates by the action of G of a set of generators over $\mathcal{O}G$ is a set of generators over $\mathcal{O}$). Recall also that an $\mathcal{O}G$-module comes down to the same thing as an $\mathcal{O}$-module M together with a group homomorphism $\rho : G \to \mathrm{Aut}_{\mathcal{O}}(M)$, that is, a *representation* of G over $\mathcal{O}$. If $A = \mathrm{End}_{\mathcal{O}}(M)$, the group homomorphism $\rho : G \to \mathrm{Aut}_{\mathcal{O}}(M) = A^*$ makes the algebra A into an interior G-algebra. This is our second important example.

If $M = \mathcal{O}$ with trivial action of G (that is, every $g \in G$ acts as the identity), then one obtains the *trivial* $\mathcal{O}G$-module and the corresponding interior G-algebra is also called *trivial*. If $\mathcal{O} = k$ is a field, then the representation $\rho : G \to \mathrm{Aut}_k(M)$ is called *irreducible* if the corresponding kG-module M is simple.

Instead of arbitrary $\mathcal{O}G$-modules, we shall usually only work with $\mathcal{O}G$-lattices. An *$\mathcal{O}G$-lattice* is defined to be an $\mathcal{O}G$-module which is free as an $\mathcal{O}$-module. In that case the algebra $A = \mathrm{End}_{\mathcal{O}}(M)$ is isomorphic to a matrix algebra over $\mathcal{O}$ (that is, A is $\mathcal{O}$-simple) and we have a representation of G as a group of matrices over $\mathcal{O}$. There are two cases of interest: either $\mathcal{O} = k$ is an (algebraically closed) field of characteristic p and we are dealing with arbitrary (finitely generated) kG-modules, or $\mathcal{O}$ is an integral domain in characteristic zero and an $\mathcal{O}G$-lattice M is indeed a lattice in the K-vector space $K \otimes_{\mathcal{O}} M$, where K is the field of fractions of $\mathcal{O}$. Note that conversely any interior G-algebra A which is $\mathcal{O}$-simple is isomorphic to the algebra of $\mathcal{O}$-linear endomorphism of an $\mathcal{O}G$-lattice M; indeed by $\mathcal{O}$-simplicity of A, we have $A = \mathrm{End}_{\mathcal{O}}(M)$ for some $\mathcal{O}$-lattice M and the interior G-algebra structure provides a homomorphism $G \to \mathrm{Aut}_{\mathcal{O}}(M) = A^*$ which defines an $\mathcal{O}G$-module structure on M.

The tensor product $M \otimes_{\mathcal{O}} N$ of two $\mathcal{O}G$-lattices M and N is again an $\mathcal{O}G$-lattice. The action of $g \in G$ is defined by $g\cdot(x \otimes y) = g\cdot x \otimes g\cdot y$ for $x \in M$ and $y \in N$, and then the action of an arbitrary element of $\mathcal{O}G$ is defined by $\mathcal{O}$-linearity. There is an isomorphism of interior G-algebras $\mathrm{End}_{\mathcal{O}}(M) \otimes_{\mathcal{O}} \mathrm{End}_{\mathcal{O}}(N) \cong \mathrm{End}_{\mathcal{O}}(M \otimes_{\mathcal{O}} N)$, mapping $a \otimes b$ to the endomorphism $x \otimes y \mapsto a(x) \otimes b(y)$. Indeed one can use bases to check that this is an isomorphism of algebras, and it is straightforward to deal with the interior structure.

If M and N are two $\mathcal{O}G$-lattices, then $\mathrm{Hom}_{\mathcal{O}}(M,N)$ is again an $\mathcal{O}G$-lattice. The action of $g \in G$ is defined by $(g\cdot f)(x) = g\cdot f(g^{-1}\cdot x)$ for $f \in \mathrm{Hom}_{\mathcal{O}}(M,N)$ and $x \in M$, and then the action of an arbitrary element of $\mathcal{O}G$ is defined by $\mathcal{O}$-linearity. In particular the action of $g \in G$ on $\mathrm{End}_{\mathcal{O}}(M)$ coincides with the action of g coming from the G-algebra structure. Taking $N = \mathcal{O}$, the trivial module, we see that the *dual lattice* $M^* = \mathrm{Hom}_{\mathcal{O}}(M,\mathcal{O})$ is again an $\mathcal{O}G$-lattice. Note that the right $\mathcal{O}G$-module structure on M^* defined in Section 6 has been turned here into a left module structure by defining the left action of $g \in G$ to be equal to the right action of g^{-1}. There is an isomorphism of $\mathcal{O}G$-lattices $M^* \otimes_{\mathcal{O}} N \cong \mathrm{Hom}_{\mathcal{O}}(M,N)$ mapping $f \otimes y \in M^* \otimes_{\mathcal{O}} N$ to the homomorphism $x \mapsto f(x)y$ (where $x \in M$). Indeed one can choose bases to show that this is an isomorphism of $\mathcal{O}$-lattices, and it is straightforward to check that this isomorphism commutes with the action of G (Exercise 10.6).

Many standard results for $\mathcal{O}G$-lattices turn out to be special cases of results on interior G-algebras. This more general point of view will always be adopted in this text. Also we shall see in Chapter 5 that it is often very important to work with the algebra $\mathrm{End}_{\mathcal{O}}(M)$ rather than the module M itself. But in order to be able to specialize to $\mathcal{O}G$-lattices the results on interior algebras, one often needs to apply the following lemma.

(10.7) LEMMA. *Two $\mathcal{O}G$-lattices L and M are isomorphic if and only if the interior G-algebras $\mathrm{End}_{\mathcal{O}}(L)$ and $\mathrm{End}_{\mathcal{O}}(M)$ are isomorphic.*

Proof. Let $A = \mathrm{End}_{\mathcal{O}}(L)$ and $B = \mathrm{End}_{\mathcal{O}}(M)$. If $L \cong M$, it is clear that $A \cong B$. Assume that $A \cong B$ as interior G-algebras. Since L is free as an $\mathcal{O}$-module, A is isomorphic to a matrix algebra over $\mathcal{O}$. As in Lemma 7.1, L can be identified with Ai, where i is any primitive idempotent of A (for instance i is the projection onto $\mathcal{O}e_1$, where e_1 is the first basis vector of L, and Ai is the set of all matrices having only the first column non-zero). Let $f : A \to B$ be an isomorphism of interior G-algebras and let $j = f(i)$. Then M can be identified with Bj and it is clear that the restriction to Ai of the isomorphism f induces an isomorphism of $\mathcal{O}$-modules $Ai \cong Bj$. This is an isomorphism of $\mathcal{O}G$-modules because f is an isomorphism of interior G-algebras, so that we have $f(g{\cdot}a) = g{\cdot}f(a)$ for all $g \in G$ and $a \in A$. $\square$

This result does not hold for arbitrary $\mathcal{O}G$-modules (unless further assumptions are made either on $\mathcal{O}$ or on the modules). Indeed, already without the presence of the group G, one may have isomorphic algebras $\mathrm{End}_{\mathcal{O}}(L) \cong \mathrm{End}_{\mathcal{O}}(M)$ for two non-isomorphic $\mathcal{O}$-modules L and M (Exercise 10.8). However, the interior G-algebra $\mathrm{End}_{\mathcal{O}}(M)$ is always a very useful tool for studying an arbitrary $\mathcal{O}G$-module M.

(10.8) EXAMPLE: Modules over twisted group algebras.
Again let A be an $\mathcal{O}$-simple algebra over $\mathcal{O}$, so that $A = \mathrm{End}_{\mathcal{O}}(M)$ for some free $\mathcal{O}$-module M. Assume that A is endowed with a G-algebra structure (but not necessarily interior as in the previous example). By the Skolem–Noether theorem 7.2, the action of an element $g \in G$ on A is an inner automorphism, thus of the form $\mathrm{Inn}(\rho(g))$ for some $\rho(g) \in A$. The element $\rho(g)$ is not uniquely determined by g, but it is well-defined up to a central element of A (because $\mathrm{Inn}(a) = \mathrm{Inn}(b)$ if and only if ab^{-1} is central). Therefore $\rho(g)$ is well-defined up to a scalar in $\mathcal{O}^* \cdot 1_A$ (which we identify with $\mathcal{O}^*$). This defines a map

$$\rho : G \longrightarrow A^*/\mathcal{O}^* \cong GL(M)/\mathcal{O}^* = PGL(M)$$

which is a group homomorphism since the inner automorphism $\mathrm{Inn}(\rho(gh))$ is equal to $\mathrm{Inn}(\rho(g)\rho(h)) = \mathrm{Inn}(\rho(g))\,\mathrm{Inn}(\rho(h))$ (because both are equal to the action of gh on A). Here $GL(M)$ and $PGL(M)$ denote respectively the general linear group and the projective general linear group on the $\mathcal{O}$-module M. In other words ρ is a "projective" representation of the group G, in the sense of Schur (a terminology which has nothing to do with projective modules).

We want to view a "projective" representation of G as a module over a suitable twisted group algebra of the group G. Given the group homomorphism $\rho : G \to PGL(M)$, we let $\widehat{G}$ be the central extension of the group G by the central subgroup $\mathcal{O}^*$ defined by the following pull-back diagram.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathcal{O}^* & \xrightarrow{\phi} & \widehat{G} & \xrightarrow{\pi} & G & \longrightarrow & 1 \\
 & & \big\downarrow \mathrm{id} & & \big\downarrow \widehat{\rho} & & \big\downarrow \rho & & \\
1 & \longrightarrow & \mathcal{O}^* & \longrightarrow & GL(M) & \xrightarrow{\pi_M} & PGL(M) & \longrightarrow & 1
\end{array}$$

The triple $(\widehat{G}, \widehat{\rho}, \pi)$ is unique up to a unique group isomorphism. In practice we can choose $\widehat{G}$ to be the set of all pairs $(a, g) \in GL(M) \times G$ such that $\pi_M(a) = \rho(g)$, and then $\widehat{\rho}$ and π are the first and second projections respectively. By the construction above, the equation $\pi_M(a) = \rho(g)$ means that the action of g on A is equal to the inner automorphism $\mathrm{Inn}(a)$. Therefore $\widehat{G}$ is the set of all pairs $(a, g) \in GL(M) \times G$ such that $\mathrm{Inn}(a)$ realizes the action of g.

The "projective" representation ρ is now lifted to an ordinary representation $\widehat{\rho}$ of the (infinite) group $\widehat{G}$ on the $\mathcal{O}$-module M. The representation $\widehat{\rho}$ is not arbitrary since it maps the central subgroup $\mathcal{O}^*$ to the centre $\mathcal{O}^*$ of $GL(M)$ by the identity map. Taking into account only this special type of representation comes down to the same thing as considering modules over the twisted group algebra $\mathcal{O}_\sharp \widehat{G}$, in just the same way as a representation of G over $\mathcal{O}$ is the same thing as an $\mathcal{O}G$-module. More precisely the group homomorphism $\widehat{\rho} : \widehat{G} \to GL(M)$ extends by $\mathcal{O}$-linearity to an algebra homomorphism $\widehat{\rho} : \mathcal{O}\widehat{G} \to \mathrm{End}_{\mathcal{O}}(M)$, and since $\widehat{\rho}(\phi(\lambda)) = \lambda \cdot id_M$ for every $\lambda \in \mathcal{O}^*$, it is clear that the ideal I which appears in the definition of a twisted group algebra (see Example 10.4 above) is in the kernel of $\widehat{\rho}$. Therefore we obtain an algebra homomorphism $\overline{\rho} : \mathcal{O}_\sharp \widehat{G} \to \mathrm{End}_{\mathcal{O}}(M)$ which provides M with an $\mathcal{O}_\sharp \widehat{G}$-module structure. Thus the lift $\widehat{\rho}$ of the "projective" representation $\rho : G \to PGL(M)$ induces an $\mathcal{O}_\sharp \widehat{G}$-module structure on M. Conversely with any $\mathcal{O}_\sharp \widehat{G}$-module M is associated a canonical group homomorphism $\rho : G \to PGL(M)$, because the module structure defines a group homomorphism $\widehat{\rho} : \widehat{G} \to GL(M)$ which induces a "projective" representation $\rho : G \to PGL(M)$ by passing to the quotient by $\mathcal{O}^*$ on both sides.

Starting from any G-algebra A over $\mathcal{O}$ which is $\mathcal{O}$-simple, so that $A \cong \mathrm{End}_{\mathcal{O}}(M)$ for some free $\mathcal{O}$-module M, the G-algebra structure on $\mathrm{End}_{\mathcal{O}}(M)$ lifts to a canonical $\mathcal{O}_\sharp \widehat{G}$-module structure on M, where

$\mathcal{O}_\sharp\widehat{G}$ is the twisted group algebra canonically associated with A. Conversely for any module M over a twisted group algebra $\mathcal{O}_\sharp\widehat{G}$, there is an induced group homomorphism $G \to PGL(M)$, hence a G-algebra structure on $A = \mathrm{End}_{\mathcal{O}}(M)$ since $PGL(M) = A^*/\mathcal{O}^*$ is the group of (inner) automorphisms of A.

We note that the analysis above also shows that any G-algebra A over $\mathcal{O}$ which is $\mathcal{O}$-simple is automatically an interior $\widehat{G}$-algebra (via the homomorphism $\widehat{\rho}$), in the sense defined in Example 10.4 above.

(10.9) EXAMPLE: Simple G-algebras which are interior for a subgroup. Again let A be an $\mathcal{O}$-simple algebra, so that $A = \mathrm{End}_{\mathcal{O}}(M)$ for some free $\mathcal{O}$-module M. Suppose that A has a G-algebra structure such that $\mathrm{Res}^G_H(A)$ is endowed with an interior H-algebra structure, where H is a subgroup of G. We continue with the notation of Example 10.8. Thus we have a group homomorphism $\rho : G \to PGL(M)$, but we wish to lift it to a group homomorphism $\widehat{\rho} : \widehat{G} \to GL(M)$ which takes into account the interior structure for the subgroup H. As $\mathrm{Res}^G_H(A)$ is interior, M is in fact an $\mathcal{O}H$-module. In other words a homomorphism $\widehat{\rho}_H : H \to GL(M)$ is given, which lifts the restriction of ρ to H. By definition of a pull-back, there is a unique group homomorphism $i : H \to \widehat{G}$ whose composition with $\pi : \widehat{G} \to G$ is the inclusion of H into G and such that $\widehat{\rho}\, i = \widehat{\rho}_H$. In other words the central extension splits on restriction to H. We identify H with a subgroup of $\widehat{G}$ via i, so that the group algebra $\mathcal{O}H$ is identified with a subalgebra of the twisted group algebra $\mathcal{O}_\sharp\widehat{G}$. It follows that the group homomorphism $\widehat{\rho} : \widehat{G} \to GL(M)$ extends the map $\widehat{\rho}_H$ and this gives an $\mathcal{O}_\sharp\widehat{G}$-module structure on M whose restriction to H is the given $\mathcal{O}H$-module structure. Thus we obtain that a G-algebra structure on $A = \mathrm{End}_{\mathcal{O}}(M)$ which extends a given interior H-algebra structure lifts to an $\mathcal{O}_\sharp\widehat{G}$-module structure on M which extends the given $\mathcal{O}H$-module structure.

If H is a normal subgroup of G, it is natural to take into account the conjugation action of G on H and to assume that $\widehat{\rho}_H$ is a G-map, in the sense that $\widehat{\rho}_H(ghg^{-1}) = {}^g(\widehat{\rho}_H(h))$ for all $g \in G$ and $h \in H$. Notice that this equation automatically holds if $g \in H$ since the action of g is just conjugation by $\widehat{\rho}_H(g)$. It is not difficult to prove that this additional assumption on $\widehat{\rho}_H$ implies that i is also a G-map, so that H is identified with a *normal* subgroup of $\widehat{G}$ via i.

(10.10) EXAMPLE: Extensions of simple modules from a normal subgroup.
Let H be a normal subgroup of G and let M be an $\mathcal{O}H$-module. If $g \in G$, the *conjugate module* ${}^gM$ is the $\mathcal{O}H$-module obtained as follows:

the underlying $\mathcal{O}$-module structure of ${}^gM$ is the same as that of M, but the action of $h \in H$ is equal to the action of $g^{-1}hg$ in the old module structure of M. It is clear that we have ${}^{g'g}M = {}^{g'}({}^gM)$. The *inertial subgroup* of M is the set of all $g \in G$ such that the conjugate module ${}^gM$ is isomorphic to M. It is clearly a subgroup, and it contains H, because the action of $h \in H$ on M realizes an isomorphism between ${}^hM$ and M.

Assume now that M is a simple kH-module and that the inertial subgroup of M is the whole of G (in which case M is said to be *G-invariant*). Then an isomorphism between ${}^gM$ and M is an automorphism ψ_g of M as a k-vector space such that $\psi_g((g^{-1}hg)\cdot v) = h\cdot\psi_g(v)$ for all $v \in M$ and $h \in H$ (or equivalently $\psi_g^{-1}(h\cdot w) = (g^{-1}hg)\cdot\psi_g^{-1}(w)$ for all $w \in M$ and $h \in H$). If ψ'_g has the same property, then we immediately deduce that $\psi_g^{-1}\psi'_g(h\cdot v) = h\cdot\psi_g^{-1}\psi'_g(v)$ for all $v \in M$ and $h \in H$, so that $\psi_g^{-1}\psi'_g$ is an automorphism of the kH-module M. Since M is simple, $\mathrm{End}_{kH}(M) \cong k$ by Schur's lemma (and the fact that k is algebraically closed). Therefore $\psi_g^{-1}\psi'_g = \lambda\cdot id_M$ for some $\lambda \in k^*$, and so $\psi'_g = \lambda\psi_g$. This shows that the automorphism ψ_g is well-defined up to multiplication by a scalar in k^* and therefore conjugation by ψ_g is a uniquely defined automorphism of $\mathrm{End}_k(M)$. If $g, g' \in G$, it follows from a straightforward computation that $\psi_{g'}\psi_g$ is an isomorphism between ${}^{g'g}M$ and M, so that $\psi_{g'}\psi_g$ and $\psi_{g'g}$ induce the same conjugation map on $\mathrm{End}_k(M)$. This shows that $\mathrm{End}_k(M)$ is a G-algebra. Moreover if $h \in H$, then one can choose for ψ_h the action of h on M and this means that the H-algebra structure on $\mathrm{Res}^G_H(\mathrm{End}_k(M))$ comes from an interior structure, namely the given interior H-algebra structure. By Example 10.9, we obtain a $k_\sharp\widehat{G}$-module structure on M which extends (in a canonical way) the given kH-module structure on M. In other words any simple kH-module which is G-invariant can be "extended" in a canonical way to G, provided we use a twisted group algebra.

We note that the additional property that $H \to GL(M)$ is a G-map is satisfied in this situation (because $(g^{-1}hg)\cdot v = \psi_g^{-1}(h\cdot\psi_g(v))$ as we have noticed above). Therefore, by the remark at the end of Example 10.9, H can be identified with a normal subgroup of $\widehat{G}$.

Exercises

(10.1) Let A be an $\mathcal{O}$-algebra.

(a) Show that two interior G-algebra structures on A induce the same G-algebra structure if and only if they differ by a group homomorphism of G into the centre of A.

(b) Construct an example of a G-algebra whose structure is not induced by an interior G-algebra structure. [Hint: Choose A commutative.]

(10.2) Let A be an $\mathcal{O}$-algebra endowed with a left $\mathcal{O}$-linear action of G and a right $\mathcal{O}$-linear action of G. Prove that the following conditions are equivalent:

(i) The map $G \to A$, $g \mapsto g \cdot 1_A$ defines an interior G-algebra structure on A.

(ii) The left and right actions of G satisfy the relations 10.1.

(iii) The left and right actions of G satisfy the relations 10.2.

(10.3) Let A and B be two interior G-algebras. Show that an algebra homomorphism $f : A \to B$ is a homomorphism of interior G-algebras if and only if $f(g \cdot 1_A) = g \cdot f(1_A)$ for all $g \in G$ and $f(1_A)$ is fixed under G-conjugation.

(10.4) Let G be a cyclic group. Show that any twisted group algebra $k_\sharp \widehat{G}$ of G is isomorphic to the group algebra kG. Prove that this isomorphism is not unique, unless G is a p-group. [Hint: Remembering that k is algebraically closed, prove that any central extension $\widehat{G}$ of G by k^* necessarily splits. Describe all the splittings in order to deal with the non-uniqueness.]

(10.5) Complete the details of the proof of the second statement of Proposition 10.5.

(10.6) Let M and N be two $\mathcal{O}G$-lattices. Provide the details of the proof that the two $\mathcal{O}G$-lattices $M^* \otimes_{\mathcal{O}} N$ and $\mathrm{Hom}_{\mathcal{O}}(M,N)$ are isomorphic.

(10.7) Let M be an $\mathcal{O}G$-lattice and let $A = \mathrm{End}_{\mathcal{O}}(M)$. Prove that $\mathrm{End}_{\mathcal{O}}(M^*)$ is isomorphic to A^{op} as interior G-algebras.

(10.8) Suppose that $\mathcal{O}$ is a domain with field of fractions K and that the maximal ideal $\mathfrak{p}$ is not principal.

(a) Prove that $\mathfrak{p} \not\cong \mathcal{O}$ as $\mathcal{O}$-modules but $\mathrm{End}_{\mathcal{O}}(\mathfrak{p}) \cong \mathrm{End}_{\mathcal{O}}(\mathcal{O})$. [Hint: Extending scalars to K, show that $\mathrm{End}_K(K \otimes_{\mathcal{O}} \mathfrak{p}) \cong \mathrm{End}_K(K)$.]

(a) Deduce that Lemma 10.7 does not hold for arbitrary $\mathcal{O}G$-modules.

Notes on Section 10

The concept of G-algebra was introduced by Green [1968], as a convenient tool for handling both $\mathcal{O}G$-modules and group algebras. The definition of an interior G-algebra is due to Puig [1981].

§ 11 SUBALGEBRAS OF FIXED ELEMENTS AND THE BRAUER HOMOMORPHISM

We introduce in this section various basic objects and maps associated with an arbitrary G-algebra A.

If H is a subgroup of G, the set of H*-fixed elements* of A is written

$$A^H = \{a \in A \mid {}^h a = a \text{ for all } h \in H\}.$$

Clearly A^H is a subalgebra of A (with the same unity element). For instance if $A = \mathrm{End}_{\mathcal{O}}(M)$ is the algebra of $\mathcal{O}$-endomorphisms of an $\mathcal{O}G$-module M (Example 10.6), then an endomorphism $f \in A$ is fixed under H if and only if f commutes with every element of H, that is, if and only if f is an $\mathcal{O}H$-linear endomorphism of M. Therefore $A^H = \mathrm{End}_{\mathcal{O}H}(M)$.

For a conjugate subgroup ${}^gH = gHg^{-1}$, we have $A^{{}^gH} = {}^g(A^H)$ because ${}^{ghg^{-1}}({}^g a) = {}^g a$ if $a \in A^H$. In particular the action of the normalizer $N_G(H)$ preserves A^H, and therefore A^H is endowed with an $N_G(H)$-algebra structure. Since H acts trivially on A^H, we can also view this structure as that of an $\overline{N}_G(H)$-algebra, where $\overline{N}_G(H) = N_G(H)/H$. Note that if A is an *interior* G-algebra, A^H is in general not an interior $N_G(H)$-algebra; however, we get an interior structure on restriction to the centralizer $C_G(H)$, because $g{\cdot}1 \in A^H$ if $g \in C_G(H)$. We shall sometimes use the notation $\mathrm{Conj}(g)$ for the action of $g \in N_G(H)$ on A^H. When A is an interior G-algebra, $\mathrm{Conj}(g)$ is the restriction of the inner automorphism $\mathrm{Inn}(g{\cdot}1_A)$, but is not necessarily inner (unless $g \in C_G(H)$).

If K is a subgroup of H, then obviously $A^H \subseteq A^K$; in particular the smallest subalgebra of fixed elements is A^G and the largest is $A^{\{1\}} = A$. In order to always make clear in which algebra we work (and also in order to prepare the more general setting of Chapter 8), we shall give a name to the inclusions between various subalgebras of fixed elements. Thus if K is a subgroup of H, we define $r^H_K : A^H \to A^K$ to be the inclusion (and we sometimes call it *restriction* map); it is obviously a unitary algebra homomorphism. We shall use this notation whenever we feel that it clarifies understanding.

There is also a map going in the reverse direction, called the *relative trace map* and defined by

$$t_K^H : A^K \longrightarrow A^H \,, \qquad t_K^H(a) = \sum_{h\in[H/K]} {}^h a \,,$$

where $[H/K]$ denotes a set of representatives of the right cosets of K in H . Since $a \in A^K$, it is clear that ${}^h a$ does not depend on the choice of h in its coset; thus the map t_K^H is well-defined. Its image is contained in A^H because for $g \in H$, we have

$${}^g(t_K^H(a)) = \sum_{h\in[H/K]} {}^{gh}a = \sum_{h'\in[H/K]} {}^{h'}a = t_K^H(a) \,,$$

because $h' = gh$ also runs through some set of representatives $[H/K]$. It is also clear that t_K^H is $\mathcal{O}$-linear, but of course in general t_K^H is not an algebra homomorphism.

The behaviour of t_K^H with respect to multiplication is given by the formulae

(11.1) $t_K^H(ab) = t_K^H(a)\,b$ and $t_K^H(ba) = b\,t_K^H(a)$ if $a \in A^K$, $b \in A^H$,

or in other words $t_K^H(a\,r_K^H(b)) = t_K^H(a)\,b$ and $t_K^H(r_K^H(b)\,a) = b\,t_K^H(a)$. The proof is straightforward:

$$t_K^H(ab) = \sum_{h\in[H/K]} {}^h(ab) = \sum_{h\in[H/K]} {}^h a\, b = t_K^H(a)\,b \,,$$

and similarly on the other side.

An immediate consequence of 11.1 is that the image of the relative trace map $t_K^H(A^K)$ is an ideal in A^H . This ideal will be written A_K^H . It plays an important role in the sequel.

We also need to know about the composition of the restriction and the relative trace maps. There are two properties, the first being easy:

(11.2) $$t_K^H\, r_K^H(a) = |H:K| \cdot a \qquad \text{if } a \in A^H \,.$$

The second property is called *the Mackey decomposition formula*: if K and L are subgroups of H and if $a \in A^K$, then

(11.3) $$r_L^H\, t_K^H(a) = \sum_{h\in[L\backslash H/K]} t_{L\cap {}^hK}^L\, r_{L\cap {}^hK}^{{}^hK}({}^h a) \,,$$

where $[L\backslash H/K]$ denotes a set of representatives of the double cosets LhK. Ignoring inclusions, we can also write $t_K^H(a) = \sum_{h\in[L\backslash H/K]} t^L_{L\cap {}^hK}({}^ha)$, but some thinking is required to know where each element of this formula lies. For the proof of 11.3, we first write the decomposition of H/K into L-orbits

$$H/K = \bigcup_{h\in[L\backslash H/K]} L\cdot(hK)$$

and we note that the stabilizer of the element hK of H/K is $L\cap {}^hK$. Thus we can write

$$t_K^H(a) \;=\; \sum_{h\in[L\backslash H/K]}\;\sum_{g\in[L/L\cap {}^hK]} {}^{gh}a \;=\; \sum_{h\in[L\backslash H/K]} t^L_{L\cap {}^hK}({}^ha)\,,$$

and 11.3 is proved.

We now collect the above results and add some trivial properties of the restriction and relative trace maps.

(11.4) PROPOSITION. *Let A be a G-algebra. With the notation above, the following properties hold.*

(a) If $L\le K\le H$, then $r^K_L\, r^H_K = r^H_L$ and $t^H_K\, t^K_L = t^H_L$.
(b) $r^H_H = t^H_H = id_{A^H}$.
(c) If $K\le H$, $a\in A^K$, and $b\in A^H$, then ${}^g(r^H_K(b)) = r^{{}^gH}_{{}^gK}({}^gb)$ and ${}^g(t^H_K(a)) = t^{{}^gH}_{{}^gK}({}^ga)$.
(d) (Mackey decomposition formula) If $L,K\le H$ and $a\in A^K$, then

$$r^H_L\, t^H_K(a) = \sum_{h\in[L\backslash H/K]} t^L_{L\cap {}^hK}\, r^{{}^hK}_{L\cap {}^hK}({}^ha)\,.$$

(e) If $K\le H$, $a\in A^K$, and $b\in A^H$, then $t^H_K(a\,r^H_K(b)) = t^H_K(a)\,b$ and $t^H_K(r^H_K(b)\,a) = b\,t^H_K(a)$.
(f) If $K\le H$, $a,b\in A^H$, then $r^H_K(ab) = r^H_K(a)\,r^H_K(b)$.
(g) $t^H_K\, r^H_K$ is multiplication by $|H:K|$.

These properties show that the family of algebras A^H (with H running over the set of subgroups of G), together with the family of maps r^H_K and t^H_K, is a cohomological Green functor for G over $\mathcal{O}$, in the sense of Chapter 8.

If $f: A\to B$ is a homomorphism of G-algebras, then for every subgroup H of G, the map f restricts to a homomorphism of $\mathcal{O}$-algebras $f^H: A^H\to B^H$. The maps f^H commute with the restriction and relative trace maps in the obvious sense:

(11.5) $$r^H_K\, f^H = f^K\, r^H_K \qquad\text{and}\qquad t^H_K\, f^K = f^H\, t^H_K\,.$$

With the terminology of Chapter 8, this says that the family of maps f^H defines a morphism of Green functors for G.

We now introduce one of the key concepts: the Brauer homomorphism. Given a subgroup P of G, we know that $A_Q^P = t_Q^P(A^Q)$ is an ideal of A^P for every subgroup Q of P. Thus the sum of all those ideals, for Q running over the set of all proper subgroups of P, is again an ideal and we can consider the quotient algebra $A^P / \sum_{Q<P} A_Q^P$. For technical reasons (see Remark 11.8 below), it is also convenient to pass to the quotient by the ideal $\mathfrak{p}A^P$ and we define the *Brauer quotient*

$$\overline{A}(P) = A^P / \big(\sum_{Q<P} A_Q^P + \mathfrak{p}A^P \big) .$$

Since $\mathfrak{p}\overline{A}(P) = 0$, it is clear that $\overline{A}(P)$ is a k-algebra. Moreover the action of $N_G(P)$ on A^P obviously preserves the ideal $\sum_{Q<P} A_Q^P$ (by Proposition 11.4 (c)) as well as the ideal $\mathfrak{p}A^P$ (because G acts $\mathcal{O}$-linearly), and therefore induces an $N_G(P)$-algebra structure on $\overline{A}(P)$. Since P acts trivially on A^P, it is often convenient to view $\overline{A}(P)$ as an $\overline{N}_G(P)$-algebra, where $\overline{N}_G(P) = N_G(P)/P$. Note in particular that for $P = 1$, we have $\overline{A}(1) = A/\mathfrak{p}A \cong k \otimes_{\mathcal{O}} A$.

The canonical surjection

$$br_P^A : A^P \longrightarrow \overline{A}(P)$$

is called the *Brauer homomorphism* corresponding to the subgroup P. Whenever we are working with a single G-algebra A, we often write simply br_P instead of br_P^A. By construction, br_P is a homomorphism of $N_G(P)$-algebras. If A is an interior G-algebra, then A^P is an interior $C_G(P)$-algebra; therefore so is $\overline{A}(P)$ and br_P is a homomorphism of interior $C_G(P)$-algebras. For every subgroup H containing P, we can compose with the inclusion $r_P^H : A^H \to A^P$, and since the image of r_P^H is fixed under $N_H(P)$, we obtain an algebra homomorphism

$$br_P \, r_P^H : A^H \longrightarrow \overline{A}(P)^{N_H(P)} .$$

If $f : A \to B$ is a homomorphism of G-algebras, then its restriction $f^P : A^P \to B^P$ commutes with the relative trace map (by 11.5) and maps $\mathfrak{p}A^P$ to $\mathfrak{p}B^P$. Therefore f^P induces a homomorphism of k-algebras $\overline{f}(P) : \overline{A}(P) \to \overline{B}(P)$ such that

$$\overline{f}(P) \, br_P^A = br_P^B \, f^P . \tag{11.6}$$

We now use for the first time our assumption that p is the characteristic of the residue field $k = \mathcal{O}/\mathfrak{p}$. Any integer which is prime to p is invertible in k, hence in $\mathcal{O}$ since $\mathcal{O}$ is a local ring.

(11.7) LEMMA. *Let A be a G-algebra and let H be a subgroup of G.*
(a) Let Q be a Sylow p-subgroup of H. Then $A^H = A^H_Q$.
(b) If H is not a p-group, then $\overline{A}(H) = 0$.

Proof. (a) Since $|H{:}Q|$ is invertible in $\mathcal{O}$, we have $a = t^H_Q(|H{:}Q|^{-1}a)$ for every $a \in A^H$, by 11.2. Now (b) follows immediately from (a). □

If P is a p-subgroup of G, the k-algebra $\overline{A}(P)$ is in general non-zero. For instance if $A = \mathcal{O}$ with trivial G-action, then for each $Q < P$, we have

$$A^P_Q = |P : Q| \cdot A^P = |P : Q| \cdot \mathcal{O} \subseteq \mathfrak{p}$$

because $p \in \mathfrak{p}$ and $|P : Q|$ is a power of p. Therefore $\overline{A}(P) = \mathcal{O}/\mathfrak{p} = k$.

(11.8) REMARK. Every non-trivial p-subgroup P contains a subgroup Q of index p. Thus

$$A^P_Q \supseteq t^P_Q r^P_Q(A^P) = |P : Q| \cdot A^P = p \cdot A^P,$$

and it follows that $B = A^P / \sum_{Q<P} A^P_Q$ is annihilated by p. Thus B is an algebra over the field $\mathbb{F}_p$ with p elements, but not necessarily over k. This is why it is convenient to also take the quotient by $\mathfrak{p}$ in the definition of $\overline{A}(P)$. This procedure does not change the points of B, since the surjection $B \to \overline{A}(P)$ induces a bijection $\mathcal{P}(B) \to \mathcal{P}(\overline{A}(P))$ (because $\mathfrak{p}B \subseteq J(B)$). For instance assume that $\mathcal{O}$ is a complete discrete valuation ring of characteristic zero with maximal ideal $\mathfrak{p}$ generated by an element π. If $\mathcal{O}$ is unramified over the ring $\mathbb{Z}_p$ of p-adic integers (that is, if one can choose $\pi = p$ as a generator of $\mathfrak{p}$), then we do not need to take the quotient by $\mathfrak{p}$ and $B = \overline{A}(P)$ is a k-algebra. However, if $\mathcal{O}$ is ramified and p generates the ideal $\pi^e{\cdot}\mathcal{O}$, then B is an algebra over the artinian ring $\overline{\mathcal{O}} = \mathcal{O}/\pi^e{\cdot}\mathcal{O}$, and it seems natural to take the quotient by the nilpotent ideal $\overline{\pi}{\cdot}\overline{\mathcal{O}}$ to obtain the k-algebra $\overline{A}(P)$.

The next result is a fundamental property of the Brauer homomorphism which connects the relative trace maps in the G-algebra A and in the $\overline{N}_G(P)$-algebra $\overline{A}(P)$.

(11.9) PROPOSITION. *Let A be a G-algebra, let P be a p-subgroup of G, and let H be a subgroup of G containing P. Then for every $a \in A^P$, we have*

$$br_P\, r^H_P\, t^H_P(a) = t_1^{\overline{N}_H(P)}\, br_P(a),$$

where $t_1^{\overline{N}_H(P)} : \overline{A}(P) \to \overline{A}(P)^{\overline{N}_H(P)}$ is the relative trace map in the $\overline{N}_G(P)$-algebra $\overline{A}(P)$. In particular $br_P\, r^H_P(A^H_P) = \overline{A}(P)_1^{\overline{N}_H(P)}$.

Proof. The proof is an easy application of the Mackey decomposition formula and of the fact that, for $h \in H$, we have $br_P(A^P_{P\cap {}^hP}) = 0$ if $P\cap {}^hP < P$, that is, if $h \notin N_H(P)$.

$$br_P\, r^H_P\, t^H_P(a) = \sum_{h\in[P\backslash H/P]} br_P(t^P_{P\cap {}^hP}({}^ha)) = \sum_{h\in[N_H(P)/P]} br_P({}^ha)$$
$$= t_P^{N_H(P)}(br_P(a)) = t_1^{\overline{N}_H(P)}(br_P(a)) . \ \square$$

We now derive a more general result (which is the proposition when $P = K$).

(11.10) COROLLARY. *Let A be a G-algebra and let $P \leq K \leq H \leq G$ where P is a p-subgroup of G . Then for every $a \in A^K_P$, we have*

$$br_P\, r^H_P\, t^H_K(a) = t^{\overline{N}_H(P)}_{\overline{N}_K(P)}\, br_P\, r^K_P(a) .$$

Proof. Since $a \in A^K_P$, we can write $a = t^K_P(b)$. Applying the proposition for both subgroups K and H , we get

$$br_P\, r^H_P\, t^H_K(a) = br_P\, r^H_P\, t^H_P(b) = t_1^{\overline{N}_H(P)}\, br_P(b) = t^{\overline{N}_H(P)}_{\overline{N}_K(P)}\, t_1^{\overline{N}_K(P)}\, br_P(b)$$
$$= t^{\overline{N}_H(P)}_{\overline{N}_K(P)}\, br_P\, r^K_P\, t^K_P(b) = t^{\overline{N}_H(P)}_{\overline{N}_K(P)}\, br_P\, r^K_P(a) . \ \square$$

Exercises

(11.1) Let $A = \mathcal{O}G$ be the group algebra. Show that $A^G = Z(\mathcal{O}G)$, the centre of $\mathcal{O}G$. Find an $\mathcal{O}$-basis of A^G . More generally find an $\mathcal{O}$-basis of A^H where H is a subgroup of G .

(11.2) Let $A = \mathcal{O}G$ be the group algebra. Prove that t^G_1 is surjective if and only if p does not divide $|G|$.

(11.3) Show that the Jacobson radical is in general not preserved by the maps r^H_K and t^H_K by constructing examples of a G-algebra A with either $r^H_K(J(A^H)) \not\subseteq J(A^K)$ or $t^H_K(J(A^K)) \not\subseteq J(A^H)$.

(11.4) Let A be a G-algebra with a G-invariant basis X . If P is a p-subgroup of G , let X^P be the set of P-fixed elements in X . Show that $\{ br_P(x) \mid x \in X^P \}$ is a k-basis of $\overline{A}(P)$.

(11.5) For the group algebra $A = \mathcal{O}G$, prove that $\overline{A}(P) \cong kC_G(P)$ for every p-subgroup P of G. [Hint: Use the previous exercise.]

Notes on Section 11

The systematic study of subalgebras of fixed elements in an arbitrary G-algebra finds its origin in the paper of Green [1968]. In the case of the group algebra, the concept of Brauer homomorphism was introduced by Brauer [1956, 1959], but with a different point of view. The idea of defining such a homomorphism for an arbitrary G-algebra is due to Broué and Puig [1980].

§ 12 EXOMORPHISMS AND EMBEDDINGS OF G-ALGEBRAS

In this section we discuss exomorphisms and embeddings of G-algebras. We show that the notion of embedding generalizes the concept of direct summand of modules. We prove some fundamental results about restriction of exomorphisms and cancellation of embeddings.

If $\mathrm{Inn}(a)$ is an inner automorphism of an interior G-algebra A, then for every $g \in G$, we have by definition $a(g\cdot 1)a^{-1} = g\cdot aa^{-1} = g\cdot 1$, so that $(g\cdot 1)^{-1}a(g\cdot 1) = a$, that is $a \in (A^G)^*$. Conversely any $a \in (A^G)^*$ defines an inner automorphism of the interior G-algebra A. The situation is more complicated in the case of G-algebras. An inner automorphism $\mathrm{Inn}(a)$ of a G-algebra A commutes by definition with the G-action and it follows easily that $({}^g a)^{-1}a$ must lie in the centre $Z(A)$ of A. Thus a is fixed under G in $A^*/Z(A)^*$, but does not necessarily lie in $(A^G)^*$. Conversely any element $a \in A^*$ whose image in $A^*/Z(A)^*$ is fixed under G defines an inner automorphism $\mathrm{Inn}(a)$ of the G-algebra A. However, we shall only consider inner automorphisms $\mathrm{Inn}(a)$ such that $a \in A^G$ because we do not want to allow an inner automorphism to move the points of A^G, and this phenomenon may happen if $a \in (A^*/Z(A)^*)^G$ but $a \notin A^G$ (Exercise 12.1). With this restriction on inner automorphisms (which is no restriction in the case of interior algebras), we can say that an inner automorphism is "harmless", and so it is worth working modulo inner automorphisms, as in the following definitions.

If A and B are G-algebras, we define an *exomorphism of G-algebras* $\mathcal{F} : A \to B$ to be an equivalence class of homomorphisms of G-algebras $f : A \to B$, where two such homomorphisms f and f' are equivalent if

$f' = \mathrm{Inn}(b) f \,\mathrm{Inn}(a)$ for some $a \in (A^G)^*$ and $b \in (B^G)^*$. By the argument already used for exomorphisms of $\mathcal{O}$-algebras (see 8.1), it suffices to compose f with inner automorphisms of B, so that

$$\mathcal{F} = \{\mathrm{Inn}(b) \cdot f \mid b \in (B^G)^*\}.$$

It should be noted that an exomorphism $\mathcal{F} : A \to B$ of G-algebras is (in general) not an exomorphism of $\mathcal{O}$-algebras, because we compose with fewer inner automorphisms $\mathrm{Inn}(b)$ (namely b lies in $(B^G)^*$ rather than B^*). However, the restriction to G-fixed elements $\mathcal{F}^G : A^G \to B^G$ is an exomorphism of $\mathcal{O}$-algebras. As in the case of $\mathcal{O}$-algebras, an exomorphism is called an *exo-isomorphism* if it consists of isomorphisms, and an *exo-automorphism* or *outer automorphism* if it consists of automorphisms. Also one can compose exomorphisms of G-algebras, as in the case of $\mathcal{O}$-algebras (see Lemma 8.2).

If one considers interior G-algebras, then an *exomorphism of interior G-algebras* is defined in the same way. Thus it is obtained by composing a homomorphism of interior G-algebras $f : A \to B$ with all inner automorphisms $\mathrm{Inn}(b)$ where $b \in (B^G)^*$.

Let $\mathcal{F} : A \to B$ be an exomorphism of G-algebras. On restriction to a subgroup H, any $f \in \mathcal{F}$ is also a homomorphism of H-algebras, which is denoted $\mathrm{Res}^G_H(f)$. The exomorphism containing $\mathrm{Res}^G_H(f)$ is written $\mathrm{Res}^G_H(\mathcal{F}) : \mathrm{Res}^G_H(A) \to \mathrm{Res}^G_H(B)$. Note that $\mathrm{Res}^G_H(\mathcal{F})$ contains in general more homomorphisms than $\mathcal{F}$, because one has to compose with more inner automorphisms. The evaluation on H-fixed elements gives rise to an exomorphism of $\mathcal{O}$-algebras $\mathcal{F}^H : A^H \to B^H$. One of the first features of interior G-algebras is the following result, often used for the trivial subgroup $H = 1$. It is not clear whether a similar result holds in the case of G-algebras.

(12.1) PROPOSITION. *Let $\mathcal{F} : A \to B$ and $\mathcal{F}' : A \to B$ be two exomorphisms of interior G-algebras. If $\mathrm{Res}^G_H(\mathcal{F}) = \mathrm{Res}^G_H(\mathcal{F}')$ for some subgroup H of G, then $\mathcal{F} = \mathcal{F}'$.*

Proof. Let $f \in \mathcal{F}$ and $f' \in \mathcal{F}'$, and let $i = f(1_A)$ and $i' = f'(1_A)$ (which both belong to B^G). By assumption there exists $b \in (B^H)^*$ such that $f'(a) = bf(a)b^{-1}$ for all $a \in A$. Applying this to $a = 1_A \cdot g$ where $g \in G$, we have

$$g \cdot i' = i' \cdot g = b(i \cdot g)b^{-1}$$

and in particular $i'b = bi$ (when $g = 1$). Therefore

$$g \cdot bi = g \cdot i'b = bi \cdot g$$

and this shows that $bi \in B^G$. Similarly

$$b^{-1}i' \cdot g = b^{-1}(g \cdot i') = (i \cdot g)b^{-1} = g \cdot ib^{-1} = g \cdot b^{-1}i'$$

so that $b^{-1}i' \in B^G$.

Since $(bi)(b^{-1}i') = (i')^2 = i'$ and $(b^{-1}i')(bi) = i^2 = i$, it follows from Exercise 3.2 that i and i' are conjugate in B^G (since $bi, b^{-1}i' \in B^G$). Therefore, replacing f' by another representative of $\mathcal{F}'$, we can assume that $f(1_A) = f'(1_A) = i$. In particular the arguments above show that $bi = ib \in B^G$ and $b^{-1}i = ib^{-1} \in B^G$. Now let $c = bi + (1_B - i) \in B^G$, with inverse $c^{-1} = b^{-1}i + (1_B - i)$. Then for all $a \in A$,

$$cf(a)c^{-1} = cf(1_A a 1_A)c^{-1} = cif(a)ic^{-1} = bif(a)ib^{-1} = bf(a)b^{-1} = f'(a)\,,$$

and this means that $f' = \mathrm{Inn}(c)f$. Since $c \in B^G$, we conclude that f and f' belong to the same exomorphism of interior G-algebras. □

An exomorphism $\mathcal{F} : A \to B$ of G-algebras is called an *embedding* if some $f \in \mathcal{F}$ (and hence every $f \in \mathcal{F}$) is injective and has as image the whole of $f(1_A)Bf(1_A)$. In other words $\mathrm{Res}^G_1(\mathcal{F})$ is required to be an embedding, but we emphasize that $f(1_A)$ is necessarily fixed under G . Note that if $i \in B^G$ is any idempotent fixed under G , then iBi is always a G-algebra; in case B is interior, then iBi is interior with respect to the map

$$G \longrightarrow (iBi)^* \,, \quad g \mapsto g{\cdot}i = i{\cdot}g = i{\cdot}g{\cdot}i\,.$$

The exomorphism containing the inclusion $iBi \to B$ is an embedding. Any embedding is the composition of an exo-isomorphism followed by an embedding of this special type.

As in the case of $\mathcal{O}$-algebras (Propositions 8.6 and 8.7), we have two results on the cancellation of embeddings. The second one uses Proposition 12.1 and therefore holds for interior G-algebras.

(12.2) PROPOSITION. *Let $\mathcal{F}, \mathcal{F}' : A \to B$ be two exomorphisms of G-algebras and let $\mathcal{E} : B \to C$ be an embedding of G-algebras.*
(a) If $\mathcal{E}\mathcal{F} = \mathcal{E}\mathcal{F}'$, then $\mathcal{F} = \mathcal{F}'$.
(b) $\mathcal{F}$ is an embedding if and only if $\mathcal{E}\mathcal{F}$ is an embedding.

Proof. We give a complete proof for interior G-algebras (using Proposition 12.1) and sketch at the end another proof which works for arbitrary G-algebras. In order to prove (a), it suffices by Proposition 12.1 to prove that $\mathrm{Res}^G_1(\mathcal{F}) = \mathrm{Res}^G_1(\mathcal{F}')$. Thus we are left with a statement about $\mathcal{O}$-algebras, which was proved in Proposition 8.6. This result also applies for part (b) since $\mathcal{F}$ is an embedding of interior G-algebras if and only if

$\mathrm{Res}_1^G(\mathcal{F})$ is an embedding of $\mathcal{O}$-algebras. This completes the proof in the interior case.

For arbitrary G-algebras, one can prove the result by following each step of the proof of Proposition 8.6, which is the analogous result for $\mathcal{O}$-algebras. It is elementary to check that the elements c, b and b_0 which appear in that proof are fixed under G. This is the only modification one needs to observe, for the rest of the proof applies verbatim. □

(12.3) PROPOSITION. *Let $\mathcal{F}, \mathcal{F}' : A \to B$ be two exomorphisms of interior G-algebras and let $\mathcal{E} : C \to A$ be an embedding of G-algebras. Assume that C and A have the same number of points (as $\mathcal{O}$-algebras).*

(a) If $\mathcal{F}\mathcal{E} = \mathcal{F}'\mathcal{E}$, then $\mathcal{F} = \mathcal{F}'$.

(b) $\mathcal{F}$ is an embedding if and only if $\mathcal{F}\mathcal{E}$ is an embedding.

Proof. In order to prove (a), it suffices by Proposition 12.1 to prove that $\mathrm{Res}_1^G(\mathcal{F}) = \mathrm{Res}_1^G(\mathcal{F}')$. Thus we are left with a statement about $\mathcal{O}$-algebras, which was proved in Proposition 8.7. This result also applies for part (b) since $\mathcal{F}$ is an embedding of interior G-algebras if and only if $\mathrm{Res}_1^G(\mathcal{F})$ is an embedding of $\mathcal{O}$-algebras. □

It is not clear whether a similar result holds in the case of G-algebras. Contrary to the previous result, there is this time no obvious modification in the proof of Proposition 8.7 which would allow us to deal with G-algebras.

We end this section with the discussion of the case of $\mathcal{O}G$-modules. We want to show that the concept of embedded subalgebra corresponds to taking a direct summand of a module. Let M be an $\mathcal{O}G$-module and let iM be a direct summand of M, where $i \in \mathrm{End}_{\mathcal{O}G}(M)$ is an idempotent projection with image iM. Relative to the decomposition $M = iM \oplus (1-i)M$, the algebra $\mathrm{End}_{\mathcal{O}}(M)$ decomposes in matrix notation

$$\mathrm{End}_{\mathcal{O}}(M) = \begin{pmatrix} \mathrm{End}_{\mathcal{O}}(iM) & \mathrm{Hom}_{\mathcal{O}}((1-i)M, iM) \\ \mathrm{Hom}_{\mathcal{O}}(iM, (1-i)M) & \mathrm{End}_{\mathcal{O}}((1-i)M) \end{pmatrix}$$

and it follows that $i\,\mathrm{End}_{\mathcal{O}}(M)i$ can be identified with $\mathrm{End}_{\mathcal{O}}(iM)$. We now prove this in a more explicit fashion.

(12.4) LEMMA. *Let* M *be an* $\mathcal{O}G$*-module and let* $i \in \mathrm{End}_{\mathcal{O}G}(M)$ *be an idempotent. Then the interior* G*-algebras* $\mathrm{End}_{\mathcal{O}}(iM)$ *and* $i\,\mathrm{End}_{\mathcal{O}}(M)i$ *are isomorphic.*

Proof. Let $\pi : M \to iM$ be the projection with kernel $(1-i)M$ and let $\varepsilon : iM \to M$ be the inclusion map. Both ε and π commute with the action of G because G commutes with i. Define

$$f : i\,\mathrm{End}_{\mathcal{O}}(M)i \longrightarrow \mathrm{End}_{\mathcal{O}}(iM)\,, \qquad \phi \mapsto \pi\phi\varepsilon\,.$$

It is easy to check that f is a homomorphism of $\mathcal{O}$-algebras. It preserves the interior structures because $f(g{\cdot}i) = \pi g{\cdot}i\varepsilon = g{\cdot}\pi i\varepsilon = g{\cdot}id_{iM}$. The inverse of f is the map

$$\mathrm{End}_{\mathcal{O}}(iM) \longrightarrow i\,\mathrm{End}_{\mathcal{O}}(M)i\,, \qquad \psi \mapsto \varepsilon\psi\pi\,.$$

Indeed we have $\pi\varepsilon\psi\pi\varepsilon = \psi$ for $\psi \in \mathrm{End}_{\mathcal{O}}(iM)$ since $\pi\varepsilon = id_{iM}$, while $\varepsilon\pi\phi\varepsilon\pi = i\phi i = \phi$ for $\phi \in i\,\mathrm{End}_{\mathcal{O}}(M)i$ since $\varepsilon\pi = i$. It follows that f is an isomorphism of interior G-algebras. □

For simplicity we shall only work with $\mathcal{O}G$-lattices instead of arbitrary $\mathcal{O}G$-modules. In this special case we know from Lemma 10.7 that we can recover an $\mathcal{O}G$-lattice from its endomorphism algebra. The precise relationship between embeddings and direct summands is provided by the following result.

(12.5) PROPOSITION. *Let* L *and* M *be two* $\mathcal{O}G$*-lattices. There exists an embedding of interior* G*-algebras* $\mathcal{F} : \mathrm{End}_{\mathcal{O}}(L) \to \mathrm{End}_{\mathcal{O}}(M)$ *if and only if* L *is isomorphic to a direct summand of* M*. Moreover in that case the embedding* $\mathcal{F}$ *is unique.*

Proof. Let $\mathcal{F} : \mathrm{End}_{\mathcal{O}}(L) \to \mathrm{End}_{\mathcal{O}}(M)$ be an embedding, let $f \in \mathcal{F}$, and let

$$i = f(id_L) \in \mathrm{End}_{\mathcal{O}}(M)^G = \mathrm{End}_{\mathcal{O}G}(M)\,.$$

By definition of an embedding, f induces an isomorphism of interior G-algebras $\mathrm{End}_{\mathcal{O}}(L) \cong i\,\mathrm{End}_{\mathcal{O}}(M)i$. By Lemma 12.4 above, we have $\mathrm{End}_{\mathcal{O}}(L) \cong \mathrm{End}_{\mathcal{O}}(iM)$. Now iM is an $\mathcal{O}G$-lattice since any direct summand of a lattice is a lattice (because a direct summand of a free $\mathcal{O}$-module is free by Corollary 1.4). Therefore Lemma 10.7 applies and it follows that the $\mathcal{O}G$-modules L and iM are isomorphic, proving that L is isomorphic to a direct summand of M. Conversely if $L \cong iM$ for some idempotent $i \in \mathrm{End}_{\mathcal{O}G}(M)$, then $\mathrm{End}_{\mathcal{O}}(L) \cong \mathrm{End}_{\mathcal{O}}(iM) \cong i\,\mathrm{End}_{\mathcal{O}}(M)i$ and this isomorphism induces an embedding $\mathrm{End}_{\mathcal{O}}(L) \to \mathrm{End}_{\mathcal{O}}(M)$.

We now prove uniqueness. Let $A = \mathrm{End}_{\mathcal{O}}(L)$ and $B = \mathrm{End}_{\mathcal{O}}(M)$. Let $\mathcal{F}' : A \to B$ be another embedding, choose $f \in \mathcal{F}$ and $f' \in \mathcal{F}'$, and let $i = f(1_A)$ and $i' = f'(1_A)$. By definition of an embedding, A is isomorphic to both iBi and $i'Bi'$. Since $iBi \cong \mathrm{End}_{\mathcal{O}}(iM)$ and $i'Bi' \cong \mathrm{End}_{\mathcal{O}}(i'M)$ by Lemma 12.4, we have $iM \cong i'M$ by Lemma 10.7. Now by Corollary 4.5 applied to the algebra $B^G = \mathrm{End}_{\mathcal{O}G}(M)$, the two idempotents i and i' are conjugate in B^G, say by some element $b \in B^G$. Changing the choice of $f' \in \mathcal{F}'$ (that is, replacing f' by $\mathrm{Inn}(b)f'$), we can assume that $i = i'$. Then f and f' induce two isomorphisms $A \cong iBi$ and so there exists an automorphism of interior G-algebras $h : A \xrightarrow{\sim} A$ such that $f' = fh$. But $A = \mathrm{End}_{\mathcal{O}}(L)$ is an $\mathcal{O}$-simple algebra and by the Skolem–Noether theorem 7.2, $h = \mathrm{Inn}(a)$ is an inner automorphism. As h is an automorphism of interior G-algebras, we must have $a \in A^G$ and this proves that $f' = f\,\mathrm{Inn}(a)$ belongs to the exomorphism $\mathcal{F}$. Thus $\mathcal{F} = \mathcal{F}'$, as was to be shown. □

This proposition shows that embeddings are generalizations of the notion of direct summand. But we emphasize that the general case of G-algebras is more complicated than that of $\mathcal{O}G$-lattices. Indeed an embedding $\mathcal{F} : A \to B$ is not necessarily unique, because of two factors which do not appear in the case of $\mathcal{O}G$-lattices, as is shown clearly in the proof above. The first one is that for two idempotents $i, i' \in B^G$, the two embedded subalgebras iBi and $i'Bi'$ may be isomorphic without i and i' being conjugate in B^G (Exercise 12.3); in that case the inclusion $iBi \hookrightarrow B$ and the composite $iBi \cong i'Bi' \hookrightarrow B$ belong to two distinct embeddings. The second factor is that one can always compose $\mathcal{F}$ with an outer automorphism $\mathcal{H}$ of A to obtain a new embedding $\mathcal{F}\mathcal{H} : A \to B$. These two reasons explain why we have chosen to prove uniqueness as we did in Proposition 12.5. There is another approach based on the observation that there is a unique embedding of $\mathcal{O}$-algebras $A \to B$ by Corollary 4.5 (where $A = \mathrm{End}_{\mathcal{O}}(L)$ and $B = \mathrm{End}_{\mathcal{O}}(M)$ as above). Thus if $\mathcal{F}, \mathcal{F}' : A \to B$ are two embeddings of interior G-algebras, we have $\mathrm{Res}^G_1(\mathcal{F}) = \mathrm{Res}^G_1(\mathcal{F}')$, and therefore $\mathcal{F} = \mathcal{F}'$ by Proposition 12.1.

Exercises

(12.1) Let G be the cyclic group of order 2 acting on the algebra of 2×2-matrices $A = M_2(\mathcal{O})$ by exchanging the rows and columns. Assume that the characteristic of k is not 2 and consider the matrices

$$i = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad j = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}, \quad a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

(a) Prove that i and j are primitive idempotents in A^G but do not belong to the same point of A^G. Show that a defines an inner automorphism $\mathrm{Inn}(a)$ which is an automorphism of G-algebras, but permutes the idempotents i and j.

(b) Prove that A has two different interior G-algebra structures which induce the above G-algebra structure. Moreover show that $\mathrm{Inn}(a)$ is not an automorphism of interior G-algebras.

(12.2) Let A be an interior G-algebra. Prove that there exists a unique unitary exomorphism of interior G-algebras $\mathcal{F} : \mathcal{O}G \to A$ and that $\mathcal{F}$ consists of a single homomorphism. Deduce that the group of (outer) automorphisms of $\mathcal{O}G$ is trivial.

(12.3) Find an example of a G-algebra A and two idempotents $i, i' \in A^G$ such that iAi and $i'Ai'$ are isomorphic G-algebras, but i and i' are not conjugate in A^G. [Hint: Consider the direct product of two isomorphic G-algebras.]

(12.4) Let P be a p-subgroup of G, let $\mathcal{F} : A \to B$ be an embedding of G-algebras, and let $\mathcal{F}^P : A^P \to B^P$ be the embedding of $\mathcal{O}$-algebras obtained by restriction. Prove that $\mathcal{F}$ induces an embedding of k-algebras $\overline{\mathcal{F}}(P) : \overline{A}(P) \to \overline{B}(P)$ such that $\overline{\mathcal{F}}(P)\, br_P^A = br_P^B\, \mathcal{F}^P$.

Notes on Section 12

The main results of this section and the idea of working systematically with exomorphisms and embeddings are due to Puig [1981, 1984].

§ 13 POINTED GROUPS AND MULTIPLICITY MODULES

We define in this section the fundamental concept of pointed group and we discuss the various objects attached to every pointed group. Then we introduce the order relation between pointed groups and describe it in the special case of modules.

Let A be a G-algebra. We consider the points in each algebra of fixed elements A^H (where H runs over the set of subgroups of G). A *pointed group on* A is defined to be a pair (H,α), where H is a subgroup of G and $\alpha \in \mathcal{P}(A^H)$ is a point of A^H. One of the fundamental ideas is to treat pointed groups as a generalization of subgroups, for instance by introducing a partial order relation between pointed groups on A. Thus we think of a pointed group as a subgroup together with some additional structure, namely a point. For this reason, a pointed group (H,α) will always be written H_α. The set of all pointed groups on A is a finite set, written $\mathcal{PG}(A)$.

With any pointed group H_α on A are associated several mathematical objects which we now describe. First, following Theorem 4.3, we have the maximal ideal $\mathfrak{m}_\alpha$ of A^H corresponding to α, the simple quotient $S(\alpha) = A^H/\mathfrak{m}_\alpha$, and the quotient map $\pi_\alpha : A^H \to S(\alpha)$. The simple k-algebra $S(\alpha)$ is called the *multiplicity algebra* of the pointed group H_α. If we write $S(\alpha) \cong \mathrm{End}_k(V(\alpha))$, then the simple A^H-module $V(\alpha)$ is called a *multiplicity module* of H_α. We are going to see below that $S(\alpha)$ and $V(\alpha)$ carry more structure, coming from the group G. Recall from 4.13 that we also have an ideal $A^H\alpha A^H$, which is minimal with respect to the property $A^H\alpha A^H + \mathfrak{m}_\alpha = A^H$ and satisfies $A^H\alpha A^H \subseteq \mathfrak{m}_\beta$ for every point $\beta \in \mathcal{P}(A^H)$ different from α (that is, for every pointed group H_β different from H_α).

The next fundamental object is the localization of A with respect to H_α, which is written A_α. The first approach consists in defining A_α to be the $\mathcal{O}$-algebra iAi, where $i \in \alpha$ is an arbitrary idempotent in α. Since i is fixed under H (because α is a point of A^H), the group H acts on iAi so that iAi is an H-algebra. If A is an interior G-algebra, then iAi is an interior H-algebra (via the map $H \to (iAi)^*$, $h \mapsto i{\cdot}h = h{\cdot}i = i{\cdot}h{\cdot}i$). If we choose another idempotent $j \in \alpha$, then j is conjugate to i by some element $a \in (A^H)^*$. It follows that conjugation by a induces an isomorphism of H-algebras $jAj \cong iAi$ (commuting with the action of H because a is fixed under H). Thus we see that, up to isomorphism, the localization A_α is independent of the choice of $i \in \alpha$. Note that since i is primitive in A^H, then $(iAi)^H = iA^Hi$ is a local ring.

However, we wish to have a concept which is unique up to a *unique* exo-isomorphism, and therefore we follow the same route as in Section 8. Given a pointed group H_α on a G-algebra A, we define an *embedding* *associated* with H_α to be an embedding of H-algebras $\mathcal{F} : B \to \operatorname{Res}^G_H(A)$ such that $f(1_B) \in \alpha$ for some $f \in \mathcal{F}$ (hence for every $f \in \mathcal{F}$). To show the existence of such an embedding, it suffices to choose $i \in \alpha$ and consider the embedding containing the inclusion $iAi \to A$. Uniqueness follows from the next lemma.

(13.1) LEMMA. *Let $\mathcal{F} : B \to \operatorname{Res}^G_H(A)$ and $\mathcal{F}' : B' \to \operatorname{Res}^G_H(A)$ be two embeddings associated with a pointed group H_α on a G-algebra A. Then there exists a unique exo-isomorphism of H-algebras $\mathcal{E} : B' \to B$ such that $\mathcal{F}' = \mathcal{F} \cdot \mathcal{E}$.*

Proof. The argument is the same as that of Lemma 8.3, using only conjugations by elements fixed under H. □

Note that an embedding $\mathcal{F} : B \to \operatorname{Res}^G_H(A)$ associated with H_α is in general not an embedding associated with a point of A (as introduced for $\mathcal{O}$-algebras in Section 8), because α need not be a point of A (an idempotent $i \in \alpha$ is not necessarily primitive in A). But the restriction to H-fixed elements $\mathcal{F}^H : B^H \to A^H$ is an embedding associated with the point α, in the sense of Section 8.

If $\mathcal{F} : B \to \operatorname{Res}^G_H(A)$ is an embedding associated with a pointed group H_α, the H-algebra B will be called a *localization* of A with respect to H_α and will be written A_α. The embedding $\mathcal{F}$ will usually be written $\mathcal{F}_\alpha : A_\alpha \to \operatorname{Res}^G_H(A)$. We emphasize that there are two notions: the localization A_α is simply an H-algebra (unique up to exo-isomorphism), while an embedding associated with H_α is a pair $(A_\alpha, \mathcal{F}_\alpha)$ (unique up to a unique exo-isomorphism).

In the special case of endomorphism algebras of $\mathcal{O}G$-lattices, we know that embeddings correspond to the notion of direct summand of lattices (Proposition 12.5). It is often convenient to deal with a lattice which is isomorphic to a direct summand without being a genuine direct summand. We have a similar situation in the definition above since we have allowed the localization A_α to be isomorphic to a subalgebra of A without being a genuine subalgebra. This will turn out to be extremely useful in the development of the theory.

If a G-algebra A has the property that A^G is a local ring, it will be called a *primitive* G-algebra. This is equivalent to requiring that A^G has a single point with multiplicity one. For example for any pointed group H_α on a G-algebra A, the H-algebra A_α is a primitive H-algebra. It should be noted that this notion has nothing to do with the ring-theoretic concept of primitive ring (that is, a ring having a faithful simple module). In fact, if an $\mathcal{O}$-algebra in our sense is a primitive ring, then it is a simple k-algebra by Theorem 2.7.

Up to now the action of the group G has been little used. We first note that G acts on the set of pointed groups: if H_α is a pointed group on A and if $g \in G$, then ${}^g(H_\alpha) = ({}^gH)_{{}^g\alpha}$ where ${}^gH = gHg^{-1}$ is the conjugate subgroup and ${}^g\alpha$ is the image of α under the action of g (note that ${}^g(A^H) = A^{{}^gH}$ so that ${}^g\alpha$ is indeed a point of $A^{{}^gH}$). The stabilizer of H_α is written $N_G(H_\alpha)$ and is called the *normalizer* of the pointed group H_α. It is a subgroup of the normalizer $N_G(H)$ of the subgroup H. Moreover $H \leq N_G(H_\alpha)$ because H normalizes H and acts trivially on A^H. If A is an interior G-algebra, then we know that A^H is an interior $C_G(H)$-algebra. Therefore the action of an element $g \in C_G(H)$ on a point α of A^H is by conjugation by the element $g\cdot 1_A \in A^H$. By definition of a point, we then have ${}^g\alpha = \alpha$, and it follows that $C_G(H) \leq N_G(H_\alpha)$. Thus we have proved the following result.

(13.2) LEMMA. *Let A be a G-algebra and let H_α be a pointed group on A. Then we have $H \leq N_G(H_\alpha) \leq N_G(H)$. If moreover A is an interior G-algebra, then $HC_G(H) \leq N_G(H_\alpha)$.*

One can even slightly improve this result if A is an interior G-algebra. If $g \in N_G(H)$ centralizes the image of H in A (but not necessarily H itself), then $g\cdot 1_A \in A^H$ and therefore $g \in N_G(H_\alpha)$. If $C_G(H\cdot 1_A)$ denotes the centralizer of $H\cdot 1_A$ in G, then we have equality $C_G(H\cdot 1_A) = C_G(H)$ if for instance the map $G \to A^*$ is injective. But $C_G(H\cdot 1_A)$ is in general larger than $C_G(H)$ and we have $C_G(H\cdot 1_A) \cap N_G(H) \leq N_G(H_\alpha)$, which improves Lemma 13.2. However, the isomorphism type of the group $H\cdot 1_A$ is not invariant under embeddings, because for $h \in H$ and for some idempotent i of A, we may have $h\cdot 1_A \neq 1_A$ but $h\cdot i = i$. Therefore the group $C_G(H\cdot 1_A)$ is not invariant under embeddings (whereas $N_G(H_\alpha)$ is, as we shall see in Section 15). For this reason we usually only work with $C_G(H)$ when dealing with the interior algebra structure on A^H.

We now describe the extra structure of the multiplicity algebra $S(\alpha)$ and the multiplicity module $V(\alpha)$ of a pointed group H_α on A. Since the group $N_G(H_\alpha)$ stabilizes α by definition, it stabilizes the maximal ideal $\mathfrak{m}_\alpha$. Therefore $N_G(H_\alpha)$ acts on the quotient $S(\alpha) = A^H/\mathfrak{m}_\alpha$. In other words, $S(\alpha)$ is an $N_G(H_\alpha)$-algebra. Since H acts trivially on A^H, it is also convenient to view $S(\alpha)$ as an $\overline{N}_G(H_\alpha)$-algebra, where $\overline{N}_G(H_\alpha) = N_G(H_\alpha)/H$. We now use in an essential way our assumption that the residue field $k = \mathcal{O}/\mathfrak{p}$ is algebraically closed. By Proposition 1.7, $S(\alpha) \cong \mathrm{End}_k(V(\alpha))$ for some simple $S(\alpha)$-module $V(\alpha)$ and the centre of $S(\alpha)$ is equal to $k \cdot 1_{S(\alpha)}$. Therefore we can apply Example 10.8 to conclude that the multiplicity module $V(\alpha)$ can be canonically endowed with a module structure over a twisted group algebra $k_\sharp\widehat{\overline{N}}_G(H_\alpha)$ which is associated with $S(\alpha)$. Instead of passing to the quotient by H, it is also possible if necessary to view $S(\alpha)$ as an $N_G(H_\alpha)$-algebra and $V(\alpha)$ as a module over the corresponding twisted group algebra $k_\sharp \widehat{N}_G(H_\alpha)$.

If A is an interior G-algebra, then A^H is an interior $C_G(H)$-algebra, and therefore so is its quotient $S(\alpha)$. In other words $V(\alpha)$ is a module over the group algebra $kC_G(H)$ and we are precisely in the situation of Example 10.9. Of course the corresponding $C_G(H)$-algebra structure of $S(\alpha)$ is the same as the one obtained by restriction from the canonical $N_G(H_\alpha)$-algebra structure. However, there is in general no way of extending the interior structure from $C_G(H)$ to $N_G(H_\alpha)$. The central extension $\widehat{N}_G(H_\alpha)$ of the group $N_G(H_\alpha)$ can be mapped into $S(\alpha)^*$ by a group homomorphism which extends the map $C_G(H) \to S(\alpha)^*$. Thus the multiplicity module $V(\alpha)$ is endowed with a $k_\sharp \widehat{N}_G(H_\alpha)$-module structure which extends the given $kC_G(H)$-module structure.

The $N_G(H_\alpha)$-algebra structure on $S(\alpha)$ is trivial on restriction to H , but the interior $C_G(H)$-algebra structure on $S(\alpha)$ does not in general pass to the quotient by H . Indeed if $h \in H \cap C_G(H) = Z(H)$, we only know that $h{\cdot}1_{S(\alpha)}$ acts trivially on $S(\alpha)$, and this means that $h{\cdot}1_{S(\alpha)} \in k$, the centre of $S(\alpha)$. Since any finite multiplicative subgroup of k^* is cyclic, $Z(H){\cdot}1_{S(\alpha)}$ is cyclic, but not necessarily trivial. However, there is one important special case where one can pass to the quotient by H , namely when H is a p-group. Indeed $Z(H){\cdot}1_{S(\alpha)}$ is then a p-subgroup of k^* , forcing $Z(H){\cdot}1_{S(\alpha)} = \{1\}$ because there is no non-trivial p-th root of unity in a field of characteristic p (since 1 is the only root of the polynomial $X^{p^m} - 1 = (X-1)^{p^m}$). Thus in that case the $\overline{N}_G(H_\alpha)$-algebra structure on $S(\alpha)$ is interior on restriction to $\overline{C}_G(H) = HC_G(H)/H \cong C_G(H)/Z(H)$. Therefore if H is a p-group, the multiplicity module $V(\alpha)$ is endowed with a $k_\sharp \widehat{\overline{N}}_G(H_\alpha)$-module structure which extends the given $k\overline{C}_G(H)$-module structure.

By the *multiplicity module* $V(\alpha)$ of a pointed group H_α , we shall always mean the k-vector space $V(\alpha)$ endowed with its $k_\sharp \widehat{\overline{N}}_G(H_\alpha)$-module structure. Similarly the *multiplicity algebra* $S(\alpha)$ always comes equipped with its $\overline{N}_G(H_\alpha)$-algebra structure, and with its interior $C_G(H)$-algebra structure in the interior case.

Having concentrated for some time on a single pointed group, we now introduce a relation between different pointed groups. It is an order relation on $\mathcal{PG}(A)$ which is a refinement of the order relation between subgroups. If $K \leq H$, recall that $r_K^H : A^H \to A^K$ denotes the inclusion map. If H_α and K_β are pointed groups on A , then we say that K_β is *contained in* H_α and we write $K_\beta \leq H_\alpha$ if $K \leq H$ and for some $i \in \alpha$, there exists $j \in \beta$ such that j appears in a decomposition of $r_K^H(i)$. We first give equivalent characterizations of this relation. One of them uses the surjection $\pi_\beta : A^K \to S(\beta)$ and another uses the ideal $(r_K^H)^{-1}(\mathfrak{m}_\beta)$ of A^H .

(13.3) LEMMA. *Let A be a G-algebra and let H_α and K_β be two pointed groups on A. Assume that $K \leq H$. The following conditions are equivalent.*

(a) $K_\beta \leq H_\alpha$.

(b) For every $i \in \alpha$, there exists $j \in \beta$ such that j appears in a decomposition of $r^H_K(i)$.

(c) $\pi_\beta(r^H_K(\alpha)) \neq \{0\}$.

(d) $(r^H_K)^{-1}(\mathfrak{m}_\beta) \subseteq \mathfrak{m}_\alpha$.

Proof. (a) $\Leftrightarrow$ (b). It suffices to conjugate by some element of A^H (which is also fixed under K).

(a) $\Rightarrow$ (c). The primitive idempotents $j \in \beta$ are precisely those which are not mapped to zero by π_β. Therefore $0 \neq \pi_\beta(j) = \pi_\beta(r^H_K(i)j)$ and this forces $\pi_\beta(r^H_K(i)) \neq 0$.

(c) $\Rightarrow$ (d). There exists $i \in \alpha$ such that $\pi_\beta(r^H_K(i)) \neq \{0\}$, that is, $r^H_K(i) \notin \mathfrak{m}_\beta$. Therefore we have $i \notin (r^H_K)^{-1}(\mathfrak{m}_\beta)$ and by Corollary 4.10 we obtain $(r^H_K)^{-1}(\mathfrak{m}_\beta) \subseteq \mathfrak{m}_\alpha$.

(d) $\Rightarrow$ (a). Let $i \in \alpha$. Then $i \notin \mathfrak{m}_\alpha$ and so $r^H_K(i) \notin \mathfrak{m}_\beta$ by assumption. Since all primitive idempotents outside β belong to $\mathfrak{m}_\beta$ (see Theorem 4.3), at least one idempotent in β must appear in a decomposition of $r^H_K(i)$. □

We have purposely stressed the role of the restriction map r^H_K, but as we shall often free ourselves from the use of this map, we now restate the conditions of the lemma.

(a) - (b) For some (respectively every) $i \in \alpha$, there exists $j \in \beta$ such that $j = iji$.

(c) $\pi_\beta(\alpha) \neq \{0\}$.

(d) $\mathfrak{m}_\beta \cap A^H \subseteq \mathfrak{m}_\alpha$.

It is clear from either the definition or (d) that the relation $\leq$ is reflexive and transitive. Moreover if $K_\beta \leq H_\alpha$ and $H_\alpha \leq K_\beta$, then $K = H$ and (d) implies that $\mathfrak{m}_\alpha = \mathfrak{m}_\beta$, that is, $\alpha = \beta$. Therefore the relation $\leq$ is a partial order relation on $\mathcal{PG}(A)$. It is easily seen that $\leq$ is compatible with the action of G (see Exercise 13.4). We also write $H_\alpha \geq K_\beta$ instead of $K_\beta \leq H_\alpha$, and $K_\beta < H_\alpha$ when $K_\beta \leq H_\alpha$ and $K_\beta \neq H_\alpha$. If A is a primitive G-algebra and if $\alpha = \{1_A\}$ denotes the unique point of A^G, then any pointed group H_β on A is contained in G_α because every idempotent $i \in A^H$ satisfies $1_A i 1_A = i$.

(13.4) EXAMPLE. Let M be an $\mathcal{O}G$-module and $A = \mathrm{End}_{\mathcal{O}}(M)$. Recall from 10.6 that A is an interior G-algebra. If H is a subgroup of G, then an endomorphism $f \in A$ is fixed under H if and only if f commutes with every element of H, that is, if and only if f is an $\mathcal{O}H$-linear endomorphism of M. Therefore $A^H = \mathrm{End}_{\mathcal{O}H}(M)$. Consequently an idempotent i in A^H is the same thing as a projection onto a direct summand of $\mathrm{Res}^G_H(M)$ (that is, M considered as an $\mathcal{O}H$-module by restriction). Moreover i is primitive in A^H if and only if the corresponding direct summand iM is indecomposable as an $\mathcal{O}H$-module. Note in particular that A is a primitive G-algebra if and only if M is an indecomposable $\mathcal{O}G$-module. Now two direct summands iM and jM of $\mathrm{Res}^G_H(M)$ are isomorphic if and only if the corresponding idempotents i and j are conjugate in A^H (see Corollary 4.5). Therefore a point α of A^H corresponds to an isomorphism class of indecomposable direct summands of $\mathrm{Res}^G_H(M)$. We write M_α for such a direct summand, so that $M_\alpha \cong iM \cong jM$. Note that up to isomorphism, the localization A_α is the endomorphism algebra of M_α because for $i \in \alpha$, we have $iAi \cong \mathrm{End}_{\mathcal{O}}(iM)$ by Lemma 12.4.

The *inertial subgroup* $N_G(H, M_\alpha)$ of the $\mathcal{O}H$-module M_α is by definition the subgroup of $N_G(H)$ consisting of all $g \in N_G(H)$ such that $M_\alpha \cong {}^g(M_\alpha)$, where ${}^g(M_\alpha)$ denotes the *conjugate module* (that is, the module structure on ${}^g(M_\alpha)$ is obtained by first applying $\mathrm{Conj}(g^{-1})$ and then the old module structure of M_α). Now the stabilizer $N_G(H_\alpha)$ of the pointed group H_α is equal to the inertial subgroup $N_G(H, M_\alpha)$ of M_α. This follows from the observation that the direct summand $M_{{}^g\alpha}$ corresponding to the conjugate pointed group ${}^g(H_\alpha)$ is precisely the conjugate module ${}^g(M_\alpha)$, and that ${}^g(M_\alpha) \cong M_\alpha$ if and only if ${}^g\alpha = \alpha$ (Corollary 4.5).

The order relation between pointed groups on $A = \mathrm{End}_{\mathcal{O}}(M)$ is now easy to interpret: it corresponds for indecomposable modules to the property of being isomorphic to a direct summand of the restriction. More precisely let H_α and K_β be pointed groups on A, corresponding to direct summands M_α and M_β respectively. Let $i \in \alpha$ and suppose that $K \leq H$. Then by condition (a) in Lemma 13.3, $K_\beta \leq H_\alpha$ if and only if there exists $j \in \beta$ such that jM is a direct summand of $\mathrm{Res}^H_K(iM)$, that is, M_β is isomorphic to a direct summand of $\mathrm{Res}^H_K(M_\alpha)$.

We shall usually restrict to the case of $\mathcal{O}G$-lattices (but this is no restriction when $\mathcal{O} = k$). If M is an $\mathcal{O}G$-lattice, any direct summand iM of M is again an $\mathcal{O}G$-lattice, because a direct summand of a free $\mathcal{O}$-module is free by Corollary 1.4. This fundamental example has several special features, the first being that $A = \mathrm{End}_{\mathcal{O}}(M)$ is an $\mathcal{O}$-simple algebra. As we have seen in Proposition 12.5, embeddings are unique whenever they exist and the existence of an embedding $\mathrm{End}_{\mathcal{O}}(M) \to \mathrm{End}_{\mathcal{O}}(L)$ is equivalent to the property that M is isomorphic to a direct summand of L. Also there is a unique minimal pointed group 1_α (where 1 denotes the trivial subgroup), because A is $\mathcal{O}$-simple and hence $A = A^1$ has a unique point α.

(13.5) EXAMPLE. The previous example can be extended without essential change to the case of modules over a twisted group algebra. Let A be a G-algebra which is $\mathcal{O}$-simple, so that $A = \mathrm{End}_{\mathcal{O}}(M)$ for some free $\mathcal{O}$-module M. Then by Example 10.8, M is endowed with a module structure over a twisted group algebra $\mathcal{O}_\sharp \widehat{G}$. For any subgroup H of G, there is a subalgebra $\mathcal{O}_\sharp \widehat{H}$ of $\mathcal{O}_\sharp \widehat{G}$: the inverse image $\widehat{H}$ of H in $\widehat{G}$ is a central extension of H by $\mathcal{O}^*$ and the corresponding twisted group algebra is clearly a subalgebra of $\mathcal{O}_\sharp \widehat{G}$. By the construction of the action of $\mathcal{O}_\sharp \widehat{G}$ on M, we see that $f \in A^H$ if and only if f commutes with every element of $\mathcal{O}_\sharp \widehat{H}$, that is, if and only if f is an $\mathcal{O}_\sharp \widehat{H}$-linear endomorphism of M. Therefore $A^H = \mathrm{End}_{\mathcal{O}_\sharp \widehat{H}}(M)$, as in the previous example, and all the observations of that example remain valid. Thus a primitive idempotent i of A^H is a projection onto an indecomposable direct summand of $\mathrm{Res}^G_H(M)$, where for simplicity we write $\mathrm{Res}^G_H(M)$ instead of $\mathrm{Res}^{\mathcal{O}_\sharp \widehat{G}}_{\mathcal{O}_\sharp \widehat{H}}(M)$. Again a point of A^H corresponds to an isomorphism class of indecomposable direct summands of $\mathrm{Res}^G_H(M)$, and the order relation between pointed groups is interpreted as before.

The reader who is familiar with a module-theoretic approach to representation theory can use these two examples as both a motivation and a guide for the more general treatment of pointed groups on G-algebras. In the examples, the condition that jV be a direct summand of $\mathrm{Res}^H_K(iV)$ can be reinterpreted in terms of algebras by the fact that the subalgebra $jAj \cong \mathrm{End}_{\mathcal{O}}(jV)$ embeds into $iAi \cong \mathrm{End}_{\mathcal{O}}(iV)$. This translation of a condition on modules to a property of algebras has the advantage of being applicable to any G-algebra. In other words the order relation can be restated in terms of localizations. We now prove this, using the conceptual approach to localization which was introduced above.

(13.6) PROPOSITION. *Let H_α and K_β be two pointed groups on a G-algebra A and let $\mathcal{F}_\alpha : A_\alpha \to \mathrm{Res}^G_H(A)$ and $\mathcal{F}_\beta : A_\beta \to \mathrm{Res}^G_K(A)$ be embeddings associated with H_α and K_β respectively. Assume that $K \leq H$. Then $K_\beta \leq H_\alpha$ if and only if there exists an exomorphism $\mathcal{E} : A_\beta \to \mathrm{Res}^H_K(A_\alpha)$ such that the following diagram of exomorphisms* *commutes.*

$$\begin{array}{ccc} A_\beta & \xrightarrow{\mathcal{F}_\beta} & \mathrm{Res}^G_K(A) \\ \mathcal{E}\big\downarrow & \nearrow_{\mathrm{Res}^H_K(\mathcal{F}_\alpha)} & \\ \mathrm{Res}^H_K(A_\alpha) & & \end{array}$$

If this condition is satisfied, the exomorphism $\mathcal{E}$ is an embedding and is unique.

Proof. Assume that $K_\beta \leq H_\alpha$. Let $i \in \alpha$ and $j \in \beta$ be such that $ij = j = ji$. By Lemma 13.1, we can assume that $A_\alpha = iAi$ and $A_\beta = jAj$, and that $\mathcal{F}_\alpha$ and $\mathcal{F}_\beta$ are the exomorphisms determined by the inclusions into A. Let $\mathcal{E}$ be the exomorphism containing the inclusion $jAj \subseteq iAi$. Then clearly $\mathrm{Res}^H_K(\mathcal{F}_\alpha)\,\mathcal{E} = \mathcal{F}_\beta$.

Conversely assume that $\mathcal{E}$ exists and let $e \in \mathcal{E}$, $f_\alpha \in \mathcal{F}_\alpha$. Then $e(1_{A_\beta})$ is an idempotent in A^K_α and its image $j = f_\alpha\, e(1_{A_\beta})$ belongs to the point β of A^K, because $f_\alpha\, e \in \mathcal{F}_\beta$ by commutativity of the diagram and the fact that $\mathcal{F}_\beta$ is an embedding associated with K_β. Moreover $i = f_\alpha(1_{A_\alpha})$ belongs to α. Since $1_{A_\alpha} e(1_{A_\beta}) = e(1_{A_\beta}) = e(1_{A_\beta})\, 1_{A_\alpha}$, we obtain $ij = j = ji$. This proves that $K_\beta \leq H_\alpha$.

Finally the uniqueness of $\mathcal{E}$ and the fact that it is an embedding is an immediate application of Proposition 12.2. □

The unique embedding appearing in Proposition 13.6 will usually be written $\mathcal{F}^\alpha_\beta : A_\beta \to \mathrm{Res}^H_K(A_\alpha)$. This embedding expresses the property $K_\beta \leq H_\alpha$.

Exercises

(13.1) Let M be an $\mathcal{O}G$-module and let $A = \mathrm{End}_{\mathcal{O}}(M)$ be the corresponding interior G-algebra. Prove that A is primitive if and only if M is an indecomposable $\mathcal{O}G$-module.

(13.2) Let H be a subgroup of G. By constructing suitable examples of G-algebras, prove that any subgroup K such that $H \leq K \leq N_G(H)$ can be realized as the normalizer $N_G(H_\alpha)$ of a pointed group. State and prove a similar result for interior G-algebras.

(13.3) Let A be an interior G-algebra, let P be a p-subgroup of G, and let P_γ be a pointed group on A. Let $H = C_G(P{\cdot}1_A) \cap N_G(P)$ and $\overline{H} = PH/P$. Show that on restriction to $\overline{H}$, the multiplicity algebra $S(\gamma)$ of P_γ is an interior $\overline{H}$-algebra, so that the multiplicity module $V(\gamma)$ is a $k\overline{H}$-module.

(13.4) Let H_α and K_β be pointed groups on a G-algebra A and let $g \in G$. Show that if $H_\alpha \geq K_\beta$, then ${}^g(H_\alpha) \geq {}^g(K_\beta)$.

(13.5) Let A be a G-algebra.

(a) Let H_α be a pointed group on A and K a subgroup of H. Show that there exists a point $\beta \in \mathcal{P}(A^K)$ such that $K_\beta \leq H_\alpha$.

(b) Let K_β be a pointed group on A and H a subgroup of G containing K. Show that there exists a point $\alpha \in \mathcal{P}(A^H)$ such that $K_\beta \leq H_\alpha$.

(c) Let H_α and L_γ be pointed groups on A with $L_\gamma \leq H_\alpha$ and let K be a subgroup of H containing L. Show that there exists a point $\beta \in \mathcal{P}(A^K)$ such that $L_\gamma \leq K_\beta \leq H_\alpha$.

(13.6) Let A be a G-algebra. Recall that m_α denotes the multiplicity of a point α.

(a) Let H_α and K_β be pointed groups on A such that $K_\beta \leq H_\alpha$. Prove that $m_\beta \geq m_\alpha$.

(b) Let K_β be a pointed group on A with $m_\beta = 1$. Prove that there exists a unique pointed group H_α such that $K_\beta \leq H_\alpha$. Moreover $m_\alpha = 1$.

Notes on Section 13

Pointed groups were first introduced by Puig [1981], refining the notion of Brauer pairs due to Alperin and Broué [1979]. Multiplicity modules appear in Puig [1988a].

§ 14 RELATIVE PROJECTIVITY AND LOCAL POINTS

We define in this section another relation between pointed groups, called relative projectivity, by making use of the relative trace map. Then we introduce the crucial notion of local pointed group and we prove an elementary but essential property of local pointed groups.

Let A be a G-algebra. For the definition of the order relation $\leq$ between pointed groups, one only needs the restriction maps $r_K^H : A^H \to A^K$. We now use the relative trace maps $t_K^H : A^K \to A^H$. Given two pointed groups H_α and K_β on A, we say that H_α is *projective relative to* K_β, and we write $H_\alpha\, pr\, K_\beta$, if $H \geq K$ and $\alpha \subseteq t_K^H(A^K \beta A^K)$. We know that $t_K^H(A^K \beta A^K)$ is an ideal (by 11.1), so this is equivalent to requiring that some $i \in \alpha$ belongs to this ideal. For the same reason, the relation can also be written $A^H \alpha A^H \subseteq t_K^H(A^K \beta A^K)$, and this makes clear that pr is an order relation beween pointed groups. The order relation pr is easily seen to be compatible with the action of G (see Exercise 14.1).

Recall that the ideal $A^K \beta A^K$ is the set of all finite sums $\sum_r a_r j b_r$ where $a_r, b_r \in A^K$ and $j \in \beta$. We show that one can get rid of sums for the definition of relative projectivity of pointed groups.

(14.1) LEMMA. *Let A be a G-algebra, let H_α and K_β be two pointed groups on A, let $i \in \alpha$ and $j \in \beta$, and assume that $K \leq H$. Then $H_\alpha\, pr\, K_\beta$ if and only if there exist $a, b \in A^K$ such that $i = t_K^H(ajb)$.*

Proof. If $i = t_K^H(ajb)$, it is clear from the definition that $H_\alpha\, pr\, K_\beta$. If conversely $H_\alpha\, pr\, K_\beta$, then $i = \sum_{r=1}^n t_K^H(a_r j b_r)$ for some positive integer n and some $a_r, b_r \in A^K$. Multiplying on both sides by i, we have

$$i = \sum_{r=1}^{n} i\, t_K^H(a_r j b_r) i = \sum_{r=1}^{n} t_K^H(i a_r j b_r i) .$$

Since i is a primitive idempotent of A^H, the ring $iA^H i$ is local with unity element i (Corollary 4.6). Therefore there exists an index r such that $t_K^H(i a_r j b_r i)$ is invertible, so that

$$i = t_K^H(i a_r j b_r i) c = t_K^H(i a_r j b_r i c)$$

for some $c \in iA^H i$. This proves the result since $ia_r, b_r ic \in A^K$. □

A pointed group H_α is said to be *projective relative to* K if it is projective relative to K_β for some $\beta \in \mathcal{P}(A^K)$. Also H_α is called *projective* if it is projective relative to the trivial subgroup 1. In that case one also says that α is a *projective point* of A^H. There is a more direct way of detecting the projectivity relative to a subgroup. Recall that $A_K^H = t_K^H(A^K)$ is an ideal of A^H (by 11.1).

(14.2) LEMMA. *A pointed group H_α is projective relative to K if and only if $K \leq H$ and $\alpha \subseteq A_K^H$. In particular H_α is projective if and only if $\alpha \subseteq A_1^H$.*

Proof. If H_α is projective relative to K, it is clear that $K \leq H$ and $\alpha \subseteq A_K^H$. Assume now that $K \leq H$ and $\alpha \subseteq A_K^H$. Choosing a primitive decomposition of 1_{A^K} and multiplying by A^K on both sides, one obtains $A^K = \sum_{\beta \in \mathcal{P}(A^K)} A^K \beta A^K$, and therefore

$$A_K^H = \sum_{\beta \in \mathcal{P}(A^K)} t_K^H(A^K \beta A^K).$$

Applying Rosenberg's lemma (Proposition 4.9) to some $i \in \alpha$, we have $i \in t_K^H(A^K \beta A^K)$ for some β and so $\alpha \subseteq t_K^H(A^K \beta A^K)$ as required. □

If H is a subgroup of G, we say that a G-algebra A is *projective relative* to H if the relative trace map $t_H^G : A^H \to A^G$ is surjective. Since the image A_H^G of the relative trace map is an ideal, this is equivalent to requiring that $1_A \in A_H^G$. Also by Lemma 14.2, A is projective relative to H if and only if every pointed group on A of the form G_α is projective relative to H. Thus this new definition is a global analogue of the one introduced for pointed groups. We also say that a G-algebra A is *projective* if it is projective relative to the trivial subgroup 1. The following easy result is often useful.

(14.3) LEMMA. *Let A be a G-algebra and assume that A is projective relative to a subgroup H. Then $A \otimes_{\mathcal{O}} B$ is projective relative to H for any G-algebra B. In particular $A \otimes_{\mathcal{O}} B$ is projective if A is projective.*

Proof. By assumption there exists $a \in A^H$ such that $t_H^G(a) = 1_A$. Thus we have

$$\begin{aligned} t_H^G(a \otimes 1_B) &= \sum_{g \in [G/H]} {}^g a \otimes {}^g 1_B = \sum_{g \in [G/H]} {}^g a \otimes 1_B \\ &= t_H^G(a) \otimes 1_B = 1_A \otimes 1_B = 1_{A \otimes B}, \end{aligned}$$

proving the result. □

One of the important ideas of the defect theory of pointed groups (see Section 18) is to write a primitive idempotent $i \in A^H$ as an image of a trace map $i = t_Q^H(a)$ for a subgroup Q as small as possible. We are now interested in the extreme case where this is not possible for any proper subgroup Q of H. By Lemma 11.7, this forces H to be a p-subgroup, which we write as P instead of H.

(14.4) LEMMA. *Let P be a subgroup of G and let P_γ be a pointed group on a G-algebra A. The following conditions are equivalent.*
(a) P_γ *is minimal with respect to the relation* pr .
(b) P_γ *is not projective relative to a proper subgroup of* P .
(c) $\gamma \not\subseteq \sum_{Q<P} A_Q^P$.
(d) $br_P(\gamma) \neq \{0\}$.
(e) $\mathrm{Ker}(br_P) \subseteq \mathfrak{m}_\gamma$.
If these conditions are satisfied, then P *is a* p*-group.*

Proof. It is clear that (a) and (b) are equivalent. The equivalence of (b) and (c) follows from Lemma 14.2 and Rosenberg's lemma (Proposition 4.9). Since we always have $\mathfrak{p}A^P \subseteq \mathfrak{m}_\gamma$ (because $J(A^P) \subseteq \mathfrak{m}_\gamma$), we have $\gamma \not\subseteq \mathfrak{p}A^P$ (see Corollary 4.10) and therefore (c) holds if and only if

$$\gamma \not\subseteq \mathfrak{p}A^P + \sum_{Q<P} A_Q^P = \mathrm{Ker}(br_P) ,$$

which is the statement (d). Finally (d) and (e) are equivalent thanks to Corollary 4.10 again. If these equivalent conditions are satisfied, then $\mathrm{Ker}(br_P)$ is a proper ideal of A^P and so P is a p-group by Lemma 11.7. □

A pointed group P_γ on a G-algebra A is called a *local pointed group* if it satisfies the equivalent conditions of the lemma. The corresponding point γ of A^P is called a *local point* of A^P . The word *local* has nothing to do with the localization procedure introduced before, but rather with the customary terminology for objects connected with p-subgroups of a finite group. In fact pointed groups are generalizations of subgroups and local pointed groups are generalizations of p-subgroups (Exercise 14.2).

For a fixed p-subgroup P, the set of local points of A^P is written $\mathcal{LP}(A^P)$. It should be noted that, for a point of A^P , the property of being local depends on the algebra A together with its P-action, so it is not a property depending only on the $\mathcal{O}$-algebra A^P . Thus, whereas the set of all points $\mathcal{P}(A^P)$ only depends on A^P , the set $\mathcal{LP}(A^P)$ depends on A , a fact which is not incorporated in the notation.

(14.5) LEMMA. *Let A be a G-algebra and let P be a p-subgroup of G. The Brauer homomorphism $br_P : A^P \to \overline{A}(P)$ induces a bijection $\mathcal{LP}(A^P) \stackrel{\sim}{\to} \mathcal{P}(\overline{A}(P))$.*

Proof. This is an application of part (e) of Theorem 3.2, using the characterization of local points given in part (d) of Lemma 14.4 above. In terms of maximal ideals rather than points, the result is obvious by part (e) of Lemma 14.4. □

(14.6) COROLLARY. *Let* P_γ *be a local pointed group on a* G*-algebra* A*. Then the corresponding simple quotient* $S(\gamma) = A^P/\mathfrak{m}_\gamma$ *is canonically isomorphic to a quotient of* $\overline{A}(P)$ *. Conversely any simple quotient of* $\overline{A}(P)$ *corresponds to a local point of* A^P *.*

The set of all pointed groups on a G-algebra A is a *poset* (that is, a partially ordered set) and we shall be particularly interested in the subposet of local pointed groups. The first component of a local pointed group is always a p-group, but an arbitrary p-group is not necessarily the first component of a local pointed group (see Exercises 14.2, 14.3 and 14.4). Note however that any pointed group 1_γ (where 1 denotes the trivial subgroup) is always local.

We have seen in Proposition 11.9 that the Brauer homomorphism br_P has a property linking the relative trace maps in the G-algebra A and in the $\overline{N}_G(P)$-algebra $\overline{A}(P)$. Now if γ is a local point of A^P with simple quotient $S(\gamma)$, we want to show that the canonical map $\pi_\gamma : A^P \to S(\gamma)$ has a similar property, using the $\overline{N}_G(P_\gamma)$-algebra structure of $S(\gamma)$. Since π_γ factorizes through $\overline{A}(P)$ via the Brauer homomorphism (by Corollary 14.6 above), this can be seen as a specialization of Proposition 11.9 to each local point of A^P . In the following statement, one can ignore the inclusion map r_P^H if one prefers.

(14.7) PROPOSITION. *Let* A *be a* G*-algebra, let* P_γ *be a local pointed group on* A *, and let* $\pi_\gamma : A^P \to S(\gamma)$ *be the canonical map. Then for* $a \in A^P$ *and for every subgroup* H *of* G *containing* P *, we have*

$$\pi_\gamma\, r_P^H\, t_P^H(a) = \begin{cases} t_1^{\overline{N}_H(P_\gamma)}\, \pi_\gamma(a) & \text{if } a \in A^P\gamma A^P, \\ 0 & \text{if } a \in A^P\gamma' A^P \text{ and } \gamma' \text{ is not } N_H(P)\text{-conjugate to } \gamma. \end{cases}$$

Moreover $\pi_\gamma\, r_P^H(A_P^H) = \pi_\gamma\, r_P^H(t_P^H(A^P\gamma A^P)) = S(\gamma)_1^{\overline{N}_H(P_\gamma)}$.

Proof. We use the Mackey decomposition formula 11.3 and the fact that $\pi_\gamma(A_Q^P) = 0$ if $Q < P$ (because γ is local so that we have by Lemma 14.4 $\mathrm{Ker}(br_P) \subseteq \mathfrak{m}_\gamma = \mathrm{Ker}(\pi_\gamma)$). We obtain

$$\pi_\gamma\, r_P^H\, t_P^H(a) = \sum_{h\in[P\backslash H/P]} \pi_\gamma(t_{P\cap {}^hP}^P({}^ha)) = \sum_{h\in[N_H(P)/P]} \pi_\gamma({}^ha)\,.$$

If $a \in A^P\gamma' A^P$ where $\gamma' \in \mathcal{P}(A^P)$ is not $N_H(P)$-conjugate to γ , then ${}^ha \in A^P\, {}^h\gamma' A^P$ but ${}^h\gamma' \neq \gamma$, and so $\pi_\gamma({}^ha) = 0$. Thus $\pi_\gamma\, r_P^H\, t_P^H(a) = 0$.

If now $a \in A^P \gamma A^P$, then for every $h \in N_H(P) - N_H(P_\gamma)$, we have ${}^h a \in A^P\, {}^h\gamma A^P$ but ${}^h\gamma \neq \gamma$, and so $\pi_\gamma({}^h a) = 0$. Thus we are left with a sum running over $N_H(P_\gamma)/P$ and we obtain

$$\pi_\gamma\, r_P^H\, t_P^H(a) = \sum_{h \in [N_H(P_\gamma)/P]} \pi_\gamma({}^h a) = t_P^{N_H(P_\gamma)}(\pi_\gamma(a)) = t_1^{\overline{N}_H(P_\gamma)}(\pi_\gamma(a)) \,,$$

as required.

For the second assertion, we note that $A_P^H = \sum_{\gamma' \in \mathcal{P}(A^P)} t_P^H(A^P\gamma' A^P)$ and that $t_P^H(A^P\gamma' A^P) = t_P^H(A^P\gamma A^P)$ if γ' is $N_H(P)$-conjugate to γ (because if $h \in N_H(P)$ and $a \in A^P$, we have $t_P^H({}^h a) = t_P^H(a)$). By the first part of the proposition, we obtain

$$\pi_\gamma\, r_P^H(A_P^H) = \pi_\gamma\, r_P^H\, t_P^H(A^P\gamma A^P) = t_1^{\overline{N}_H(P_\gamma)}\, \pi_\gamma(A^P\gamma A^P) \,.$$

The result follows from the observation that $\pi_\gamma(A^P\gamma A^P)$ is the whole of $S(\gamma)$, because it is a non-zero ideal in this simple algebra. □

More generally the relative trace map t_K^H is related to a relative trace map in $S(\gamma)$, provided we consider only certain elements of A^K . The previous proposition corresponds to the special case $K = P$.

(14.8) COROLLARY. *Let P_γ be a local pointed group on a G-algebra A, let $\pi_\gamma : A^P \to S(\gamma)$ be the canonical map, and let $P \leq K \leq H \leq G$. For every $a \in t_P^K(A^P\gamma A^P)$, we have*

$$\pi_\gamma\, r_P^H\, t_K^H(a) = t_{\overline{N}_K(P_\gamma)}^{\overline{N}_H(P_\gamma)}\, \pi_\gamma\, r_P^K(a) \,.$$

Proof. We write $a = t_P^K(b)$ with $b \in A^P\gamma A^P$ and we apply the proposition for both subgroups K and H . Thus we have

$$\begin{aligned}\pi_\gamma\, r_P^H\, t_K^H(a) &= \pi_\gamma\, r_P^H\, t_P^H(b) = t_1^{\overline{N}_H(P_\gamma)}\, \pi_\gamma(b) = t_{\overline{N}_K(P_\gamma)}^{\overline{N}_H(P_\gamma)}\, t_1^{\overline{N}_K(P_\gamma)}\, \pi_\gamma(b) \\ &= t_{\overline{N}_K(P_\gamma)}^{\overline{N}_H(P_\gamma)}\, \pi_\gamma\, r_P^K\, t_P^K(b) = t_{\overline{N}_K(P_\gamma)}^{\overline{N}_H(P_\gamma)}\, \pi_\gamma\, r_P^K(a) \,. \ \square\end{aligned}$$

(14.9) REMARK. In the situation of Proposition 14.7, let T be the image of the homomorphism $\pi_\gamma\, r_P^H : A^H \to S(\gamma)$. Then T is a subalgebra and is contained in $S(\gamma)^{\overline{N}_H(P_\gamma)}$, because we have a homomorphism of $N_H(P_\gamma)$-algebras and $N_H(P_\gamma) \leq H$ acts trivially on A^H . Moreover the image of the ideal A_P^H is an ideal of T which is equal to $S(\gamma)_1^{\overline{N}_H(P_\gamma)}$. But $S(\gamma)_1^{\overline{N}_H(P_\gamma)}$ is also an ideal of the larger ring $S(\gamma)^{\overline{N}_H(P_\gamma)}$, so we are in a somewhat special situation. For instance if we assume that $A_P^H = A^H$, then $S(\gamma)_1^{\overline{N}_H(P_\gamma)} = T$, so in particular 1_T belongs to this ideal. But $1_T = 1_{S(\gamma)}$ and therefore we also have $S(\gamma)_1^{\overline{N}_H(P_\gamma)} = S(\gamma)^{\overline{N}_H(P_\gamma)}$. This is a very strong condition on $S(\gamma)$ which we shall exploit later in Section 19.

Exercises

(14.1) Let H_α and K_β be pointed groups on a G-algebra A and let $g \in G$. Show that if $H_\alpha \, pr \, K_\beta$, then ${}^g(H_\alpha) \, pr \, {}^g(K_\beta)$.

(14.2) Let $A = \mathcal{O}$ with trivial G-action.
(a) Show that the poset of pointed groups on A is isomorphic to the poset of all subgroups of G.
(b) Show that the poset of local pointed groups on A is isomorphic to the poset of all p-subgroups of G.

(14.3) Let $A = \mathrm{End}_{\mathcal{O}}(M)$ where M is a free $\mathcal{O}G$-module. Show that there is a unique local pointed group on A (whose first component is the trivial subgroup). [Hint: If P is a subgroup of G, then $\mathrm{Res}_P^G(M)$ is a free $\mathcal{O}P$-module; deduce from this that the relative trace map t_1^P is surjective.]

(14.4) Take $p = 2$ and let P be the direct product of two cyclic groups of order 2, generated by g and h respectively. Let M be the 2-dimensional kP-module with a k-basis $\{v, w\}$ and an action of P defined by

$$g \cdot v = v + w, \quad g \cdot w = w, \quad h \cdot v = v + \lambda w, \quad h \cdot w = w,$$

where $\lambda \in k$, $\lambda \neq 0$, $\lambda \neq 1$. Let $A = \mathrm{End}_k(M)$. Show that there are exactly two local pointed groups on A, whose first components are 1 and P respectively. [Hint: Show that the restriction of M to any proper subgroup Q of P is a free kQ-module and apply Exercise 14.3. For the subgroup P itself, show that any $a \in A^P$ leaves $W = \langle w \rangle$ invariant, that the kernel I of the restriction map $A^P \to \mathrm{End}_k(W)$ is a nilpotent ideal of A^P with quotient isomorphic to k, and that the image of the relative trace map t_Q^P is contained in I if $Q < P$.]

Notes on Section 14

The concept of local point and its basic properties are due to Puig [1981].

§ 15 POINTS AND MULTIPLICITY MODULES VIA EMBEDDINGS

We show in this section that an embedding of G-algebras induces on the one hand a very well-behaved injective map between pointed groups, and on the other hand embeddings between multiplicity algebras as well as embeddings between Brauer quotients.

If M is a direct summand of an $\mathcal{O}G$-module N and if L is an indecomposable direct summand of M, then clearly L is also an indecomposable direct summand of N. It is this simple observation that we want to generalize to G-algebras and put in a suitable setting. Our purpose is to show that if e is a G-fixed idempotent of a G-algebra B, the inclusion $eBe \to B$ induces a well-behaved injective map between pointed groups on eBe and pointed groups on B. As before we shall work with embeddings rather than inclusions $eBe \to B$.

Let $\mathcal{F} : A \to B$ be an embedding of G-algebras. For every subgroup H of G, let $\mathcal{F}^H : A^H \to B^H$ be the corresponding embedding of $\mathcal{O}$-algebras. Then $\mathcal{F}^H$ induces an injection $\mathcal{P}(A^H) \to \mathcal{P}(B^H)$ mapping α to $\mathcal{F}^H(\alpha)$, which is a point of B^H (Proposition 8.5). For simplicity we write $\mathcal{F}(\alpha) = \mathcal{F}^H(\alpha)$, but it should be noted that this set is usually larger than the set $\{ f(i) \mid f \in \mathcal{F}, i \in \alpha \}$, which is closed under conjugation by $(B^G)^*$, but not necessarily $(B^H)^*$. In any case $\mathcal{F}(\alpha)$ is the $(B^H)^*$-conjugacy closure of $f(i)$, for any $f \in \mathcal{F}$ and $i \in \alpha$. If H_α is a pointed group on A, then $H_{\mathcal{F}(\alpha)}$ is a pointed group on B, called the *image* of H_α in B.

(15.1) PROPOSITION. *Let $\mathcal{F} : A \to B$ be an embedding of G-algebras.*

(a) *$\mathcal{F}$ induces an injective map $\mathcal{F}_* : \mathcal{PG}(A) \to \mathcal{PG}(B)$, defined by $\mathcal{F}_*(H_\alpha) = H_{\mathcal{F}(\alpha)}$.*

(b) *Let H_α and K_β be pointed groups on A. Then $H_\alpha \geq K_\beta$ if and only if $H_{\mathcal{F}(\alpha)} \geq K_{\mathcal{F}(\beta)}$. Moreover if $H_{\mathcal{F}(\alpha)} \geq K_{\beta'}$ for some pointed group $K_{\beta'}$ on B, then $\beta' = \mathcal{F}(\beta)$ for some $\beta \in \mathcal{P}(A^H)$ (and so $H_\alpha \geq K_\beta$).*

(c) *Let H_α and K_β be pointed groups on A. Then $H_\alpha \, pr \, K_\beta$ if and only if $H_{\mathcal{F}(\alpha)} \, pr \, K_{\mathcal{F}(\beta)}$.*

(d) *Let P_γ be a pointed group on A. Then P_γ is local if and only if $P_{\mathcal{F}(\gamma)}$ is local.*

(e) *Let H_α be a pointed group on A. If $g \in G$, then the image of ${}^g(H_\alpha)$ is ${}^g(H_{\mathcal{F}(\alpha)})$. In particular $N_G(H_{\mathcal{F}(\alpha)}) = N_G(H_\alpha)$.*

(f) *Let H_α be a pointed group on A. If $\mathcal{F}_\alpha : A_\alpha \to \mathrm{Res}^G_H(A)$ is an embedding associated with H_α, then $\mathrm{Res}^G_H(\mathcal{F}) \, \mathcal{F}_\alpha : A_\alpha \to \mathrm{Res}^G_H(B)$ is an embedding associated with $H_{\mathcal{F}(\alpha)}$. In other words A_α is also the localization of B with respect to the pointed group $H_{\mathcal{F}(\alpha)}$.*

Proof. (a) This is a restatement of Proposition 8.5 and the remarks above.

(b) Let $f \in \mathcal{F}$ and $i \in \alpha$. If $H_\alpha \geq K_\beta$, there exists $j \in \beta$ such that $iji = j$. Applying f to this equality shows that $H_{\mathcal{F}(\alpha)} \geq K_{\mathcal{F}(\beta)}$. Conversely if $H_{\mathcal{F}(\alpha)} \geq K_{\beta'}$, then there exists $j' \in \beta'$ such that $f(i)j'f(i) = j'$. Multiplying on both sides by $f(1_A)$, we see that $j' = f(1_A)j'f(1_A)$ belongs to $f(1_A)Bf(1_A)$, which is the image of f since $\mathcal{F}$ is an embedding. Therefore $j' = f(j)$ for some $j \in A$ and the injectivity of f shows that j is a primitive idempotent of A^K such that $iji = j$. If β is the point of A^K containing j, it follows that $\beta' = \mathcal{F}(\beta)$ and $H_\alpha \geq K_\beta$.

(c) Let $f \in \mathcal{F}$. If $\alpha \subseteq t_K^H(A^K \beta A^K)$, then

$$f(\alpha) \subseteq t_K^H\big(f(A^K)f(\beta)f(A^K)\big) \subseteq t_K^H\big(B^K f(\beta) B^K\big).$$

If conversely $f(\alpha) \subseteq t_K^H\big(B^K f(\beta) B^K\big)$, one can multiply $f(\alpha)$ and $f(\beta)$ by $f(1_A)$ on both sides to get

$$f(\alpha) \subseteq t_K^H\big(f(1_A)B^K f(1_A)f(\beta)f(1_A)B^K f(1_A)\big) = t_K^H\big(f(A^K)f(\beta)f(A^K)\big).$$

The injectivity of f yields $\alpha \subseteq t_K^H(A^K \beta A^K)$.

(d) The argument is the same as in (c), using this time the ideal $A_Q^P = \sum_{Q<P} t_Q^P(A^Q)$.

(e) The first assertion is trivial because any $f \in \mathcal{F}$ commutes with the action of G. The special case follows immediately using the injectivity of the map $\alpha \mapsto \mathcal{F}(\alpha)$.

(f) The exomorphism $\mathrm{Res}_H^G(\mathcal{F})\,\mathcal{F}_\alpha$ is an embedding, because the composite of two embeddings is an embedding. If $f \in \mathcal{F}$, $f_\alpha \in \mathcal{F}_\alpha$, then $f_\alpha(1_{A_\alpha}) = i \in \alpha$ by definition and so $f\,f_\alpha(1_{A_\alpha}) = f(i) \in \mathcal{F}(\alpha)$. Therefore $\mathrm{Res}_H^G(\mathcal{F})\,\mathcal{F}_\alpha$ is an embedding associated with the pointed group $H_{\mathcal{F}(\alpha)}$. □

Given an embedding $\mathcal{F} : A \to B$, an important simplification which will be often used consists in considering the map $\mathcal{F}_* : \mathcal{PG}(A) \to \mathcal{PG}(B)$ as an inclusion rather than an injection. In other words we shall often identify the pointed groups on A with pointed groups on B. We note that multiplicities are not preserved by this identification: the multiplicity of a point α of A^H is always smaller than or equal to the multiplicity of α considered as a point of B^H. For instance A always embeds in $B = M_n(A)$ but the multiplicities are multiplied by n (Exercise 15.2).

One crucial application of this identification occurs when we consider an embedding $\mathcal{F}_\alpha : A_\alpha \to \mathrm{Res}_H^G(A)$ associated with a pointed group H_α, which is an embedding of H-algebras. The algebra A_α^H is a local ring (that is, A_α is primitive) and its unique point $\{1_{A_\alpha}\}$ (with multiplicity one) is identified with the point α of A^H. For arbitrary pointed groups on A_α, we have the following result, which shows in particular that the containment relation between pointed groups can be read in the localization.

(15.2) PROPOSITION. *Let* $\mathcal{F}_\alpha : A_\alpha \to \mathrm{Res}^G_H(A)$ *be an embedding associated with a pointed group* H_α *on a* G*-algebra* A *. Then* $\mathcal{F}_\alpha$ *induces an isomorphism between the poset* $\mathcal{PG}(A_\alpha)$ *and the poset of all pointed groups on* A *which are contained in* H_α *.*

Proof. We have noticed above that the unique point $\alpha' = \{1_{A_\alpha}\}$ of A_α^H is mapped to the point α of A^H . By part (b) of Proposition 15.1, the set of all pointed groups on A_α which are contained in $H_{\alpha'}$ is mapped bijectively onto the set of all pointed groups on A which are contained in H_α . But any pointed group on A_α is contained in $H_{\alpha'}$ because any idempotent $i \in A_\alpha^K$ satisfies $1_{A_\alpha} i \, 1_{A_\alpha} = i$. The fact that this bijection preserves the order relation $\leq$ also follows from Proposition 15.1. □

We have noticed above that the injective map $\mathcal{F}_* : \mathcal{PG}(A) \to \mathcal{PG}(B)$ induced by an embedding $\mathcal{F} : A \to B$ does not preserve multiplicities. We now discuss the precise behaviour of multiplicity algebras and multiplicity modules. Let H_α be a pointed group on A and let $H_{\alpha'} \in \mathcal{PG}(B)$ be its image under $\mathcal{F}_*$ (here we do not identify α and α'). Let $S(\alpha)$ and $S(\alpha')$ be the respective multiplicity algebras. By Proposition 15.1, H_α and $H_{\alpha'}$ have the same normalizer $N = N_G(H_\alpha) = N_G(H_{\alpha'})$. Thus both $S(\alpha)$ and $S(\alpha')$ are $\overline{N}$-algebras, where $\overline{N} = N/H$.

We use a slight modification of the argument of Exercise 8.3 to show that the embedding $\mathcal{F} : A \to B$ induces an embedding of $\overline{N}$-algebras $\overline{\mathcal{F}}(\alpha) : S(\alpha) \to S(\alpha')$. Choose $f \in \mathcal{F}$ and consider the homomorphisms of $\overline{N}$-algebras $f^H : A^H \to B^H$ (that is, the restriction of f) and the canonical map $\pi_{\alpha'} : B^H \to S(\alpha')$. Clearly $\pi_{\alpha'} f^H$ induces an injective homomorphism of $\overline{N}$-algebras

$$\overline{f} : A^H / \mathrm{Ker}(\pi_{\alpha'} f^H) \longrightarrow S(\alpha') .$$

Since $\mathcal{F}$ is an embedding, the image of f^H is equal to $iB^H i$ where $i = f(1_A)$, and since $\pi_{\alpha'}$ is surjective, the image of $\overline{f}$ is equal to $\overline{i} S(\alpha') \overline{i}$ where $\overline{i} = \pi_{\alpha'}(i)$. But $\overline{i} S(\alpha') \overline{i}$ is a simple k-algebra because if we set as usual $S(\alpha) \cong \mathrm{End}_k(V(\alpha))$, then we have $\overline{i} S(\alpha') \overline{i} \cong \mathrm{End}_k(\overline{i} V(\alpha))$ (see Lemma 12.4). Therefore $A^H / \mathrm{Ker}(\pi_{\alpha'} f^H)$ is simple (since $\overline{f}$ is injective) and so $\mathrm{Ker}(\pi_{\alpha'} f^H)$ is a maximal ideal of A^H . But since $f^H(\alpha) \subseteq \alpha'$, we have $\alpha \not\subseteq \mathrm{Ker}(\pi_{\alpha'} f^H)$, hence $\mathrm{Ker}(\pi_{\alpha'} f^H) \subseteq \mathfrak{m}_\alpha$ by Corollary 4.10. It follows that $\mathrm{Ker}(\pi_{\alpha'} f^H) = \mathfrak{m}_\alpha$ and therefore

$$A^H / \mathrm{Ker}(\pi_{\alpha'} f^H) = S(\alpha) .$$

Thus $\overline{f}$ is an injective homomorphism of $\overline{N}$-algebras $\overline{f} : S(\alpha) \to S(\alpha')$ whose image is the whole of $\overline{i} S(\alpha') \overline{i}$, and so $\overline{f}$ belongs to an exomorphism $\overline{\mathcal{F}}(\alpha)$ of $\overline{N}$-algebras which is an embedding. If one changes the choice of $f \in \mathcal{F}$, one has to modify f by $\mathrm{Inn}(b)$ where $b \in B^G$. Then $b = r_H^G(b) \in B^H$ is fixed under $\overline{N}$ and its image $\bar{b} = \pi_{\alpha'}(b)$ belongs to $S(\alpha')^{\overline{N}}$. In the construction above, we see that $\overline{f}$ is modified by $\mathrm{Inn}(\bar{b})$, so that we end up with a homomorphism belonging to the same exomorphism $\overline{\mathcal{F}}(\alpha)$. Therefore we have proved the following result.

(15.3) PROPOSITION. *Let $\mathcal{F} : A \to B$ be an embedding of G-algebras, let H_α be a pointed group on A, let $H_{\alpha'}$ be its image in B, and let $\overline{N} = \overline{N}_G(H_\alpha) = \overline{N}_G(H_{\alpha'})$. Then $\mathcal{F}$ induces an embedding of $\overline{N}$-algebras $\overline{\mathcal{F}}(\alpha) : S(\alpha) \to S(\alpha')$ such that the following diagram commutes*

$$\begin{array}{ccc} A^H & \xrightarrow{\mathcal{F}^H} & B^H \\ {\scriptstyle \pi_\alpha}\big\downarrow & & \big\downarrow{\scriptstyle \pi_{\alpha'}} \\ S(\alpha) & \xrightarrow{\overline{\mathcal{F}}(\alpha)} & S(\alpha') \end{array}$$

where $\mathcal{F}^H : A^H \to B^H$ is the embedding of $\overline{N}$-algebras induced by $\mathcal{F}$.

We now consider the behaviour of multiplicity modules with respect to the above embedding $\overline{\mathcal{F}}(\alpha)$. Changing notation for simplicity, and generalizing to $\mathcal{O}$-simple algebras for later use, we let $\mathcal{H} : S \to S'$ be an embedding of $\mathcal{O}$-simple G-algebras. By Example 10.8, we have $S \cong \mathrm{End}_\mathcal{O}(V)$ and V is endowed with an $\mathcal{O}_\sharp\widehat{G}$-module structure. Similarly we have $S' \cong \mathrm{End}_\mathcal{O}(V')$ and V' is endowed with an $\mathcal{O}_\sharp\widehat{G}'$-module structure. We use the following explicit description of $\widehat{G}$ and $\widehat{G}'$ (see Example 10.8):

$$\widehat{G} = \{\, (a,g) \in S^* \times G \mid \mathrm{Inn}(a)(s) = {}^g s \ \text{ for all } s \in S \,\},$$
$$\widehat{G}' = \{\, (a',g) \in (S')^* \times G \mid \mathrm{Inn}(a')(s') = {}^g s' \ \text{ for all } s' \in S' \,\}.$$

Now we prove that the embedding $\mathcal{H} : S \to S'$ induces an isomorphism of central extensions $\mathcal{H}^* : \widehat{G}' \to \widehat{G}$ (which is naturally defined in the reverse direction).

(15.4) PROPOSITION. *Let $S \cong \mathrm{End}_\mathcal{O}(V)$ and $S' \cong \mathrm{End}_\mathcal{O}(V')$ be two $\mathcal{O}$-simple G-algebras and let $\mathcal{H} : S \to S'$ be an embedding of G-algebras.*

(a) Let $h \in \mathcal{H}$ and $i = h(1_S)$. If $(a',g) \in \widehat{G}'$, then $ia' = a'i = ia'i$ and the unique element $a \in S$ such that $h(a) = ia'$ is independent of the choice of $h \in \mathcal{H}$.

(b) There is an isomorphism of central extensions

$$\mathcal{H}^* : \widehat{G}' \longrightarrow \widehat{G}, \quad (a',g) \mapsto (a,g),$$

where a is defined by $h(a) = ia'$ for $h \in \mathcal{H}$. Moreover $\mathcal{H}^*$ induces the identity on both the quotient G and the central subgroup $\mathcal{O}^*$.

(c) *Using the isomorphism $\mathcal{H}^* : \widehat{G}' \to \widehat{G}$ of part (b), the $\mathcal{O}_\sharp\widehat{G}$-module V has an $\mathcal{O}_\sharp\widehat{G}'$-module structure. Endowed with this structure, V is isomorphic (via $\mathcal{H}$) to a direct summand of V'.*

Proof. (a) We first note that if $(a', g) \in \widehat{G}'$, then a' commutes with $(S')^G$. Indeed $\mathrm{Inn}(a')$ is equal to the action of g, which is the identity on $(S')^G$. In particular a' commutes with $i = h(1_S)$, proving the first assertion. Let $\mathrm{Inn}(b)h$ be another representative of $\mathcal{H}$, where $b \in (S')^G$, and let $j = \mathrm{Inn}(b)h(1_S) = \mathrm{Inn}(b)(i)$. If $a \in S$ is the unique element such that $h(a) = ia'$, then $\mathrm{Inn}(b)h(a) = \mathrm{Inn}(b)(i)\,\mathrm{Inn}(b)(a') = ja'$, because a' commutes with b by the remark above. This shows that a is independent of the choice of h.

(b) To show that $(a, g) \in \widehat{G}$, we must prove that a is invertible and that $\mathrm{Inn}(a)$ is the action of g on S. Since h defines an isomorphism $S \xrightarrow{\sim} iS'i$, it suffices to show that $h(a)$ is invertible in $iS'i$ and that $\mathrm{Inn}(h(a))$ is the action of g on $iS'i$. First note that $i(a')^{-1}$ is the inverse of $h(a) = ia'$ in $iS'i$ because a' commutes with i. Now for $c \in iS'i$, we have

$$\mathrm{Inn}(h(a))(c) = ia'ci(a')^{-1} = a'ici(a')^{-1} = \mathrm{Inn}(a')(ici) = \mathrm{Inn}(a')(c) = {}^g c\,,$$

using the fact that $c = ici$. This completes the proof that $(a, g) \in \widehat{G}$, so that $\mathcal{H}^*$ is well-defined.

Let $(a_1', g_1), (a_2', g_2) \in \widehat{G}'$ and let $a_1, a_2 \in S$ be such that $h(a_1) = ia_1'$ and $h(a_2) = ia_2'$. Then the image of the product $(a_1'a_2', g_1g_2)$ is equal to the product (a_1a_2, g_1g_2) of the images, because

$$h(a_1a_2) = h(a_1)h(a_2) = ia_1'ia_2' = i^2a_1'a_2' = ia_1'a_2'\,.$$

Thus $\mathcal{H}^*$ is a group homomorphism, which by construction induces the identity on the quotient G. Finally $\mathcal{H}^*$ is also the identity on $\mathcal{O}^*$, because $\mathcal{O}^*$ is identified with the central subgroups $\mathcal{O}^*{\cdot}1_S \times \{1\} \subset \widehat{G}$ and $\mathcal{O}^*{\cdot}1_{S'} \times \{1\} \subset \widehat{G}'$ respectively, and clearly $h(\lambda{\cdot}1_S) = i\lambda{\cdot}1_{S'}$ for $\lambda \in \mathcal{O}^*$.

(c) The $\mathcal{O}_\sharp\widehat{G}$-module structure of V is provided by the first projection $\rho : \widehat{G} \to S^* \cong GL(V)$. Similarly the $\mathcal{O}_\sharp\widehat{G}'$-module structure of V' is given by the map $\rho' : \widehat{G}' \to (S')^* \cong GL(V')$. Choose $h \in \mathcal{H}$ and let $i = h(1_S)$. Let $(a', g) \in \widehat{G}'$ and $(a, g) = \mathcal{H}^*(a', g)$ (so that $h(a) = ia'$). Using the isomorphism $\mathcal{H}^*$, the action of (a', g) on V is the endomorphism a of V. Via the embedding $\mathcal{H}$, this corresponds to the action of the element $h(a) = ia'$ of $iS'i \cong \mathrm{End}_{\mathcal{O}}(iV')$, which is precisely the action of (a', g) restricted to the direct summand iV' (because a' and $ia' = a'i$ coincide on this summand). Another choice of h yields another isomorphic direct summand of V'. $\square$

Note that the isomorphism $\mathcal{H}^* : \widehat{G}' \to \widehat{G}$ depends on the embedding $\mathcal{H} : S \to S'$. Thus a different embedding yields a different isomorphism, hence a different $\mathcal{O}_\sharp\widehat{G}'$-module structure on V, which may correspond to another isomorphism class of direct summands of V' (Exercise 15.3).

By Proposition 15.3, an embedding of G-algebras $\mathcal{F} : A \to B$ induces an embedding of $\overline{N}$-algebras $\overline{\mathcal{F}}(\alpha) : S(\alpha) \to S(\alpha')$. Applying Proposition 15.4, we obtain in particular the following statement about multiplicity modules.

(15.5) COROLLARY. *Let $\mathcal{F} : A \to B$ be an embedding of G-algebras, let H_α be a pointed group on A, and let $H_{\alpha'}$ be its image in B. Let $\overline{N} = \overline{N}_G(H_\alpha) = \overline{N}_G(H_{\alpha'})$, and let $\overline{\mathcal{F}}(\alpha) : S(\alpha) \to S(\alpha')$ be the embedding of $\overline{N}$-algebras induced by $\mathcal{F}$ (Proposition 15.3). Then $\overline{\mathcal{F}}(\alpha)$ induces an isomorphism of central extensions $\overline{\mathcal{F}}(\alpha)^* : \widehat{\overline{N}}' \to \widehat{\overline{N}}$, inducing the identity on both k^* and $\overline{N}$. Using the isomorphism $\overline{\mathcal{F}}(\alpha)^*$, the multiplicity module $V(\alpha)$ has a $k_\sharp\widehat{\overline{N}}'$-module structure; endowed with this structure, $V(\alpha)$ is isomorphic (via $\overline{\mathcal{F}}(\alpha)$) to a direct summand of $V(\alpha')$.*

We end this section with the observation that embeddings also induce embeddings between Brauer quotients.

(15.6) PROPOSITION. *Let $\mathcal{F} : A \to B$ be an embedding of G-algebras, let P be a p-subgroup of G, and let $\overline{N} = N_G(P)/P$. Then $\mathcal{F}$ induces an embedding of $\overline{N}$-algebras $\overline{\mathcal{F}}(P) : \overline{A}(P) \to \overline{B}(P)$ such that the following diagram commutes*

$$\begin{array}{ccc} A^P & \xrightarrow{\mathcal{F}^P} & B^P \\ {\scriptstyle br_P^A}\downarrow & & \downarrow{\scriptstyle br_P^B} \\ \overline{A}(P) & \xrightarrow{\overline{\mathcal{F}}(P)} & \overline{B}(P) \end{array}$$

where $\mathcal{F}^P : A^P \to B^P$ is the embedding of $\overline{N}$-algebras induced by $\mathcal{F}$.

Proof. We only sketch the proof, leaving the details as an exercise for the reader. Choose $f \in \mathcal{F}$ and let $i = f(1_A)$. Since i is fixed under any subgroup of G, the Brauer homomorphism $br_P^B : B^P \to \overline{B}(P)$ restricts to a surjective homomorphism $iB^Pi \to br_P^B(i)\overline{B}(P)br_P^B(i)$ which can only be the Brauer homomorphism of iBi. Indeed the ideal appearing in the definition of the kernel of the Brauer homomorphism is

$$\sum_{Q<P} t_Q^P((iBi)^Q) = \sum_{Q<P} t_Q^P(iB^Qi) = \sum_{Q<P} i\,t_Q^P(B^Q)i = \big(\sum_{Q<P} t_Q^P(B^Q)\big) \cap iB^Pi\,.$$

Therefore $\overline{(iBi)}(P) \cong br_P^B(i)\overline{B}(P)br_P^B(i)$. Since f induces a G-algebra isomorphism $A \xrightarrow{\sim} iBi$, we obtain an isomorphism

$$\overline{A}(P) \xrightarrow{\sim} br_P^B(i)\overline{B}(P)br_P^B(i) ,$$

hence an embedding $\overline{A}(P) \to \overline{B}(P)$, as required. □

We know from Proposition 15.1 that $\mathcal{F}$ induces an injective map $\mathcal{LP}(A^P) \to \mathcal{LP}(B^P)$. This can also be deduced from the above proposition since $\mathcal{LP}(A^P) \cong \mathcal{P}(\overline{A}(P))$ (Lemma 14.5).

Exercises

(15.1) Complete the details of the proof of part (d) in Proposition 15.1.

(15.2) Let A be a G-algebra. Define a natural G-algebra structure on the matrix algebra $M_n(A)$ and a canonical embedding $\mathcal{F} : A \to M_n(A)$. Show that the induced map $\mathcal{F}_* : \mathcal{PG}(A) \to \mathcal{PG}(M_n(A))$ is a bijection and that the multiplicities of points are multiplied by n .

(15.3) Let G be a cyclic group of order 2 generated by g and suppose that the characteristic p is not equal to 2. Let $S = M_2(k) = \mathrm{End}_k(V)$, endowed with the action of g defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & -b \\ -c & d \end{pmatrix} .$$

Prove that the corresponding twisted group algebra $k_\sharp\widehat{G}$ is isomorphic to the ordinary group algebra kG , but not canonically (there are two such isomorphisms). Prove that there are two distinct embeddings of G-algebras $k \to S$ (where k is the trivial G-algebra). In each case describe in detail the corresponding isomorphism of central extensions and the identification of the one dimensional module for k with a direct summand of V (Proposition 15.4). Show that this procedure for the two embeddings yields two non-isomorphic direct summands of V (corresponding, under some non-canonical isomorphism $k_\sharp\widehat{G} \cong kG$, to the trivial and the sign representations of G respectively).

(15.4) Provide the details of the proof of Proposition 15.6.

Notes on Section 15

For the results of this section, we have followed Puig [1981, 1984, 1988a].

CHAPTER 3

Induction and defect theory

The main purpose of this chapter is the defect theory of pointed groups which is a reduction to the case of p-groups and projective modules. In the case of interior G-algebras, it is closely related to an induction procedure, which is only defined for interior structures. One of the most important tool is the Puig correspondence, which implies the Green correspondence. We continue with our assumption that G is a finite group and that $\mathcal{O}$ is a commutative complete local noetherian ring with an algebraically closed residue field k of characteristic p.

§ 16 INDUCTION OF INTERIOR G-ALGEBRAS

In this section we introduce an induction procedure for interior G-algebras which has no analogue for arbitrary G-algebras. The construction is a generalization of the concept of induction of modules.

Let H be a subgroup of G and let B be an interior H-algebra. We define $\mathrm{Ind}_H^G(B)$ to be the $\mathcal{O}$-module $\mathcal{O}G \otimes_{\mathcal{O}H} B \otimes_{\mathcal{O}H} \mathcal{O}G$ and we wish to put an interior G-algebra structure on $\mathrm{Ind}_H^G(B)$. First note that $\mathcal{O}G$ is a free right $\mathcal{O}H$-module with basis $[G/H]$, and also a free left $\mathcal{O}H$-module with basis $[H\backslash G]$. Choosing $[H\backslash G]$ as the set of inverse elements of the elements of $[G/H]$, it follows that

$$\mathrm{Ind}_H^G(B) = \bigoplus_{f,g\in[G/H]} f\mathcal{O}H \otimes_{\mathcal{O}H} B \otimes_{\mathcal{O}H} \mathcal{O}Hg^{-1} = \bigoplus_{f,g\in[G/H]} f \otimes B \otimes g^{-1} .$$

In particular if B is $\mathcal{O}$-free (with some basis $(b_i)_{i\in I}$), then $\mathrm{Ind}_H^G(B)$ is $\mathcal{O}$-free (with basis (fb_ig^{-1}) where $i \in I$ and $f, g \in [G/H]$). Thus $\dim_{\mathcal{O}}(\mathrm{Ind}_H^G(B)) = |G : H|^2 \dim_{\mathcal{O}}(B)$.

The multiplication of elements of $\mathrm{Ind}_H^G(B)$ is defined as follows. If $x, x', y, y' \in G$ and $b, b' \in B$, then

$$(x \otimes b \otimes y)(x' \otimes b' \otimes y') = \begin{cases} x \otimes b \cdot yx' \cdot b' \otimes y' & \text{if } yx' \in H, \\ 0 & \text{if } yx' \notin H. \end{cases}$$

The multiplication of arbitrary elements of $\mathrm{Ind}_H^G(B)$ is defined by extending this product $\mathcal{O}$-linearly. It is immediate from the definition that for $h_1, h_2, h_3, h_4 \in H$, we have

$$(xh_1 \otimes b \otimes h_2y)(x'h_3 \otimes b' \otimes h_4y') = (x \otimes h_1bh_2 \otimes y)(x' \otimes h_3b'h_4 \otimes y') ,$$

and therefore the multiplication is well-defined and is $\mathcal{O}$-bilinear. It is also clear that this product is associative and has a unity element equal to

$$1_{\mathrm{Ind}_H^G(B)} = \sum_{g\in[G/H]} g \otimes 1_B \otimes g^{-1} .$$

Thus $\mathrm{Ind}_H^G(B)$ is endowed with an $\mathcal{O}$-algebra structure.

(16.1) LEMMA. *Let H be a subgroup of G of index n . Then we have $\mathrm{Ind}_H^G(B) \cong M_n(B)$ as $\mathcal{O}$-algebras.*

Proof. We choose a transversal $[G/H]$ and we index the entries of an $n \times n$-matrix by pairs in $[G/H]$. Then we define an $\mathcal{O}$-linear isomorphism $\theta : \mathrm{Ind}_H^G(B) \to M_n(B)$ by extending $\mathcal{O}$-linearly the map sending $f \otimes b \otimes g^{-1}$ (where $f, g \in [G/H]$ and $b \in B$) to the matrix whose (f, g)-entry is equal to b and whose other entries are all zero. Since elementary matrices of this kind multiply in the same way as the corresponding elements of $\mathrm{Ind}_H^G(B)$, the map θ is an isomorphism of $\mathcal{O}$-algebras. □

We now put an interior G-algebra structure on $\mathrm{Ind}_H^G(B)$. It is defined by the map

$$\phi : G \longrightarrow \mathrm{Ind}_H^G(B)\,, \qquad g \mapsto \sum_{f\in[G/H]} gf\otimes 1_B\otimes f^{-1}\,.$$

To check that ϕ is a group homomorphism from G to $\mathrm{Ind}_H^G(B)^*$, let $g,g'\in G$. We first note that for each $f\in[G/H]$, there is a unique $f'\in[G/H]$ such that $f^{-1}g'f'\in H$ (and $f\mapsto f'$ defines a permutation of $[G/H]$, induced by left multiplication by $(g')^{-1}$). Therefore we obtain

$$\begin{aligned}\phi(g)\phi(g') &= \sum_{f\in[G/H]} gf\otimes f^{-1}g'f'\cdot 1_B\otimes (f')^{-1}\\ &= \sum_{f\in[G/H]} gff^{-1}g'f'\otimes 1_B\otimes (f')^{-1}\\ &= \sum_{f'\in[G/H]} gg'f'\otimes 1_B\otimes (f')^{-1}\\ &= \phi(gg')\,.\end{aligned}$$

Thus $\mathrm{Ind}_H^G(B)$ is an interior G-algebra. Notice that the expression of the unity element can be rewritten as $1_{\mathrm{Ind}_H^G(B)} = t_H^G(1\otimes 1_B\otimes 1)$. In particular $\mathrm{Ind}_H^G(B)$ is projective relative to H.

The interior G-algebra structure induces an $(\mathcal{O}G,\mathcal{O}G)$-bimodule structure by left and right multiplication by elements $\phi(g)$ for $g\in G$. But on the other hand $\mathrm{Ind}_H^G(B) = \mathcal{O}G\otimes_{\mathcal{O}H} B\otimes_{\mathcal{O}H}\mathcal{O}G$ has in a natural way an $(\mathcal{O}G,\mathcal{O}G)$-bimodule structure.

(16.2) LEMMA. *The two $(\mathcal{O}G,\mathcal{O}G)$-bimodule structures on $\mathrm{Ind}_H^G(B)$ coincide. Explicitly*

$$\phi(g)\cdot(f\otimes b\otimes f') = gf\otimes b\otimes f' \quad \text{and} \quad (f\otimes b\otimes f')\cdot\phi(g) = f\otimes b\otimes f'g$$

for $g,f,f'\in G$ and $b\in B$.

Proof. We only check the left $\mathcal{O}G$-module structure. We can choose a transversal $[G/H]$ containing f. Then

$$\begin{aligned}\phi(g)\cdot(f\otimes b\otimes f') &= \sum_{x\in[G/H]} (gx\otimes 1_B\otimes x^{-1})\cdot(f\otimes b\otimes f')\\ &= gf\otimes f^{-1}fb\otimes f' = gf\otimes b\otimes f'\,,\end{aligned}$$

as required. □

Alternatively, the interior G-algebra structure on $\mathrm{Ind}_H^G(B)$ could be defined by using Exercise 10.2: the natural $(\mathcal{O}G, \mathcal{O}G)$-bimodule structure satisfies the conditions of this exercise, hence induces an interior G-algebra structure.

Now we prove that induction is transitive.

(16.3) PROPOSITION. *Let $K \leq H \leq G$ and let A be an interior K-algebra. Then there is an isomorphism of interior G-algebras*

$$\phi : \mathrm{Ind}_H^G(\mathrm{Ind}_K^H(A)) \xrightarrow{\sim} \mathrm{Ind}_K^G(A)\,, \quad g \otimes (h \otimes a \otimes h') \otimes g' \mapsto gh \otimes a \otimes h'g'\,.$$

Proof. We choose transversals $[G/H]$ and $[H/K]$. Then the set $\{gh \mid g \in [G/H], h \in [H/K]\}$ is a transversal of K in G. It is now staightforward to check that ϕ is well-defined and is an $\mathcal{O}$-linear isomorphism. The proof that ϕ is a homomorphism of interior G-algebras is an easy exercise which is left to the reader. □

(16.4) EXAMPLE. Let $H \leq G$ and let M be an $\mathcal{O}H$-module. The *induced module* $\mathrm{Ind}_H^G(M)$ is by definition the $\mathcal{O}G$-module $\mathcal{O}G \otimes_{\mathcal{O}H} M$. We know from Example 10.6 that $\mathrm{End}_{\mathcal{O}}(M)$ is an interior H-algebra, and similarly $\mathrm{End}_{\mathcal{O}}(\mathrm{Ind}_H^G(M))$ is an interior G-algebra. The relationship between the two induction procedures is that there is an isomorphism of interior G-algebras

$$\mathrm{Ind}_H^G(\mathrm{End}_{\mathcal{O}}(M)) \cong \mathrm{End}_{\mathcal{O}}(\mathrm{Ind}_H^G(M))\,.$$

In order to prove this, we first note that, since $\mathcal{O}G$ is a free right $\mathcal{O}H$-module with basis $[G/H]$, there is an $\mathcal{O}$-module decomposition

$$\mathrm{Ind}_H^G(M) = \bigoplus_{z \in [G/H]} z \otimes M\,.$$

Thus $\mathrm{End}_{\mathcal{O}}(\mathrm{Ind}_H^G(M))$ is isomorphic to a matrix algebra of size $|G:H|$ over $\mathrm{End}_{\mathcal{O}}(M)$. By Lemma 16.1, $\mathrm{Ind}_H^G(\mathrm{End}_{\mathcal{O}}(M))$ is also isomorphic to a matrix algebra of size $|G:H|$ over $\mathrm{End}_{\mathcal{O}}(M)$. For the identification of those two algebras, we define an $\mathcal{O}$-linear action of $\mathrm{Ind}_H^G(\mathrm{End}_{\mathcal{O}}(M))$ on $\mathrm{Ind}_H^G(M)$ in the following way. If $f \in \mathrm{End}_{\mathcal{O}}(M)$, $x, y, z \in [G/H]$, and $v \in M$, then

$$(x \otimes f \otimes y^{-1}) \cdot (z \otimes v) = \begin{cases} x \otimes f(y^{-1}z \cdot v) & \text{if } y^{-1}z \in H, \\ 0 & \text{otherwise.} \end{cases}$$

This action induces a homomorphism of $\mathcal{O}$-algebras

$$\phi : \mathrm{Ind}_H^G(\mathrm{End}_{\mathcal{O}}(M)) \longrightarrow \mathrm{End}_{\mathcal{O}}(\mathrm{Ind}_H^G(M))$$

mapping $x\otimes f\otimes y^{-1}$ to the endomorphism of $\mathrm{Ind}_H^G(M)$ which sends $y\otimes M$ to $x\otimes M$ via f and is zero on the other summands of $\mathrm{Ind}_H^G(M)$ (that is, an elementary matrix with a single non-zero entry equal to f). It follows from this and Lemma 16.1 that ϕ is an isomorphism of $\mathcal{O}$-algebras.

Since $\left(\sum_{x\in[G/H]} gx\otimes id_M\otimes x^{-1}\right)\cdot(z\otimes v) = gz\otimes v$ for $g\in G$, we have

$$\phi(g\cdot 1) = \phi\Big(\sum_{x\in[G/H]} gx\otimes id_M\otimes x^{-1}\Big) = g\cdot id_{\mathrm{Ind}_H^G(M)}\,,$$

that is, the action of g on $\mathrm{Ind}_H^G(M)$. It follows that ϕ is a homomorphism of interior G-algebras.

This example suggests a generalization of known results on induction of modules to the case of interior algebras. Indeed this will be one of our leading themes, but the reader need not be acquainted with those results on modules. Here is a first instance.

(16.5) PROPOSITION. *Let H be a subgroup of G, let A be an interior G-algebra, and let B be an interior H-algebra. Then there is an isomorphism of interior G-algebras*

$$\begin{aligned}\phi : \mathrm{Ind}_H^G(\mathrm{Res}_H^G(A)\otimes_{\mathcal{O}} B) &\xrightarrow{\sim} A\otimes_{\mathcal{O}}\mathrm{Ind}_H^G(B)\\ x\otimes(a\otimes b)\otimes y &\mapsto (x\cdot a\cdot y)\otimes(x\otimes b\otimes y)\,.\end{aligned}$$

Proof. It is staightforward to check that ϕ is well-defined and is an $\mathcal{O}$-linear homomorphism. It is an isomorphism because it has the following inverse:

$$\begin{aligned}A\otimes_{\mathcal{O}}\mathrm{Ind}_H^G(B) &\longrightarrow \mathrm{Ind}_H^G(\mathrm{Res}_H^G(A)\otimes_{\mathcal{O}} B)\\ a\otimes(x\otimes b\otimes y) &\mapsto x\otimes(x^{-1}\cdot a\cdot y^{-1}\otimes b)\otimes y\,.\end{aligned}$$

The proof that ϕ is a homomorphism of interior G-algebras is an easy exercise which is left to the reader. □

It is well-known (and easy to check) that if an $\mathcal{O}G$-module M is a direct sum of $\mathcal{O}$-submodules $M = L_1\oplus\ldots\oplus L_n$ and if G permutes transitively the submodules L_i, then $M\cong\mathrm{Ind}_H^G(L_1)$ where H is the stabilizer of L_1. The analogous property for interior algebras is the following.

(16.6) PROPOSITION. *Let A be an interior G-algebra and let H be a subgroup of G. Assume that there exists an idempotent $i \in A^H$ such that $1_A = t_H^G(i)$ and $i\,{}^g i = 0$ for all $g \in G - H$. Then there is an isomorphism of interior G-algebras*

$$f : \mathrm{Ind}_H^G(iAi) \xrightarrow{\sim} A\,, \qquad x \otimes b \otimes y \mapsto x{\cdot}b{\cdot}y \qquad (x, y \in G\,,\ b \in iAi)\,.$$

Proof. It is clear that f is an $\mathcal{O}$-linear map which is well-defined. The assumptions imply that f is a homomorphism of interior G-algebras. Indeed let $a = x \otimes b \otimes y$ and $a' = x' \otimes b' \otimes y'$ belong to $\mathrm{Ind}_H^G(iAi)$. By definition of the product in $\mathrm{Ind}_H^G(iAi)$, we have

$$f(aa') = \begin{cases} x \cdot b \cdot yx' \cdot b' \cdot y' & \text{if } yx' \in H, \\ 0 & \text{if } yx' \notin H. \end{cases}$$

On the other hand $f(a)f(a') = x \cdot b \cdot yx' \cdot b' \cdot y'$, so we have to show that this is zero if $yx' \notin H$. But since $i\,{}^{yx'}i = 0$ by assumption, we have

$$b \cdot yx' \cdot b' = bi \cdot yx' \cdot ib' = bi\,{}^{yx'}i \cdot yx' \cdot b' = 0$$

as required. This proves that f is a homomorphism of $\mathcal{O}$-algebras. Moreover it is clear that f is a homomorphism of interior G-algebras.

The following argument for $a \in A$ shows the surjectivity of f:

$$\begin{aligned} a = 1 \cdot a \cdot 1 = t_H^G(i) a\, t_H^G(i) &= \sum_{x,y \in [G/H]} x \cdot i \cdot x^{-1} \cdot a \cdot y \cdot i \cdot y^{-1} \\ &= f\Big(\sum_{x,y \in [G/H]} x \otimes i \cdot x^{-1} \cdot a \cdot y \cdot i \otimes y^{-1} \Big)\,. \end{aligned}$$

To prove the injectivity of f, let $\sum_{x,y \in [G/H]} x \otimes b_{x,y} \otimes y^{-1} \in \mathrm{Ker}(f)$, where $b_{x,y} \in iAi$. Multiply the image of this element by $i \cdot z^{-1}$ on the left and $t \cdot i$ on the right, where $z, t \in [G/H]$. By the argument already used above, we have $i \cdot z^{-1}x \cdot i = 0$ and $i \cdot y^{-1}t \cdot i = 0$ unless $z^{-1}x \in H$ and $y^{-1}t \in H$, that is, $z = x$ and $t = y$. Thus we obtain

$$0 = \sum_{x,y \in [G/H]} i \cdot z^{-1}x \cdot ib_{x,y}i \cdot y^{-1}t \cdot i = i^2 b_{z,t}\, i^2 = b_{z,t}\,.$$

This shows the injectivity of f and completes the proof. □

We now consider homomorphisms and exomorphisms. If $f : A \to B$ is a homomorphism of interior H-algebras, it is easy to check that the $\mathcal{O}$-linear map

$$\mathrm{Ind}_H^G(f) : \mathrm{Ind}_H^G(A) \longrightarrow \mathrm{Ind}_H^G(B), \qquad x \otimes a \otimes y \mapsto x \otimes f(a) \otimes y$$

is well-defined and is a homomorphism of interior G-algebras. If f and f' belong to the same exomorphism of interior H-algebras $\mathcal{F} : A \to B$, then there exists $b \in (B^H)^*$ such that $f'(a) = bf(a)b^{-1}$ for all $a \in A$. Let $c = \sum_{x\in[G/H]} x \otimes b \otimes x^{-1} \in \mathrm{Ind}_H^G(B)$, which is clearly invertible (with inverse $c^{-1} = \sum_{x\in[G/H]} x \otimes b^{-1} \otimes x^{-1}$). We have

$$\begin{aligned}\mathrm{Ind}_H^G(f')(x \otimes a \otimes y) &= x \otimes bf(a)b^{-1} \otimes y = c(x \otimes f(a) \otimes y)c^{-1} \\ &= c\big(\mathrm{Ind}_H^G(f)(x \otimes a \otimes y)\big)c^{-1}\end{aligned}$$

by an easy computation. Then either by using Proposition 12.1 (applied to the restriction to the trivial subgroup) or by showing directly that c is G-invariant (which is elementary), one deduces that $\mathrm{Ind}_H^G(f)$ and $\mathrm{Ind}_H^G(f')$ belong to the same exomorphism of interior G-algebras. This induced exomorphism will be written $\mathrm{Ind}_H^G(\mathcal{F})$.

Consider now the homomorphism of interior H-algebras

$$d_H^G : B \longrightarrow \mathrm{Res}_H^G \mathrm{Ind}_H^G(B), \qquad b \mapsto 1 \otimes b \otimes 1.$$

Restricted to the trivial subgroup (that is, viewed as a homomorphism of $\mathcal{O}$-algebras), d_H^G maps B onto the top left corner of the matrix algebra $\mathrm{Res}_1^G \mathrm{Ind}_H^G(B) \cong M_{|G:H|}(B)$ (see Lemma 16.1). Thus d_H^G is injective and its image is $i\,\mathrm{Ind}_H^G(B)\,i$ where $i = 1 \otimes 1_B \otimes 1$. It follows that the exomorphism $\mathcal{D}_H^G$ containing d_H^G is an embedding of interior H-algebras. It is called the *canonical embedding* of B into its induced algebra. When we need to emphasize the dependence on B, we write $\mathcal{D}_H^G(B) = \mathcal{D}_H^G$ and $d_H^G(B) = d_H^G$.

As local pointed groups play a crucial role in the whole theory (in particular in the defect theory), it is important to know what they are on an induced algebra $\mathrm{Ind}_H^G(B)$. The following result answers this question and shows that the local pointed groups on $\mathrm{Ind}_H^G(B)$ always come from B up to conjugation.

(16.7) PROPOSITION. *Let H be a subgroup of G, let B be an interior H-algebra, and let $\mathcal{D}_H^G : B \to \mathrm{Res}_H^G \mathrm{Ind}_H^G(B)$ be the canonical embedding. For every local pointed group P_γ on $\mathrm{Ind}_H^G(B)$, there exists $g \in G$ such that ${}^g(P_\gamma)$ is in the image of $\mathcal{D}_H^G$. In particular ${}^gP \leq H$.*

Proof. Let $\pi_\gamma : \mathrm{Ind}_H^G(B)^P \to S(\gamma)$ be the canonical surjection onto the multiplicity algebra of γ. Since $t_H^G(1 \otimes 1_B \otimes 1)$ is the unity element of $\mathrm{Ind}_H^G(B)$, we have

$$1_{S(\gamma)} = \pi_\gamma\, r_P^G\, t_H^G(1 \otimes 1_B \otimes 1) = \sum_{g \in [P\backslash G/H]} \pi_\gamma\, t_{P \cap {}^gH}^P\, r_{P \cap {}^gH}^{{}^gH}(g \otimes 1_B \otimes g^{-1})$$

by the Mackey decomposition formula 11.3. Since γ is local, we have $\mathrm{Ker}(br_P) \subseteq \mathrm{Ker}(\pi_\gamma)$, and so $\pi_\gamma\, t_{P \cap {}^gH}^P = 0$ unless $P \leq {}^gH$. It follows that there exists $g \in G$ such that $P \leq {}^gH$ and $\pi_\gamma\, r_P^{{}^gH}(g \otimes 1_B \otimes g^{-1}) \neq 0$. Conjugating by $h = g^{-1}$, we get ${}^hP \leq H$ and $\pi_{({}^h\gamma)}\, r_{{}^hP}^H(1 \otimes 1_B \otimes 1) \neq 0$. This means that some idempotent $i \in {}^h\gamma$ appears in a primitive decomposition of $r_{{}^hP}^H(1 \otimes 1_B \otimes 1)$, or in other words

$$i = (1 \otimes 1_B \otimes 1)\, i\, (1 \otimes 1_B \otimes 1)\,.$$

Therefore i is in the image of the map d_H^G, so that ${}^h(P_\gamma)$ is in the image of $\mathcal{D}_H^G$. □

Exercises

(16.1) Complete the proof of Proposition 16.3.

(16.2) Complete the proof of Proposition 16.5.

(16.3) Prove the analogue of 16.5 and 16.6 for the restriction and induction of $\mathcal{O}G$-lattices and $\mathcal{O}H$-lattices (either directly or by deducing the result from 16.5 and 16.6, using Lemma 10.7).

(16.4) Let H be a subgroup of G and let M^* be the dual lattice of an $\mathcal{O}H$-lattice M. Prove that $\mathrm{Ind}_H^G(M^*) \cong \mathrm{Ind}_H^G(M)^*$.

(16.5) Let H be a subgroup of G, let M be an $\mathcal{O}G$-lattice, and let N be an $\mathcal{O}H$-lattice.

(a) Prove the Frobenius reciprocity isomorphisms:

$$\mathrm{Hom}_{\mathcal{O}G}(\mathrm{Ind}_H^G(N), M) \cong \mathrm{Hom}_{\mathcal{O}H}(N, \mathrm{Res}_H^G(M)),$$
$$\mathrm{Hom}_{\mathcal{O}G}(M, \mathrm{Ind}_H^G(N)) \cong \mathrm{Hom}_{\mathcal{O}H}(\mathrm{Res}_H^G(M), N).$$

[Hint: The first one follows from the definition of induction and the second one can be deduced from the first by duality, using the previous exercise.]

(b) Prove that the Frobenius reciprocity isomorphisms are natural (in the sense of category theory) with respect to $\mathcal{O}G$-linear maps $M \to M'$ as well as with respect to $\mathcal{O}H$-linear maps $N \to N'$.

Notes on Section 16

Induction of interior G-algebras has been introduced by Puig [1981]. We have also followed Puig [1984].

§ 17 INDUCTION AND RELATIVE PROJECTIVITY

We show in this section how, for interior G-algebras, relative projectivity can be expressed in terms of induced algebras. We prove one main theorem, working with an arbitrary idempotent j. The first application is of a global nature and follows by taking $j = 1_A$. It implies Higman's criterion for the relative projectivity of modules. The second application follows by taking for j a primitive idempotent and gives an interpretation of the relation *pr* between pointed groups in terms of induced algebras.

We first establish the following general result.

(17.1) THEOREM. *Let A be an interior G-algebra, let H be subgroup of G, and let j be an idempotent of A^H. Let $\mathcal{E} : jAj \to \mathrm{Res}^G_H(A)$ be the embedding containing the inclusion $e : jAj \to \mathrm{Res}^G_H(A)$ and let $\mathcal{D}^G_H : jAj \to \mathrm{Res}^G_H \mathrm{Ind}^G_H(jAj)$ be the canonical embedding associated with the interior H-algebra jAj. The following conditions are equivalent.*

(a) *There exist $a', a'' \in A^H$ such that $1_A = t^G_H(a'ja'')$.*

(b) *There exists an embedding $\mathcal{F} : A \to \mathrm{Ind}^G_H(jAj)$ such that the following diagram of exomorphisms commutes.*

$$\begin{array}{ccc} jAj & \xrightarrow{\mathcal{D}^G_H} & \mathrm{Res}^G_H \mathrm{Ind}^G_H(jAj) \\ \mathcal{E}\big\downarrow & \nearrow_{\mathrm{Res}^G_H(\mathcal{F})} & \\ \mathrm{Res}^G_H(A) & & \end{array}$$

If moreover these conditions are satisfied, then the embedding $\mathcal{F}$ is unique.

Proof. (b) $\Rightarrow$ (a). Let $f \in \mathcal{F}$. By the commutativity of the diagram in (b), $f(j)$ is conjugate to $1 \otimes j \otimes 1 = d^G_H(j)$ (here $d^G_H \in \mathcal{D}^G_H$ is the canonical homomorphism). Therefore there exists $c \in \mathrm{Ind}^G_H(jAj)^H$ such that $1 \otimes j \otimes 1 = cf(j)c^{-1}$. We have

$$1_{\mathrm{Ind}^G_H(jAj)} = \sum_{x \in [G/H]} x \otimes j \otimes x^{-1} = t^G_H(1 \otimes j \otimes 1) = t^G_H(cf(j)c^{-1}) .$$

Multiplying on both sides by $f(1_A)$ and using the fact that $f(1_A)$ is fixed under G, it follows that

$$f(1_A) = t^G_H\big(f(1_A)cf(j)c^{-1}f(1_A)\big) = t^G_H\big(f(1_A)cf(1_A)f(j)f(1_A)c^{-1}f(1_A)\big) .$$

Since $\mathcal{F}$ is an embedding, we can write $f(1_A)cf(1_A) = f(a')$ for a uniquely determined element $a' \in A^H$ and similarly $f(1_A)c^{-1}f(1_A) = f(a'')$ where $a'' \in A^H$. Thus we obtain

$$f(1_A) = t^G_H\big(f(a')f(j)f(a'')\big) = t^G_H(f(a'ja'')) = f(t^G_H(a'ja''))$$

and therefore $1_A = t_H^G(a'ja'')$, proving (a).

(a) $\Rightarrow$ (b). We have $1_A = t_H^G(a'ja'')$ by assumption and we define

$$f : A \longrightarrow \mathrm{Ind}_H^G(jAj)\,, \qquad f(a) = \sum_{x,y\in[G/H]} x \otimes ja''{\cdot}x^{-1}{\cdot}a{\cdot}y{\cdot}a'j \otimes y^{-1}\,.$$

It is clear that f is $\mathcal{O}$-linear. If $a, b \in A$, we write

$$f(b) = \sum_{z,t\in[G/H]} z \otimes ja''{\cdot}z^{-1}{\cdot}b{\cdot}t{\cdot}a'j \otimes t^{-1}$$

and we have

$$\begin{aligned} f(a)f(b) &= \sum_{x,t\in[G/H]} x \otimes ja''{\cdot}x^{-1}{\cdot}a\,\Big(\sum_{y\in[G/H]} y{\cdot}a'ja''{\cdot}y^{-1}\Big)\,b{\cdot}t{\cdot}a'j \otimes t^{-1} \\ &= f(ab) \end{aligned}$$

since the inner sum is equal to $t_H^G(a'ja'') = 1_A$. If now $g \in G$, then for each $x \in [G/H]$, write $g^{-1}x = x'h_x$ for some $x' \in [G/H]$ and $h_x \in H$ (so that $x \mapsto x'$ is a permutation of $[G/H]$). For $a \in A$, we obtain

$$\begin{aligned} f(g{\cdot}a) &= \sum_{x,y\in[G/H]} x \otimes ja''{\cdot}x^{-1}g{\cdot}a{\cdot}y{\cdot}a'j \otimes y^{-1} \\ &= \sum_{x,y\in[G/H]} g(g^{-1}x) \otimes ja''{\cdot}(g^{-1}x)^{-1}{\cdot}a{\cdot}y{\cdot}a'j \otimes y^{-1} \\ &= \sum_{x,y\in[G/H]} gx'h_x \otimes ja''{\cdot}h_x^{-1}(x')^{-1}{\cdot}a{\cdot}y{\cdot}a'j \otimes y^{-1} \\ &= \sum_{x',y\in[G/H]} gx' \otimes ja''{\cdot}(x')^{-1}{\cdot}a{\cdot}y{\cdot}a'j \otimes y^{-1} \\ &= g{\cdot}f(a) \end{aligned}$$

because $ja''{\cdot}h_x^{-1} = h_x^{-1}{\cdot}ja''$ (since $ja'' \in A^H$) and then h_x^{-1} cancels with h_x. This completes the proof that f is a homomorphism of interior G-algebras. We define $\mathcal{F}$ to be the exomorphism containing f.

We now show the commutativity of the diagram in the statement. Recall that $e : jAj \to \mathrm{Res}_H^G(A)$ denotes the inclusion. Writing for simplicity $B = \mathrm{Res}_H^G\,\mathrm{Ind}_H^G(jAj)$, we have to prove that the map $\mathrm{Res}_H^G(f)e : jAj \to B$ belongs to the same exomorphism as the canonical map

$$d_H^G : jAj \longrightarrow B\,, \qquad d_H^G(a) = 1 \otimes a \otimes 1\,.$$

Consider

$$b' = \sum_{x\in[G/H]} x \otimes ja''\cdot x^{-1}\cdot j \otimes 1 \qquad \text{and} \qquad b'' = \sum_{y\in[G/H]} 1 \otimes j\cdot y\cdot a'j \otimes y^{-1}$$

which are both easily seen to belong to B^H. We have $f(a) = b'(1\otimes a\otimes 1)b''$ for all $a \in jAj$ (using $a = jaj$) and in particular $f(j) = b'b''$. On the other hand

$$b''b' = \sum_{x\in[G/H]} 1\otimes j\cdot x\cdot a'j\cdot 1\cdot ja''\cdot x^{-1}\cdot j\otimes 1 = 1\otimes jt_H^G(a'ja'')j\otimes 1 = 1\otimes j\otimes 1 .$$

By Exercise 3.2, the two idempotents $f(j)$ and $i = 1 \otimes j \otimes 1$ of B^H are conjugate: $f(j) = {}^{u}i$ where $u \in (B^H)^*$.

We claim that the element $b = u^{-1}b' + (1_B - i)$ is invertible in B^H with inverse $b^{-1} = b''u + (1_B - i)$. Indeed we have $b'i = b'$ and $ib'' = b''$, so that $b'(1_B - i) = 0$ and $(1_B - i)b'' = 0$. Therefore

$$\begin{aligned}(u^{-1}b' + (1_B - i))\,(b''u + (1_B - i)) &= u^{-1}b'b''u + (1_B - i)\\ &= u^{-1}f(j)u + (1_B - i)\\ &= i + 1_B - i \,=\, 1_B\,.\end{aligned}$$

By Exercise 3.3, we also have $(b''u + (1_B - i))\,(u^{-1}b' + (1_B - i)) = 1_B$ and this completes the proof of the claim. It follows that $ubi = b'i = b'$ and $ib^{-1}u^{-1} = ib'' = b''$.

Now for all $a \in jAj$, we have

$$f(a) = b'(1 \otimes a \otimes 1)b'' = ubi(1 \otimes a \otimes 1)ib^{-1}u^{-1} = ub(1 \otimes a \otimes 1)b^{-1}u^{-1}\,,$$

because $i(1\otimes a\otimes 1)i = 1\otimes a\otimes 1$. Thus $f(a) = {}^{ub}(d_H^G(a))$, and since both u and b belong to $(B^H)^*$, we obtain that $\mathrm{Res}_H^G(f)e$ and d_H^G belong to the same exomorphism, as required.

Finally we have to prove that $\mathcal{F}$ is an embedding. Note first that since $1_A = \sum_{g\in[G/H]} {}^{g}(a'ja'')$ we have in particular $A = AjA$ (because ${}^{g}j = g\cdot j\cdot g^{-1} \in AjA$). By Theorem 9.9, jAj and A have the same number of points. But by Lemma 16.1, there is an isomorphism of $\mathcal{O}$-algebras $\mathrm{Ind}_H^G(jAj) \cong M_n(jAj)$ (where $n = |G : H|$) and $M_n(jAj)$ is Morita equivalent to jAj. Consequently A and $\mathrm{Ind}_H^G(jAj)$ have the same number of points. Thus Proposition 12.3 applies (since we are dealing with interior G-algebras) and asserts that $\mathrm{Res}_H^G(\mathcal{F})$ is an embedding (because $\mathrm{Res}_H^G(\mathcal{F})\mathcal{E} = \mathcal{D}_H^G$ is an embedding). This obviously means that $\mathcal{F}$ is an embedding.

In order to establish the additional statement, we note that, by Proposition 12.3 again, the equation $\mathrm{Res}_H^G(\mathcal{F})\mathcal{E} = \mathcal{D}_H^G$ determines uniquely the embedding $\mathrm{Res}_H^G(\mathcal{F})$. By Proposition 12.1 the uniqueness of $\mathrm{Res}_H^G(\mathcal{F})$ implies the uniqueness of $\mathcal{F}$. □

We now prove the global result expressing relative projectivity in terms of induced algebras. Recall that a G-algebra A is projective relative to a subgroup H if the relative trace map $t_H^G : A^H \to A^G$ is surjective. This is equivalent to requiring that $1_A \in A_H^G$.

(17.2) THEOREM. *Let A be an interior G-algebra and let H be a subgroup of G. Denote by $\mathcal{D}_H^G : \mathrm{Res}_H^G(A) \to \mathrm{Res}_H^G \mathrm{Ind}_H^G \mathrm{Res}_H^G(A)$ the canonical embedding associated with the interior H-algebra $\mathrm{Res}_H^G(A)$. The following conditions are equivalent.*
(a) A is projective relative to H.
(b) There exists an exomorphism $\mathcal{F} : A \to \mathrm{Ind}_H^G \mathrm{Res}_H^G(A)$ such that $\mathrm{Res}_H^G(\mathcal{F}) = \mathcal{D}_H^G$.
(c) There exists an embedding $\mathcal{E} : A \to \mathrm{Ind}_H^G(B)$ where B is some interior H-algebra.
Moreover, if these conditions are satisfied, the exomorphism $\mathcal{F}$ is an embedding and is unique.

Proof. It is clear that (a) implies (b), by Theorem 17.1 applied with $j = 1_A$ (and $jAj = \mathrm{Res}_H^G(A)$).

If (b) holds, then $\mathcal{F}$ is necessarily an embedding because $\mathcal{D}_H^G$ is an embedding. Thus (c) is satisfied with $B = \mathrm{Res}_H^G(A)$. Moreover $\mathcal{F}$ is unique by Proposition 12.1, proving the additional statement of the theorem.

Assume now that (c) holds and let $e \in \mathcal{E}$. Since we cannot directly apply the previous theorem, we have to produce a similar argument. As $e(1_A)$ is fixed under G, we have

$$e(1_A) = e(1_A)\,1_{\mathrm{Ind}_H^G(B)}\,e(1_A) = t_H^G\big(e(1_A)(1 \otimes 1_B \otimes 1)e(1_A)\big)\,.$$

Since $\mathcal{E}$ is an embedding, we can write $e(1_A)(1 \otimes 1_B \otimes 1)e(1_A) = e(a)$ for a uniquely determined $a \in A^H$. Then $1_A = t_H^G(a)$, because this relation holds after applying e. This proves (a) and completes the proof of the theorem. □

In the special case of $\mathcal{O}G$-modules, Theorem 17.2 is known as Higman's criterion. We state the result in full.

(17.3) COROLLARY (Higman's criterion). *Let M be an $\mathcal{O}G$-lattice and let H be a subgroup of G. The following conditions are equivalent.*
(a) The G-algebra $\mathrm{End}_{\mathcal{O}}(M)$ is projective relative to H.
(b) M is isomorphic to a direct summand of $\mathrm{Ind}_H^G \mathrm{Res}_H^G(M)$.
(c) M is isomorphic to a direct summand of $\mathrm{Ind}_H^G(L)$ where L is some $\mathcal{O}H$-lattice.

Proof. We consider the interior G-algebra $A = \mathrm{End}_{\mathcal{O}}(M)$ and we apply Theorem 17.2. By Example 16.4, condition (b) in that theorem (together with the extra statement that $\mathcal{F}$ is an embedding) says that there is an embedding

$$\mathrm{End}_{\mathcal{O}}(M) \longrightarrow \mathrm{Ind}_H^G(\mathrm{End}_{\mathcal{O}}(\mathrm{Res}_H^G(M)) \cong \mathrm{End}_{\mathcal{O}}(\mathrm{Ind}_H^G \mathrm{Res}_H^G(M)) .$$

By Proposition 12.5, this is equivalent to condition (b) of the corollary. A similar argument shows that condition (c) in Theorem 17.2 applied to $B = \mathrm{End}_{\mathcal{O}}(L)$ yields condition (c) of the corollary. The result follows immediately from these observations. □

We shall see below (Proposition 17.7) that Higman's criterion actually holds for arbitrary $\mathcal{O}G$-modules. For an $\mathcal{O}G$-module M, the usual definition of the *projectivity relative to* H is the third statement of the corollary, namely that M is isomorphic to a direct summand of $\mathrm{Ind}_H^G(L)$ for some $\mathcal{O}H$-module L. Thus Higman's criterion asserts that M is projective relative to H as an $\mathcal{O}G$-module if and only if $\mathrm{End}_{\mathcal{O}}(M)$ is projective relative to H as a G-algebra. As a useful special case, we consider now the case $H = 1$. Recall that a G-algebra A is called projective if it is projective relative to 1. The next result justifies this terminology.

(17.4) COROLLARY. *An $\mathcal{O}G$-lattice M is a projective $\mathcal{O}G$-module if and only if the G-algebra $\mathrm{End}_{\mathcal{O}}(M)$ is projective.*

Proof. By Corollary 17.3 (applied with $H = 1$), the G-algebra $\mathrm{End}_{\mathcal{O}}(M)$ is projective if and only if M is isomorphic to a direct summand of $\mathrm{Ind}_1^G(L)$ for some $\mathcal{O}$-lattice L. Thus it suffices to prove that $\mathrm{Ind}_1^G(L)$ is a free $\mathcal{O}G$-module. But this is clear since $\mathrm{Ind}_1^G(L) = \mathcal{O}G \otimes_{\mathcal{O}} L$ and L is free as an $\mathcal{O}$-module. □

We warn the reader that this corollary does not hold for arbitrary $\mathcal{O}G$-modules, simply because arbitrary $\mathcal{O}$-modules are no longer projective (or equivalently free) over $\mathcal{O}$.

The condition of projectivity for G-algebras is a condition on the relative trace map. The use of this map for describing the projectivity of modules (Corollary 17.4) finds its origin in the averaging argument which appears in the classical proof of Maschke's theorem. We recover this result of course, which we extend slightly as follows.

(17.5) THEOREM (Maschke). *The following conditions are equivalent.*
(a) p does not divide $|G|$.
(b) The group algebra $\mathcal{O}G$ is a projective G-algebra.
(c) Every $\mathcal{O}G$-lattice is projective.
(d) The trivial $\mathcal{O}G$-lattice $\mathcal{O}$ is projective.
(e) The group algebra $\mathcal{O}G$ is $\mathcal{O}$-semi-simple.

Proof. (a) $\Rightarrow$ (b). The assumption implies that $|G|{\cdot}1_k \neq 0$, so that $|G|{\cdot}1_k$ is invertible in k. It follows that $|G|{\cdot}1_{\mathcal{O}}$ is invertible in $\mathcal{O}$. Therefore the relative trace map in $\mathcal{O}G$ satisfies

$$t_1^G((|G|{\cdot}1)^{-1}) = (|G|{\cdot}1)^{-1} t_1^G(1) = (|G|{\cdot}1)^{-1}(|G|{\cdot}1) = 1\,.$$

Thus $(\mathcal{O}G)_1^G$ contains 1.

(b) $\Rightarrow$ (c). Let M be an $\mathcal{O}G$-lattice and $A = \mathrm{End}_{\mathcal{O}}(M)$. There is a unique unitary homomorphism of interior G-algebras $\phi : \mathcal{O}G \to A$. By assumption there exists $a \in \mathcal{O}G$ such that $t_1^G(a) = 1_{\mathcal{O}G}$. Applying ϕ to this equation, it follows that $t_1^G(\phi(a)) = 1_A$ and therefore the G-algebra A is projective. By Corollary 17.4, M is a projective $\mathcal{O}G$-module.

(c) $\Rightarrow$ (d). Trivial.

(d) $\Rightarrow$ (a). Consider the augmentation map $\varepsilon : \mathcal{O}G \to \mathcal{O}$ mapping every basis element $g \in G$ to 1. This is $\mathcal{O}G$-linear and since $\mathcal{O}$ is a projective $\mathcal{O}G$-module by assumption, there exists an $\mathcal{O}G$-linear map $\sigma : \mathcal{O} \to \mathcal{O}G$ such that $\varepsilon\sigma = id$. Let $a = \sigma(1)$. Then we have $g{\cdot}a = \sigma(g{\cdot}1) = \sigma(1) = a$ because G acts trivially on $\mathcal{O}$. It follows that if we write $a = \sum_{g\in G} \lambda_g g$ with $\lambda_g \in \mathcal{O}$, then all coefficients λ_g must be equal, so that $a = \lambda \sum_{g\in G} g$. Thus

$$1 = \varepsilon\sigma(1) = \varepsilon(a) = \lambda \sum_{g\in G} \varepsilon(g) = \lambda |G|{\cdot}1\,,$$

proving that $|G|{\cdot}1$ is invertible in $\mathcal{O}$. Therefore $|G|{\cdot}1_k$ is also invertible in k and so the characteristic p cannot divide $|G|$.

(a) $\Leftrightarrow$ (e). Since (a) does not make any reference to the ground ring $\mathcal{O}$, we can apply the equivalence between (a) and (c) (which we have just proved) in the situation where k is the ground ring. Thus (a) is equivalent to the projectivity of all kG-modules, which in turn is equivalent to the semi-simplicity of the algebra kG, because the projectivity of simple modules forces the semi-simplicity of all modules. Finally by Exercise 7.6, the semi-simplicity of kG is equivalent to the $\mathcal{O}$-semi-simplicity of $\mathcal{O}G$. □

When p does not divide $|G|$, it is easy to describe all $\mathcal{O}G$-lattices.

(17.6) COROLLARY. *Suppose that* p *does not divide* $|G|$.

(a) *For every simple* kG*-module* $V(\alpha)$ *(corresponding to* $\alpha \in \mathcal{P}(\mathcal{O}G)$ *), there exists an* $\mathcal{O}G$*-lattice* $L(\alpha)$ *, unique up to isomorphism, such that* $L(\alpha)/\mathfrak{p}L(\alpha) \cong V(\alpha)$ *. Moreover* $L(\alpha)$ *is projective indecomposable.*

(b) *Every indecomposable* $\mathcal{O}G$*-lattice is isomorphic to* $L(\alpha)$ *for some* $\alpha \in \mathcal{P}(\mathcal{O}G)$.

Proof. By Theorem 17.5, every $\mathcal{O}G$-lattice is projective, and so is a direct sum of indecomposable projective $\mathcal{O}G$-lattices. The result follows from the bijection between $\mathrm{Proj}(\mathcal{O}G)$ and $\mathrm{Irr}(\mathcal{O}G)$ (Proposition 5.1). Indeed the Jacobson radical of $\mathcal{O}G$ is $\mathfrak{p}\mathcal{O}G$ because $\mathcal{O}G/\mathfrak{p}\mathcal{O}G = kG$ is semi-simple. Thus an indecomposable projective $\mathcal{O}G$-lattice L maps by reduction modulo $\mathfrak{p}$ to a simple kG-module $L/\mathfrak{p}L$.

Alternatively, $\mathcal{O}G$ is $\mathcal{O}$-semi-simple by Theorem 17.5, and one can apply Lemma 7.1 to each simple factor of $\mathcal{O}G$. □

Higman's criterion (Corollaries 17.3 and 17.4) also holds for modules over a twisted group algebra $\mathcal{O}_\sharp\widehat{G}$, but one needs some additional facts. The first approach would be to use the concept of interior $\widehat{G}$-algebra already mentioned in Example 10.4 and to define induction for such interior structures. The main results on induction remain valid in this more general context. Specializing to the case of modules, one obtains the two corollaries above for twisted group algebras. But for simplicity we give a different and direct approach, which is module theoretic. In the special case of ordinary group algebras, this provides a new proof of Corollary 17.3, which in fact holds for arbitrary (finitely generated) $\mathcal{O}G$-modules. The above proof does not apply for arbitrary $\mathcal{O}G$-modules because of the use of Lemma 10.7.

Let $\mathcal{O}_\sharp\widehat{G}$ be a twisted group algebra corresponding to a central extension $\widehat{G}$ of G by $\mathcal{O}^*$. Recall that for any subgroup H of G , the inverse image of H in $\widehat{G}$ is a subgroup $\widehat{H}$ which is a central extension of H by $\mathcal{O}^*$. Moreover the twisted group algebra $\mathcal{O}_\sharp\widehat{H}$ is clearly a subalgebra of $\mathcal{O}_\sharp\widehat{G}$. In particular for $H = 1$, we obtain the subalgebra $\mathcal{O}$. For any $\mathcal{O}_\sharp\widehat{G}$-module M , we use the notation $\mathrm{Res}^G_H(M)$ as in Example 13.5. If N is an $\mathcal{O}_\sharp\widehat{H}$-module, we define

$$\mathrm{Ind}^G_H(N) = \mathcal{O}_\sharp\widehat{G} \otimes_{\mathcal{O}_\sharp\widehat{H}} N \,.$$

Let $[\widehat{G}/\widehat{H}]$ be a set of coset representatives of $\widehat{H}$ in $\widehat{G}$ (in bijection with a set $[G/H]$ of coset representatives of H in G , via the canonical map $\widehat{G} \to G$). Then $\mathcal{O}_\sharp\widehat{G}$ is a free module over $\mathcal{O}_\sharp\widehat{H}$ with basis $[\widehat{G}/\widehat{H}]$, and therefore

$$\mathrm{Ind}^G_H(N) = \bigoplus_{x\in[\widehat{G}/\widehat{H}]} x \otimes N \,.$$

We also note that $\mathrm{Ind}_H^G(N) \cong \mathrm{Ind}_{\widehat{H}}^{\widehat{G}}(N)$, using the ordinary definition of induction from the subgroup $\widehat{H}$ (which has finite index in $\widehat{G}$). Now we can state Higman's criterion for modules over a twisted group algebra.

(17.7) PROPOSITION (Higman's criterion). *Let M be an $\mathcal{O}_\sharp\widehat{G}$-module and let H be a subgroup of G. The following conditions are equivalent.*

(a) *The G-algebra $\mathrm{End}_{\mathcal{O}}(M)$ is projective relative to H.*

(b) *M is isomorphic to a direct summand of $\mathrm{Ind}_H^G \mathrm{Res}_H^G(M)$.*

(c) *M is isomorphic to a direct summand of $\mathrm{Ind}_H^G(N)$ where N is some $\mathcal{O}_\sharp\widehat{H}$-module.*

Proof. (a) $\Rightarrow$ (b). Consider the homomorphism of $\mathcal{O}_\sharp\widehat{G}$-modules

$$\pi : \mathrm{Ind}_H^G \mathrm{Res}_H^G(M) \longrightarrow M\,, \qquad x \otimes v \mapsto x\cdot v\,.$$

We can assume that the transversal $[\widehat{G}/\widehat{H}]$ contains 1. Then π has an $\mathcal{O}_\sharp\widehat{H}$-linear section s defined by $s(v) = 1 \otimes v$. By assumption there exists $a \in \mathrm{End}_{\mathcal{O}}(M)$ such that $t_H^G(a) = id_M$. We construct a new section of π as follows:

$$\sigma : M \longrightarrow \mathrm{Ind}_H^G \mathrm{Res}_H^G(M)\,, \qquad v \mapsto \sum_{x\in[\widehat{G}/\widehat{H}]} x\cdot sa(x^{-1}\cdot v)\,.$$

Since π commutes with the action of $\widehat{G}$, we have

$$\pi\sigma(v) = \sum_{x\in[\widehat{G}/\widehat{H}]} x\cdot\pi sa(x^{-1}\cdot v) = \sum_{x\in[\widehat{G}/\widehat{H}]} x\cdot a(x^{-1}\cdot v) = t_H^G(a)(v) = v\,,$$

so that σ is indeed a section of π. The proof that σ commutes with the action of $\widehat{G}$ is elementary (and is the same as the proof that the image of t_H^G is contained in the set of G-fixed elements). Thus π has a section σ which is $\mathcal{O}_\sharp\widehat{G}$-linear, and this proves that M is isomorphic (via σ) to a direct summand of $\mathrm{Ind}_H^G \mathrm{Res}_H^G(M)$.

(b) $\Rightarrow$ (c). This is trivial.

(c) $\Rightarrow$ (a). By assumption there exists an idempotent

$$i \in \mathrm{End}_{\mathcal{O}_\sharp\widehat{G}}(\mathrm{Ind}_H^G(N)) = \mathrm{End}_{\mathcal{O}}(\mathrm{Ind}_H^G(N))^G$$

such that $M \cong i\,\mathrm{Ind}_H^G(N)$. Thus $\mathrm{End}_{\mathcal{O}}(M) \cong i\,\mathrm{End}_{\mathcal{O}}(\mathrm{Ind}_H^G(N))\,i$ and we have to show that i belongs to the image of the trace map t_H^G. It suffices to prove that the whole G-algebra $\mathrm{End}_{\mathcal{O}}(\mathrm{Ind}_H^G(N))$ is projective relative to H. Consider the decomposition

$$\mathrm{Ind}_H^G(N) = \bigoplus_{x\in[\widehat{G}/\widehat{H}]} x\otimes N$$

and let $a \in \mathrm{End}_{\mathcal{O}}(\mathrm{Ind}_H^G(N))$ be the projection onto $1\otimes N$. Then for $y\in[\widehat{G}/\widehat{H}]$, we have

$$\begin{aligned} t_H^G(a)(y\otimes v) &= \sum_{x\in[\widehat{G}/\widehat{H}]} x\cdot a(x^{-1}\cdot(y\otimes v)) = \sum_{x\in[\widehat{G}/\widehat{H}]} x\cdot a(x^{-1}y\otimes v) \\ &= y\cdot(1\otimes v) = y\otimes v\,, \end{aligned}$$

so that $t_H^G(a) = id_{\mathrm{Ind}_H^G(N)}$, proving the relative projectivity. □

As before the special case $H=1$ is particularly important. The statement only holds for lattices.

(17.8) COROLLARY. *An $\mathcal{O}_\sharp\widehat{G}$-lattice M is projective if and only if the G-algebra $\mathrm{End}_{\mathcal{O}}(M)$ is projective.*

Proof. The argument is the same as that of Corollary 17.4. Indeed if L is a free $\mathcal{O}$-module, then $\mathrm{Ind}_1^G(L) = \mathcal{O}_\sharp\widehat{G}\otimes_{\mathcal{O}} L$ is a free $\mathcal{O}_\sharp\widehat{G}$-module. □

We now turn to the second application of Theorem 17.1, a result connecting induced algebras and relative projectivity of pointed groups. We first fix the notation. Let G_α and H_β be pointed groups on an interior G-algebra A and assume that $G_\alpha \geq H_\beta$. By Proposition 13.6, there exists a unique embedding $\mathcal{F}_\beta^\alpha : A_\beta \to \mathrm{Res}_H^G(A_\alpha)$ which expresses the containment $H_\beta \leq G_\alpha$. Let also $\mathcal{D}_H^G : A_\beta \to \mathrm{Res}_H^G\,\mathrm{Ind}_H^G(A_\beta)$ be the canonical embedding associated with the interior H-algebra A_β.

(17.9) THEOREM. *Let G_α and H_β be pointed groups on an interior G-algebra A. Assume that $G_\alpha \geq H_\beta$. The following conditions are equivalent.*

(a) $G_\alpha\,pr\,H_\beta$.

(b) There exists an embedding $\mathcal{F} : A_\alpha \to \mathrm{Ind}_H^G(A_\beta)$ such that the following diagram of exomorphisms commutes (using the notation above).

$$\begin{array}{ccc} A_\beta & \xrightarrow{\mathcal{D}_H^G} & \mathrm{Res}_H^G\,\mathrm{Ind}_H^G(A_\beta) \\ {\scriptstyle \mathcal{F}_\beta^\alpha}\big\downarrow & \nearrow{\scriptstyle \mathrm{Res}_H^G(\mathcal{F})} & \\ \mathrm{Res}_H^G(A_\alpha) & & \end{array}$$

If this condition is satisfied, the embedding $\mathcal{F}$ is unique.

Proof. Assume first that the embedding $\mathcal{F}$ exists. We have to prove that $G_\alpha\, pr\, H_\beta$ in the interior G-algebra A. We use the identification of pointed groups given by Proposition 15.1. Since there is an embedding $\mathcal{F}_\alpha : A_\alpha \to A$, it suffices to prove that $G_\alpha\, pr\, H_\beta$ in A_α. We use here the fact that the pointed group H_β is the image of a pointed group on A_α, because $G_\alpha \geq H_\beta$ by assumption (Proposition 15.2). Now there is also an embedding $\mathcal{F} : A_\alpha \to \mathrm{Ind}_H^G(A_\beta)$, so we have to prove that $G_{\alpha'}\, pr\, H_{\beta'}$ in $\mathrm{Ind}_H^G(A_\beta)$, where α' and β' denote the images of the points α and β under $\mathcal{F}$. By the commutativity of the diagram of exomorphisms in the statement, the point β', being the image of β via the composite of $\mathcal{F}_\beta^\alpha$ and $\mathrm{Res}_H^G(\mathcal{F})$, is also the image of β under the exomorphism $\mathcal{D}_H^G$. But the point β on A_β is just the singleton 1_{A_β} and its image β' under $\mathcal{D}_H^G$ is the point of $\mathrm{Ind}_H^G(A_\beta)^H$ containing $i = 1 \otimes 1_{A_\beta} \otimes 1$ (by definition of $\mathcal{D}_H^G$). Thus we have to prove that $\alpha' \subseteq t_H^G(B^H i B^H)$ where $B = \mathrm{Ind}_H^G(A_\beta)$. By the construction of induced algebras, we have

$$1_B = \sum_{g \in [G/H]} g \otimes 1_{A_\beta} \otimes g^{-1} = t_H^G(i)\,.$$

Therefore the ideal $t_H^G(B^H i B^H)$ contains 1_B and so is the whole of B^G. Thus α' (like any other point of B^G) is contained in this ideal, as required.

Now we assume that $G_\alpha\, pr\, H_\beta$ and we have to construct $\mathcal{F}$. Since H_β is the image of a pointed group on A_α (because $G_\alpha \geq H_\beta$), only A_α comes into play (together with the embedded algebra A_β). Thus we can assume that $A = A_\alpha$, so that $\alpha = \{1_A\}$ and A^G is a local ring. We can choose $A_\beta = jAj$ where $j \in \beta$ and then take $\mathcal{F}_\beta^\alpha$ to be the exomorphism containing the inclusion $f_\beta^\alpha : jAj \to A$. By Lemma 14.1, our hypothesis that $G_\alpha\, pr\, H_\beta$ is equivalent to the existence of $a', a'' \in A^H$ such that $1_A = t_H^G(a' j a'')$. Thus we are exactly in the situation of Theorem 17.1. It follows that there exists an embedding $\mathcal{F} : A \to \mathrm{Ind}_H^G(A_\beta)$ such that $\mathrm{Res}_H^G(\mathcal{F})\mathcal{F}_\beta^\alpha = \mathcal{D}_H^G$, and that this embedding is unique. □

We remark that in Theorem 17.1 and Theorem 17.9 it is in general *not* possible to choose representatives of the exomorphisms in such a way that one gets a commutative diagram of homomorphisms (Exercise 17.1). This is one of the key reasons for introducing exomorphisms.

(17.10) COROLLARY. *Let A be an interior G-algebra and let G_α and H_β be pointed groups on A such that $G_\alpha \geq H_\beta$ and $G_\alpha\, pr\, H_\beta$. Then the $\mathcal{O}$-algebras A_α and A_β are Morita equivalent.*

Proof. The restriction $\mathrm{Res}^H_1(\mathcal{F}^\alpha_\beta)$ yields an embedding of $\mathcal{O}$-algebras $A_\beta \to A_\alpha$. By the theorem, there exists an embedding $\mathcal{F} : A_\alpha \to \mathrm{Ind}^G_H(A_\beta)$ and its restriction to the trivial subgroup is an embedding $A_\alpha \to M_n(A_\beta)$ where $n = |G{:}H|$ (by Lemma 16.1). Therefore by Lemma 8.9, A_α and A_β have the same number of points and by Theorem 9.9 they are Morita equivalent. □

Theorem 17.9 gives a characterization of the relation pr under the assumption that the other relation $\geq$ holds. But the relation pr may hold when $\geq$ does not hold (Exercise 17.5), and one may ask for a direct interpretation of the relation pr in terms of induced algebras. There is a general answer to this question, but in this text we only treat the case of $\mathcal{O}G$-modules, and this provides an improvement of Theorem 17.9 in that case. Although it is actually not a restriction to work with a pointed group G_α corresponding to the whole group G, we state the result for an arbitrary pair of pointed groups.

(17.11) PROPOSITION. *Let* $A = \mathrm{End}_\mathcal{O}(M)$ *be the interior algebra associated with an* $\mathcal{O}G$*-module* M, *let* H_α *be a pointed group on* A *corresponding to an indecomposable direct summand* M_α *of* $\mathrm{Res}^G_H(M)$, *and let* K_β *be a pointed group on* A *corresponding to an indecomposable direct summand* M_β *of* $\mathrm{Res}^G_K(M)$. *The following conditions are equivalent.*

(a) $H_\alpha \, pr \, K_\beta$.

(b) M_α *is isomorphic to a direct summand of* $\mathrm{Ind}^H_K(M_\beta)$.

Proof. As we cannot apply Theorem 17.9, we need to use another argument, which is module-theoretic (hence applies to arbitrary $\mathcal{O}G$-modules rather than $\mathcal{O}G$-lattices). We choose $i \in \alpha$ and $M_\alpha = iM$, and similarly $j \in \beta$ and $M_\beta = jM$.

Assume that (a) holds, that is, $i \in t^H_K(A^K jA^K)$. By Lemma 14.1, there exist $a, b \in A^K$ such that $t^H_K(ajb) = i$. The $\mathcal{O}K$-linear endomorphism ia restricts to an $\mathcal{O}K$-linear map

$$jM \longrightarrow iM\,, \qquad v \mapsto ia(v)\,,$$

and this induces an $\mathcal{O}H$-linear map

$$\pi : \mathrm{Ind}^H_K(jM) \longrightarrow iM\,, \qquad h \otimes v \mapsto h{\cdot}ia(v) = i{\cdot}h{\cdot}a(v)\,.$$

It is easy to see that the following map commutes with the action of H, hence is $\mathcal{O}H$-linear:

$$\sigma : iM \longrightarrow \mathrm{Ind}^H_K(jM)\,, \qquad v \mapsto \sum_{h\in[H/K]} h \otimes jb{\cdot}h^{-1}(v)\,.$$

Now σ is a section of π because if $v \in iM$,

$$\pi\sigma(v) = \sum_{h\in[H/K]} i{\cdot}h{\cdot}ajb{\cdot}h^{-1}(v) = i\, t_K^H(ajb)(v) = i(v) = v\,.$$

Therefore iM is isomorphic (via σ) to a direct summand of $\mathrm{Ind}_K^H(jM)$.

Conversely assume now that iM is isomorphic to a direct summand of $\mathrm{Ind}_K^H(jM)$. We consider M only with its $\mathcal{O}H$-module structure and for simplicity of notation we write M instead of $\mathrm{Res}_H^G(M)$ and A instead of $\mathrm{Res}_H^G(A)$. Let $L = \mathrm{Ind}_K^H(jM)$ and consider the $\mathcal{O}H$-module $X = M \oplus L$ and its endomorphism algebra $B = \mathrm{End}_{\mathcal{O}}(X)$. Let $e \in B^H$ be the projection onto M and let $f \in B^H$ be the projection onto L, so that $id_X = e + f$ is an orthogonal decomposition in B^H with $M = eX$ and $L = fX$. Then by Lemma 12.4 there is an isomorphism of H-algebras $eBe \cong A = \mathrm{End}_{\mathcal{O}}(M)$ and we identify A with eBe. In particular we have $i, j \in eBe$ so that $i = eie$ and $j = eje$.

Let $j' \in B^K$ be the projection onto the direct summand jM of $\mathrm{Res}_K^H \mathrm{Ind}_K^H(jM) = \mathrm{Res}_K^H(L)$, so that $j' = fj'f$. Let $i' \in B^H$ be the projection onto the direct summand of L isomorphic to iM, which exists by assumption. We have $i' = fi'f$. By Corollary 4.5, $i = ci'c^{-1}$ for some $c \in B^H$ and $j = dj'd^{-1}$ for some $d \in B^K$. The identity map id_L of the induced module $L = \mathrm{Ind}_K^H(jM)$ is the relative trace of the projection onto jM (see Example 16.4). Thus $t_K^H(j')$ is the identity on L and is zero on M, that is, $t_K^H(j') = f$. In particular $i' = i'f = t_K^H(i'j')$ and therefore

$$i = ci'c^{-1} = t_K^H(ci'j'c^{-1}) = t_K^H(ci'd^{-1}jdc^{-1})\,.$$

But as $i = eie$ and $j = eje$, it follows that

$$i = eie = t_K^H(eci'd^{-1}ejedc^{-1}e) \in t_K^H(A^K jA^K)$$

because $eBe = A$. This shows that $H_\alpha \,pr\, K_\beta$ and completes the proof. □

Exercises

(17.1) Assume for simplicity that A is a primitive interior G-algebra and let $\alpha = \{1_A\}$. In the situation of Theorem 17.9, prove that one can choose representatives of the exomorphisms in such a way that one gets a commutative diagram of homomorphisms if and only if there exists $j \in \beta$ such that $1_A = t_H^G(j)$ and $j\,{}^g j = 0$ for all $g \in G - H$. In this situation A is isomorphic to $\mathrm{Ind}_H^G(A_\beta)$.

(17.2) The purpose of this exercise is to prove a result of Higman: the number of isomorphism classes of indecomposable kG-modules is finite if and only if a Sylow p-subgroup of G is cyclic.

(a) Show that any kG-module is isomorphic to a direct summand of an induced module $\mathrm{Ind}_P^G(M)$, where P is a Sylow p-subgroup of G. Deduce that the number of isomorphism classes of indecomposable kG-modules is finite if and only if the number of isomorphism classes of indecomposable kP-modules is finite, using the Krull–Schmidt theorem 4.4.

(b) Let P be a cyclic group of order p^n generated by h. Prove that $kP \cong k[t]/(t^{p^n})$ where t is an indeterminate, mapping to $h-1$ in kP. Show that the modules $k[t]/(t^r)$ (for $1 \leq r \leq p^n$) form a complete list of indecomposable kP-modules up to isomorphism.

(c) Let P be a non-cyclic p-group. Show that some quotient of P is isomorphic to a direct product of two cyclic groups of order p.

(d) Let P be the direct product of two cyclic groups of order p, generated by x and y respectively. Show that the following modules M_k (for $k \geq 1$) form an infinite sequence of pairwise non-isomorphic indecomposable kP-modules. The module M_k is $2k$-dimensional with basis $(v_1, \ldots, v_k, w_1, \ldots, w_k)$. The action of P is defined by $(x-1)\cdot w_i = 0$, $(y-1)\cdot w_i = 0$, $(x-1)\cdot v_i = w_i$ (for $1 \leq i \leq k$) and finally $(y-1)\cdot v_i = w_{i+1}$ (for $1 \leq i \leq k-1$) and $(y-1)\cdot v_k = 0$.

(e) Complete the proof of Higman's result.

(17.3) Let $\widehat{G}$ be a central extension of G by k^* and let $k_\sharp \widehat{G}$ be the corresponding twisted group algebra. Prove that if p does not divide $|G|$, then $k_\sharp \widehat{G}$ is semi-simple. [Hint: Use the method of Theorem 17.5. The converse statement will be proved in Exercise 21.3.]

(17.4) Let M be an $\mathcal{O}G$-lattice and assume that M is projective relative to a subgroup H. Prove that the $\mathcal{O}G$-lattices $M \otimes_{\mathcal{O}} N$, $\mathrm{Hom}_{\mathcal{O}}(M,N)$, and $\mathrm{Hom}_{\mathcal{O}}(N,M)$ are projective relative to H, for any $\mathcal{O}G$-lattice N. In particular these $\mathcal{O}G$-lattices are projective if M is projective. [Hint: Use Lemma 14.3. Remember also the isomorphisms $\mathrm{Hom}_{\mathcal{O}}(M,N) \cong M^* \otimes_{\mathcal{O}} N$ and $\mathrm{End}_{\mathcal{O}}(M^*) \cong \mathrm{End}_{\mathcal{O}}(M)^{op}$.]

(17.5) Let G be the symmetric group on 3 letters, let P be a subgroup of order 2, and take $p = 2$. Let $M = \mathrm{Ind}_P^G(k)$ and $A = \mathrm{End}_k(M)$.

(a) Prove that $M \cong k \oplus L$ where L is a projective kG-module. [Hint: If a is a generator of the normal subgroup of order 3, then $\{1, a, a^2\}$ are coset representatives of G/P. Prove that $(1+a+a^2) \otimes 1_k$ generates a trivial submodule of $\mathrm{Ind}_P^G(k)$, and that $\{ (1+a) \otimes 1_k , (1+a^2) \otimes 1_k \}$ is a basis of a 2-dimensional kG-submodule L of $\mathrm{Ind}_P^G(k)$, which is free on restriction to P.]

(b) Let α be the point of A^G corresponding to the direct summand L, and let γ be the point of A^P corresponding to the trivial direct summand k. Prove that $G_\alpha \, pr \, P_\gamma$, but $G_\alpha \not\geq P_\gamma$.

(17.6) Let K be a field of characteristic not dividing $|G|$ (for instance characteristic zero).

(a) Define the notion of G-algebra over K and prove that any G-algebra over K is projective.

(b) Prove that any (finitely generated) KG-module is projective. [Hint: Follow either the method of Corollaries 17.3 and 17.4, or that of Proposition 17.7 and Corollary 17.8.]

(c) Prove that KG is a semi-simple K-algebra (Maschke's theorem).

Notes on Section 17

Higman's criterion goes back to Gaschütz [1952] as well as Higman [1954]. The generalization to interior G-algebras is due to Puig [1981]. The result of Exercise 17.2 is due to Higman [1954]. For arbitrary interior G-algebras, there is a characterization of the relation *pr* in terms of induced algebras which generalizes Proposition 17.11. This appears in Barker [1994c].

§ 18 DEFECT THEORY

This section is devoted to the defect theory of pointed groups, which is a reduction to the case of p-groups and local points. The results are first developed for arbitrary G-algebras. At the end of the section, we consider the case of interior algebras, where a much finer result holds, involving the induction procedure introduced in Section 16. We shall extend the theory in the next section, where we discuss a reduction to the case of projective modules.

Let A be a G-algebra and let H_α be a pointed group on A. We define a *defect pointed group* of H_α, or simply a *defect* of H_α, to be a pointed group P_γ such that $H_\alpha \geq P_\gamma$, $H_\alpha \, pr \, P_\gamma$, and P_γ is local. Note that by Exercises 13.4 and 14.1, any H-conjugate of P_γ is also a defect of H_α. It is not clear from this definition that a defect of H_α exists. We first prove this.

(18.1) LEMMA. *Let H_α be a pointed group on a G-algebra A. Then a defect of H_α exists.*

Proof. Let P be a minimal subgroup such that $\alpha \subseteq A_P^H$. Let $i \in \alpha$ and let J be a primitive decomposition of $r_P^H(i)$, that is, $r_P^H(i) = \sum_{j\in J} j$. Since $i \in A_P^H$, we can write $i = t_P^H(a)$ for some $a \in A^P$, and we obtain

$$i = i^2 = t_P^H(a)i = t_P^H(a\, r_P^H(i)) = t_P^H\Big(\sum_{j\in J} a\, j\Big).$$

It follows that $i \in \sum_{j\in J} t_P^H(A^P jA^P)$ and by Rosenberg's lemma (Proposition 4.9), there exists j such that $i \in t_P^H(A^P jA^P)$. This means that $H_\alpha \, pr \, P_\gamma$ where γ is the point of A^P containing j. Since j appears in a decomposition of $r_P^H(i)$, we also have $H_\alpha \geq P_\gamma$. Finally, in order to prove that P_γ is local, suppose that $P_\gamma \, pr \, Q_\delta$ for some pointed group Q_δ. By transitivity, we have $H_\alpha \, pr \, Q_\delta$ and in particular H_α is projective relative to Q, that is, $\alpha \subseteq A_Q^H$. By minimality of the choice of P, we deduce that $Q = P$. By Lemma 14.4, this shows that P_γ is local and completes the proof that P_γ is a defect of H_α. □

The next result is the crucial lemma.

(18.2) LEMMA. *Let* A *be a* G*-algebra and let* H_α , K_β *and* P_γ *be pointed groups on* A . *Assume that*
(i) P_γ *is local and* $H_\alpha \geq P_\gamma$,
(ii) $H_\alpha \, pr \, K_\beta$.
Then there exists $h \in H$ *such that* $K_\beta \geq {}^h(P_\gamma)$.

Proof. Let $S(\gamma)$ be the simple quotient of A^P corresponding to γ and let $\pi_\gamma : A^P \to S(\gamma)$ be the canonical map. Let $i \in \alpha$. Since $H_\alpha \, pr \, K_\beta$, there exists $a \in A^K \beta A^K$ such that $i = t_K^H(a)$. Now restrict to P and apply π_γ . By the Mackey decomposition formula 11.3, we obtain

$$\pi_\gamma \, r_P^H(i) = \sum_{h \in [P \backslash H/K]} \pi_\gamma \, t_{P \cap {}^hK}^P \, r_{P \cap {}^hK}^{{}^hK}({}^ha) = \sum_{\substack{h \in [P \backslash H/K] \\ P \leq {}^hK}} \pi_\gamma \, r_P^{{}^hK}({}^ha)$$

because P_γ is local, so that $\mathrm{Ker}(\pi_\gamma) \supseteq \mathrm{Ker}(br_P)$ (Lemma 14.4) and $\pi_\gamma \, t_X^P = 0$ for every proper subgroup X of P . On the other hand since $H_\alpha \geq P_\gamma$, we have $\pi_\gamma \, r_P^H(i) \neq 0$ (see Lemma 13.3), and it follows that there exists $h \in H$ such that $P \leq {}^hK$ and $\pi_\gamma \, r_P^{{}^hK}({}^ha) \neq 0$. But $a \in A^K \beta A^K$ and so $\pi_\gamma \, r_P^{{}^hK}({}^h\beta) \neq 0$. This means exactly that ${}^h(K_\beta) \geq P_\gamma$. Thus $K_\beta \geq {}^{h^{-1}}(P_\gamma)$ as required. □

We can now state the first main result of the defect theory. Note that the words *minimal* and *maximal* always refer to the containment relation $\geq$ between pointed groups.

(18.3) THEOREM. *Let* H_α *be a pointed group on a* G*-algebra* A .
(a) *All defect pointed groups of* H_α *are conjugate under* H .
(b) *The following conditions on a pointed group* P_γ *on* A *are equivalent.*
(i) P_γ *is a defect of* H_α .
(ii) P_γ *is a minimal pointed group such that* $H_\alpha \, pr \, P_\gamma$.
(iii) P_γ *is a maximal pointed group such that* P_γ *is local and* $H_\alpha \geq P_\gamma$.
(iv) $H_\alpha \, pr \, P_\gamma$ *and* $br_P \, r_P^H(\alpha) \neq 0$.
(v) P_γ *is local,* $H_\alpha \geq P_\gamma$ *and* H_α *is projective relative to* P .

Proof. We first prove the equivalences of part (b). Let Q_δ be a defect of H_α , which exists by Lemma 18.1. Many steps of the proof consist in comparing P_γ with Q_δ , using Lemma 18.2.

(i) $\Rightarrow$ (ii). Let R_ε be such that $H_\alpha \, pr \, R_\varepsilon$ and $P_\gamma \geq R_\varepsilon$. By Lemma 18.2 (applied to H_α , R_ε and P_γ), we have $R_\varepsilon \geq {}^h(P_\gamma)$ for some $h \in H$. This forces the equality $P_\gamma = R_\varepsilon$ and proves the minimality condition on P_γ .

(ii) $\Rightarrow$ (iii). By Lemma 18.2 (applied to H_α, P_γ and Q_δ), we have $P_\gamma \geq {}^h(Q_\delta)$ for some $h \in H$ and by minimality of P_γ, it follows that $P_\gamma = {}^h(Q_\delta)$. In particular P_γ is local and $H_\alpha \geq P_\gamma$. Let R_ε be a pointed group such that R_ε is local and $H_\alpha \geq R_\varepsilon \geq P_\gamma$. By Lemma 18.2 (applied to H_α, P_γ and R_ε), we have $P_\gamma \geq {}^{h'}(R_\varepsilon)$ for some $h' \in H$. This forces the equality $P_\gamma = R_\varepsilon$ and proves the maximality condition on P_γ.

(iii) $\Rightarrow$ (iv). By Lemma 18.2 (applied to H_α, Q_δ and P_γ), we have ${}^h(Q_\delta) \geq P_\gamma$ for some $h \in H$ and by maximality of P_γ, it follows that $P_\gamma = {}^h(Q_\delta)$. In particular $H_\alpha \, pr \, P_\gamma$, proving the first statement. Since γ is local, $\overline{\gamma} = br_P(\gamma)$ is a point of $\overline{A}(P)$ (see Lemma 14.5) and the canonical morphism $\pi_\gamma : A^P \to S(\gamma)$ is the composite of the morphisms $br_P : A^P \to \overline{A}(P)$ and $\pi_{\overline{\gamma}} : \overline{A}(P) \to S(\gamma)$. Since $P_\gamma \leq H_\alpha$, we have by Lemma 13.3

$$0 \neq \pi_\gamma(r_P^H(\alpha)) = \pi_{\overline{\gamma}} \, br_P(r_P^H(\alpha)) \, .$$

Therefore $br_P \, r_P^H(\alpha) \neq 0$ as required.

(iv) $\Rightarrow$ (v). By Lemma 18.2 (applied to H_α, P_γ and Q_δ), we have $P_\gamma \geq {}^h(Q_\delta)$ for some $h \in H$. Since $br_P \, r_P^H(\alpha) \neq 0$, there exists $i \in \alpha$ and a primitive idempotent j of A^P such that j appears in a decomposition of $r_P^H(i)$ and $br_P(j) \neq 0$. Hence if ε denotes the point of A^P containing j, we have $H_\alpha \geq P_\varepsilon$ and P_ε is local. By Lemma 18.2 (applied to H_α, Q_δ and P_ε), we obtain $Q_\delta \geq {}^{h'}(P_\varepsilon)$ for some $h' \in H$. Combining this with the other relation above, we necessarily have $P_\gamma = {}^h(Q_\delta) = {}^{hh'}(P_\varepsilon)$. Thus P_γ is a defect of H_α, since any H-conjugate of Q_δ is a defect. In particular P_γ satisfies (v).

(v) $\Rightarrow$ (i). Since H_α is projective relative to P, there exists a point ε such that $H_\alpha \, pr \, P_\varepsilon$. By Lemma 18.2 (applied to H_α, P_ε and P_γ), there exists $h \in H$ such that $P_\varepsilon \geq {}^h(P_\gamma)$ (and therefore $h \in N_H(P)$). Conjugating by h^{-1} the relation $H_\alpha \, pr \, P_\varepsilon$, we obtain $H_\alpha \, pr \, P_\gamma$, as was to be shown.

We have seen in the proof that any pointed group satisfying either (ii), (iii) or (iv) is H-conjugate to Q_δ. This shows that all pointed groups satisfying the equivalent conditions are conjugate under H, proving (a). $\square$

A very useful way to visualize the third equivalent condition in the theorem is the following.

(18.4) COROLLARY. *Let H_α be a pointed group on a G-algebra A. The partially ordered set of local pointed groups Q_δ such that $Q_\delta \leq H_\alpha$ has a unique H-conjugacy class of maximal elements, consisting of the defect pointed groups of H_α.*

We have already noticed that pointed groups are generalizations of subgroups and that local pointed groups are generalizations of p-subgroups (Exercise 14.2). Now defect pointed groups (that is, maximal local pointed groups) are generalizations of Sylow p-subgroups and are all conjugate. Note that Corollary 18.4 actually contains as a special case the fact that all Sylow p-subgroups of a finite group are conjugate (Exercise 18.1).

If P_γ is a defect of H_α, the subgroup P is called a *defect group* of H_α, and the point γ is called a *source point* of H_α. Thus all defect groups of H_α are H-conjugate, and for a fixed defect group P, all points of A^P which are source points of H_α are conjugate under $N_G(P)$.

If we localize with respect to the source point γ, we obtain a primitive P-algebra A_γ, called a *source algebra* of H_α. An associated embedding $\mathcal{F}_\gamma : A_\gamma \to \mathrm{Res}^G_P(A)$ is unique up to a unique exo-isomorphism, but A_γ alone (that is, without the embedding $\mathcal{F}_\gamma$) is simply defined up to isomorphism. Thus, given a source point γ, a source algebra A_γ is unique up to isomorphism. But for a fixed defect group P, a source point γ is only unique up to $N_G(P)$-conjugation, and for this reason the source algebras are not unique up to isomorphism, but only up to conjugation: if $g \in N_G(P)$, then $A_{{}^g\gamma} \cong {}^g(A_\gamma)$, the conjugate P-algebra. If $g \in N_G(P_\gamma)$, then ${}^g\gamma = \gamma$ and ${}^g(A_\gamma) \cong A_\gamma$; but if $g \in N_G(P) - N_G(P_\gamma)$, then ${}^g(A_\gamma)$ need not be isomorphic to A_γ. Of course ${}^g(A_\gamma)$ is isomorphic to A_γ as an $\mathcal{O}$-algebra, but the P-algebra structure may differ. Note that if A is an interior G-algebra, then a source algebra is also an interior P-algebra.

By definition of a primitive G-algebra A, the unique point $\alpha = \{1_A\}$ of A^G is singled out and it is very convenient to assign to A itself the various invariants attached to G_α. Thus if A is a primitive G-algebra, we define a *defect pointed group of* A, a *defect group of* A, a *source point of* A and a *source algebra of* A as being those of the corresponding pointed group G_α. In the special case where the primitive G-algebra $A = \mathrm{End}_{\mathcal{O}}(V)$ corresponds to an indecomposable $\mathcal{O}G$-lattice V, a defect group of A is also called a *vertex* of the module V. Moreover if P is a vertex of V and if $j \in A^P$ belongs to a source point of A, then the indecomposable $\mathcal{O}P$-lattice jV is called a *source* of V. For a fixed source point, all sources of V are isomorphic, because a different choice of j in the source point yields an isomorphic $\mathcal{O}P$-lattice.

If A is now an arbitrary G-algebra and α is a point of A^G, then we can localize with respect to α and consider the above invariants for the primitive G-algebra A_α. If the pointed groups on A_α are identified with pointed groups on A (via the identification of Propositions 15.1 and 15.2), then it is elementary to check that a defect pointed group of A_α, a defect group of A_α, a source point of A_α, and a source algebra of A_α are precisely those of the corresponding pointed group G_α (Exercise 18.2).

This allows us to say that a source algebra A_γ of G_α is a source algebra of the primitive G-algebra A_α, and similarly for the other invariants.

Our next result shows that one can directly characterize defect groups without introducing the corresponding source points.

(18.5) PROPOSITION. *Let H_α be a pointed group on a G-algebra A. The following conditions on a subgroup P are equivalent.*

(a) P is a defect group of H_α.

(b) P is a minimal subgroup such that H_α is projective relative to P.

(c) P is a maximal subgroup such that $P \leq H$ and $br_P\, r_P^H(\alpha) \neq 0$.

(d) H_α is projective relative to P and $br_P\, r_P^H(\alpha) \neq 0$.

Proof. (a) $\Leftrightarrow$ (b). Assume that (b) holds. Since H_α is projective relative to P, there exists $\gamma \in \mathcal{P}(A^P)$ such that $H_\alpha\, pr\, P_\gamma$. Moreover the minimality of P implies the minimality of P_γ with respect to this property. Thus the property (ii) of Theorem 18.3 is satisfied and P_γ is a defect pointed group of H_α. This proves that (a) holds. One shows that (a) implies (b) by reversing this argument.

(a) $\Leftrightarrow$ (c). Assume that (c) holds and let j be a primitive idempotent of $\overline{A}(P)$ appearing in the decomposition of $br_P\, r_P^H(i)$, where $i \in \alpha$. Then j belongs to a point $\overline{\gamma} \in \mathcal{P}(\overline{A}(P))$, which lifts to a local point $\gamma \in \mathcal{LP}(A^P)$ (by Lemma 14.5). The canonical map $\pi_\gamma : A^P \to S(\gamma)$ onto the multiplicity algebra of γ factorizes as the composite of $br_P : A^P \to \overline{A}(P)$ and $\pi_{\overline{\gamma}} : \overline{A}(P) \to S(\gamma)$. Therefore we obtain

$$\pi_\gamma(r_P^H(\alpha)) = \pi_{\overline{\gamma}}\, br_P(r_P^H(\alpha)) \neq 0 \,.$$

By Lemma 13.3, this shows that $H_\alpha \geq P_\gamma$. Conversely, reversing this argument, we see that if there exists a local point $\gamma \in \mathcal{LP}(A^P)$ such that $H_\alpha \geq P_\gamma$, then $br_P\, r_P^H(\alpha) \neq 0$. Clearly the maximality of P with respect to the property (c) is equivalent to the maximality of the local pointed group P_γ with respect to the property $H_\alpha \geq P_\gamma$. This proves that (c) holds if and only if there exists γ satisfying condition (iii) of Theorem 18.3. This completes the proof of the equivalence of (a) and (c).

(a) $\Leftrightarrow$ (d). By definition, H_α is projective relative to P if and only if there exists $\gamma \in \mathcal{P}(A^P)$ such that $H_\alpha\, pr\, P_\gamma$. Thus we obtain the condition (iv) in Theorem 18.3 and this shows the equivalence of (a) and (d). □

As a special case of the proposition, we obtain that a pointed group H_α is projective if and only if the trivial subgroup 1 is a defect group of H_α.

The minimality of P with respect to a condition of relative projectivity corresponds to the most common definition of a defect group (or of a vertex in the case of an $\mathcal{O}G$-module). But in fact it turns out that one uses very often the characterization of defect groups and defect pointed groups by a maximality condition (the third one in both the theorem and the proposition). This remark applies for instance to the case of a primitive G-algebra A, as follows.

(18.6) COROLLARY. *Let A be a primitive G-algebra.*

(a) A local pointed group on A is maximal local if and only if it is a defect pointed group of A. In particular all maximal local pointed groups on A are conjugate under G.

(b) Any maximal subgroup P such that $\overline{A}(P) \neq 0$ is a defect group of A.

Proof. (a) Let $\alpha = \{1_A\}$ be the unique point of A^G. Then any pointed group P_γ on A is contained in G_α and the result follows from property (iii) in Theorem 18.3.

(b) This follows from the observation that for a given subgroup Q, there is a local point Q_δ if and only if $\overline{A}(Q) \neq 0$. Alternatively one can use part (c) of Proposition 18.5. □

In Section 15 we have seen that an embedding induces an injective map between pointed groups. We now mention that this map behaves well with respect to defects.

(18.7) PROPOSITION. *Let $\mathcal{F} : A \to B$ be an embedding of G-algebras. Let P_γ and H_α be pointed groups on A and let $P_{\gamma'}$ and $H_{\alpha'}$ be their images in B. Then P_γ is a defect of H_α if and only if $P_{\gamma'}$ is a defect of $H_{\alpha'}$.*

Proof. P_γ is a defect of H_α if and only if $H_\alpha \geq P_\gamma$, $H_\alpha \, pr \, P_\gamma$, and P_γ is local. By Proposition 15.1, each of these three properties is invariant under the map $\mathcal{PG}(A) \to \mathcal{PG}(B)$ induced by $\mathcal{F}$. The result follows immediately. □

There is an important characterization of defect pointed groups which uses the multiplicity algebra $S(\gamma)$ of P_γ. Recall that $S(\gamma)$ is endowed with its canonical $\overline{N}_G(P_\gamma)$-algebra structure.

(18.8) PROPOSITION. *Let A be a G-algebra, let H_α and P_γ be two pointed groups on A, and let $\pi_\gamma : A^P \to S(\gamma)$ be the canonical homomorphism. Assume that P_γ is local and that $H_\alpha \geq P_\gamma$. Then P_γ is a defect of H_α if and only if $\pi_\gamma(r_P^H(\alpha)) \subseteq (S(\gamma))_1^{\overline{N}_H(P_\gamma)}$.*

Proof. Since P_γ is local and $H_\alpha \geq P_\gamma$, it follows from the definition that P_γ is a defect of H_α if and only if $H_\alpha\, pr\, P_\gamma$, or in other words $\alpha \subseteq t_P^H(A^P \gamma A^P)$. Now consider the homomorphism

$$A^H \xrightarrow{r_P^H} A^P \xrightarrow{\pi_\gamma} S(\gamma)\,.$$

We have $\alpha \not\subseteq \mathrm{Ker}(\pi_\gamma\, r_P^H)$ because $H_\alpha \geq P_\gamma$ (see Lemma 13.3). Therefore by part (f) of Theorem 3.2 (applied to the surjective homomorphism $\pi_\gamma\, r_P^H : A^H \to \mathrm{Im}(\pi_\gamma\, r_P^H)$ and to the ideal $t_P^H(A^P \gamma A^P)$ of A^H), we have $\alpha \subseteq t_P^H(A^P \gamma A^P)$ if and only if

$$\pi_\gamma\, r_P^H(\alpha) \subseteq \pi_\gamma\, r_P^H(t_P^H(A^P \gamma A^P))\,.$$

Now we are exactly in the situation of Proposition 14.7 and we deduce that the latter inclusion holds if and only if $\pi_\gamma\, r_P^H(\alpha) \subseteq S(\gamma)_1^{\overline{N}_H(P_\gamma)}$. □

We now specialize to the case of an interior G-algebra A and give another characterization of defect pointed groups. For simplicity we only consider a pointed group G_α corresponding to the whole group G. This is no real restriction because for an arbitrary pointed group H_α, one can always work with the interior H-algebra $\mathrm{Res}_H^G(A)$ in which the whole defect theory of H_α is taking place. We fix the following notation. Let G_α be a pointed group on an interior G-algebra A, let P_γ be a pointed group on A such that $G_\alpha \geq P_\gamma$, and let $\mathcal{F}_\gamma^\alpha : A_\gamma \to \mathrm{Res}_P^G(A_\alpha)$ be the corresponding embedding (Proposition 13.6). Also, let $\mathcal{D}_P^G : A_\gamma \to \mathrm{Res}_P^G \mathrm{Ind}_P^G(A_\gamma)$ be the canonical embedding.

(18.9) PROPOSITION. *Let A be an interior G-algebra and let G_α and P_γ be pointed groups on A such that $G_\alpha \geq P_\gamma$. Then P_γ is a defect of G_α if and only if the following two conditions hold (with the notation above):*

(a) P_γ is local.

(b) There exists an embedding $\mathcal{F} : A_\alpha \to \mathrm{Ind}_P^G(A_\gamma)$ of interior G-algebras such that $\mathrm{Res}_P^G(\mathcal{F})\, \mathcal{F}_\gamma^\alpha = \mathcal{D}_P^G$.

If (b) is satisfied, then $\mathcal{F}$ is unique.

Proof. By Theorem 17.9, we have $G_\alpha\, pr\, P_\gamma$ if and only if condition (b) holds. □

Instead of considering conditions (a) and (b), one can also characterize a defect pointed group P_γ as a minimal pointed group satisfying (b), thanks to Theorem 18.3 again.

We also emphasize an important property of source algebras of interior algebras.

(18.10) PROPOSITION. *Let P_γ be a defect of a pointed group G_α on an interior G-algebra A. Then the $\mathcal{O}$-algebras A_α and A_γ are Morita equivalent. In particular if A is a primitive interior G-algebra, then A is Morita equivalent to a source algebra of A.*

Proof. Since $G_\alpha \geq P_\gamma$ and $G_\alpha \, pr \, P_\gamma$, this is immediate by Corollary 17.10. □

The proof above is based on the induction procedure (Theorem 17.9 and Corollary 17.10), which is only available for interior algebras. There is a more elementary proof which holds more generally for G-algebras A such that the induced action of G on $\mathcal{P}(A)$ is trivial (Exercise 18.3).

For the sake of completeness we specialize once again to the case of $\mathcal{O}G$-modules. Let $A = \mathrm{End}_{\mathcal{O}}(M)$ be the endomorphism algebra of an $\mathcal{O}G$-module M. The pointed groups G_α and P_γ on A correspond to direct summands M_α of M and M_γ of $\mathrm{Res}^G_P(M)$ respectively. By Example 13.4 the relation $G_\alpha \geq P_\gamma$ is equivalent to the property that M_γ is isomorphic to a direct summand of $\mathrm{Res}^G_P(M_\alpha)$. Similarly by Proposition 17.11 the relation $G_\alpha \, pr \, P_\gamma$ is equivalent to the property that M_α is isomorphic to a direct summand of $\mathrm{Ind}^G_P(M_\gamma)$. In order to characterize a defect it remains to translate the meaning of the word "local".

(18.11) PROPOSITION. *Let $A = \mathrm{End}_{\mathcal{O}}(M)$ be the endomorphism algebra of an $\mathcal{O}G$-module M. Let G_α and P_γ be pointed groups on A corresponding to direct summands M_α of M and M_γ of $\mathrm{Res}^G_P(M)$ respectively.*

(a) P_γ is local if and only if M_γ is not projective relative to a proper subgroup of P. In other words P_γ is local if and only if P is a vertex of M_γ.

(b) P_γ is a defect of G_α (that is, P is a vertex of M_α and M_γ is a source of M_α) if and only if the following three conditions are satisfied:

  (i) M_γ is not projective relative to a proper subgroup of P (that is, M_γ has vertex P),

  (ii) M_γ is isomorphic to a direct summand of $\mathrm{Res}^G_P(M_\alpha)$,

  (iii) M_α is isomorphic to a direct summand of $\mathrm{Ind}^G_P(M_\gamma)$.

Proof. (a) Let $A_\gamma = \mathrm{End}_{\mathcal{O}}(M_\gamma)$ and identify γ with the unique point of A_γ^P. By Lemmas 14.2 and 14.4, P_γ is local if and only if A_γ is not projective relative to a proper subgroup. By Higman's criterion (Corollary 17.3 and Proposition 17.7), this means that M_γ is not projective relative to a proper subgroup. The second assertion follows from Proposition 18.5.

(b) By the remarks preceding the proposition, this is immediate since P_γ is a defect of G_α if and only if P_γ is local, $G_\alpha \geq P_\gamma$ and $G_\alpha \, pr \, P_\gamma$. □

Of course, vertices and sources of $\mathcal{O}G$-modules can also be characterized by a minimality criterion, or by a maximality criterion, as in Theorem 18.3.

Exercises

(18.1) Let $\mathcal{O}$ be the trivial interior G-algebra (corresponding to the trivial group homomorphism $G \to \mathcal{O}^*$). Find a defect pointed group and a source algebra of $\mathcal{O}$. Deduce that all Sylow p-subgroups of a finite group are conjugate.

(18.2) Let A be a G-algebra and let α be a point of A^G. Via the identification of the pointed groups on A_α with pointed groups on A (Propositions 15.1 and 15.2), prove that a defect pointed group of A_α, a defect group of A_α, a source point of A_α and a source algebra of A_α are those of the corresponding pointed group G_α.

(18.3) Prove that Proposition 18.10 holds more generally for a primitive G-algebra A such that the induced action of G on $\mathcal{P}(A)$ is trivial and show that this condition is satisfied if A is an interior G-algebra. [Hint: One can assume that $A_\gamma = iAi$. Use the assumption on the action of G and the theorem on lifting idempotents to prove that ${}^x i$ is conjugate to i for every $x \in G$. Deduce that the ideal AiA is G-invariant and use the relative trace map to show that $AiA = A$.]

Notes on Section 18

The classical defect theory is due to Brauer in the case of group algebras, and to Green in the case of kG-modules and $\mathcal{O}G$-lattices. The common treatment using G-algebras was initiated by Green [1968] and extended by Puig [1981], who proved in particular the maximality criteria for the definition of defect pointed groups. All the other results of this section (18.6–18.10) are due to Puig [1981]. Exercise 18.3 is due to Linckelmann [1994].

§ 19 THE PUIG CORRESPONDENCE

This section is devoted to a fundamental tool in the theory: a bijective correspondence between pointed groups, due to L. Puig. It can be viewed as a reduction to the case of projective modules. Moreover the important concept of defect multiplicity module is introduced.

Recall that a pointed group H_α on a G-algebra A is called projective if it is projective relative to 1, that is, if $\alpha \subseteq A_1^H$. By Proposition 18.5, it is equivalent to require that the defect group of H_α is equal to 1. The Puig correspondence can be viewed as a reduction to the case of projective points on an algebra which is simple, namely a multiplicity algebra. In fact this simple algebra is the multiplicity algebra $S(\gamma)$ of a fixed local pointed group P_γ on a G-algebra A. Recall that $S(\gamma)$ has an $\overline{N}_G(P_\gamma)$-algebra structure and that for $H \geq P$, the composite map

$$A^H \xrightarrow{r_P^H} A^P \xrightarrow{\pi_\gamma} S(\gamma)$$

has an image contained in $S(\gamma)^{\overline{N}_H(P_\gamma)}$.

(19.1) THEOREM (Puig correspondence). *Let P_γ be a local pointed group on a G-algebra A and let H be a subgroup of G containing P. The algebra homomorphism $\pi_\gamma \, r_P^H : A^H \longrightarrow S(\gamma)^{\overline{N}_H(P_\gamma)}$ induces a bijection between the sets*

$$\{\, \alpha \in \mathcal{P}(A^H) \mid P_\gamma \text{ is a defect of } H_\alpha \} \quad \text{and}$$
$$\{\, \delta \in \mathcal{P}(S(\gamma)^{\overline{N}_H(P_\gamma)}) \mid \overline{N}_H(P_\gamma)_\delta \text{ is projective}\}.$$

If α corresponds to δ under this bijection, then the corresponding maximal ideals $\mathfrak{m}_\alpha$ and $\mathfrak{m}_\delta$ satisfy

$$\mathfrak{m}_\alpha = (\pi_\gamma \, r_P^H)^{-1}(\mathfrak{m}_\delta)\,.$$

Moreover $\pi_\gamma \, r_P^H$ induces an isomorphism between the multiplicity algebras

$$S(\alpha) = A^H/\mathfrak{m}_\alpha \xrightarrow{\sim} S(\delta) = S(\gamma)^{\overline{N}_H(P_\gamma)}/\mathfrak{m}_\delta\,.$$

In particular the multiplicities of α and δ are equal.

Proof. Let T be the image of $\pi_\gamma r_P^H$, a subalgebra of $S(\gamma)^{\overline{N}_H(P_\gamma)}$. By Lemma 13.3, a point $\alpha \in \mathcal{P}(A^H)$ is not in the kernel of $\pi_\gamma r_P^H$ if and only if $H_\alpha \geq P_\gamma$. Therefore by Theorem 3.2, $\pi_\gamma r_P^H$ induces a bijection

$$\{\alpha \in \mathcal{P}(A^H) \mid H_\alpha \geq P_\gamma\} \xrightarrow{\sim} \mathcal{P}(T).$$

Now by Proposition 14.7, $S(\gamma)_1^{\overline{N}_H(P_\gamma)}$ is an ideal of $S(\gamma)^{\overline{N}_H(P_\gamma)}$ contained in T (see also Remark 14.9). Moreover a pointed group $H_\alpha \geq P_\gamma$ has defect P_γ if and only if $\pi_\gamma r_P^H(\alpha) \subseteq S(\gamma)_1^{\overline{N}_H(P_\gamma)}$ (Proposition 18.8). Thus the bijection above restricts to a bijection

$$\{\alpha \in \mathcal{P}(A^H) \mid P_\gamma \text{ is a defect of } H_\alpha\} \xrightarrow{\sim} \{\delta \in \mathcal{P}(T) \mid \delta \subseteq S(\gamma)_1^{\overline{N}_H(P_\gamma)}\}.$$

If α corresponds to δ under this bijection, then the composite

$$A^H \xrightarrow{\pi_\gamma r_P^H} T \xrightarrow{\pi_\delta} T/\mathfrak{m}_\delta = S(\delta)$$

is a surjective map onto a simple algebra and the image of α is non-zero. Therefore this map induces an isomorphism $S(\alpha) \cong S(\delta)$ and it is clear that $\mathfrak{m}_\alpha = (\pi_\gamma r_P^H)^{-1}(\mathfrak{m}_\delta)$.

It remains to pass from T to $S(\gamma)^{\overline{N}_H(P_\gamma)}$. Recall that a pointed group $\overline{N}_H(P_\gamma)_\delta$ on $S(\gamma)$ is projective if and only if $\delta \subseteq S(\gamma)_1^{\overline{N}_H(P_\gamma)}$. Let us write

$$R = S(\gamma)^{\overline{N}_H(P_\gamma)} \quad \text{and} \quad I = S(\gamma)_1^{\overline{N}_H(P_\gamma)}.$$

Thus T is a subalgebra of R and I is an ideal of R contained in T. We have to prove that the inclusion $T \to R$ induces a bijection

$$\{\delta \in \mathcal{P}(T) \mid \delta \subseteq I\} \xrightarrow{\sim} \{\delta' \in \mathcal{P}(R) \mid \delta' \subseteq I\},$$

with isomorphisms between corresponding multiplicity algebras. An idempotent $i \in \delta$ remains primitive in R since any orthogonal decomposition $i = j + j'$ in R is also an orthogonal decomposition in T (because $j = ij \in I \subseteq T$ and similarly $j' \in T$). Therefore i belongs to a point δ' of R contained in I and $\delta \subseteq \delta'$. We shall see below that two primitive idempotents i and i' in I which are conjugate in R are already conjugate in T (in other words $\delta = \delta'$). This will establish that the desired bijection is simply the identity. The algebra homomorphism

$$T \longrightarrow R \xrightarrow{\pi_{\delta'}} R/\mathfrak{m}_{\delta'} = S(\delta')$$

is surjective since I maps onto $S(\delta')$ (because I, which contains δ', maps to a non-zero ideal of $S(\delta')$). Therefore we obtain $S(\delta) \cong S(\delta')$ and we have $\mathfrak{m}_\delta = \mathfrak{m}_{\delta'} \cap T$. Now if $i \in \delta'$, then $i \in I \subseteq T$ and the image of i in $S(\delta) \cong S(\delta')$ is non-zero, so that i must belong to the point δ of T. Thus $\delta = \delta'$, as was to be shown. □

The bijection in Theorem 19.1 is called the *Puig correspondence*. The projective pointed group $\overline{N}_H(P_\gamma)_\delta$ on $S(\gamma)$ corresponding to the pointed group H_α on A is called the *Puig correspondent* of H_α (with respect to P_γ). We also say that δ is the Puig correspondent of α when the context is clear. Conversely H_α is also called the *Puig correspondent* of $\overline{N}_H(P_\gamma)_\delta$.

Let $V(\gamma)$ be the multiplicity module of P_γ , which is endowed with a $k_\sharp\widehat{\overline{N}}_G(P_\gamma)$-module structure. By Example 13.5, we know that the pointed group $\overline{N}_H(P_\gamma)_\delta$ on $S(\gamma)$ corresponds to an isomorphism class of indecomposable direct summands W_δ of the $k_\sharp\widehat{\overline{N}}_H(P_\gamma)$-module $\mathrm{Res}^{\overline{N}_G(P_\gamma)}_{\overline{N}_H(P_\gamma)}(V(\gamma))$. Since the pointed group $\overline{N}_H(P_\gamma)_\delta$ is projective, the localization $S(\gamma)_\delta$ is a projective $\overline{N}_H(P_\gamma)$-algebra, and since this localization is the endomorphism algebra of W_δ (Lemma 12.4), the module W_δ is projective by Higman's criterion (Corollary 17.8). The indecomposable projective $k_\sharp\widehat{\overline{N}}_H(P_\gamma)$-module W_δ (up to isomorphism) is also called the *Puig correspondent* of the pointed group H_α . Thus the Puig correspondence can be viewed as a reduction to the case of indecomposable projective modules over a suitable twisted group algebra (for a much smaller group).

When we specialize to the case of a primitive G-algebra A , we obtain a much sharper result. The Puig correspondent of the unique point of A^G is a projective pointed group on the multiplicity algebra $S(\gamma)$, where P_γ is a defect of A , and the Puig correspondence reduces in that case to a bijection between two singletons. But in fact there is a direct proof of this which provides much more information. Recall that if $\pi_\gamma : A^P \to S(\gamma)$ is the canonical map, the image of $\pi_\gamma\, r^G_P : A^G \to S(\gamma)$ is contained in $S(\gamma)^{\overline{N}_G(P_\gamma)}$.

(19.2) THEOREM. *Let A be a primitive G-algebra, let P_γ be a defect of A, let $S(\gamma) \cong \mathrm{End}_k(V(\gamma))$ be the multiplicity algebra of P_γ, and let $\pi_\gamma : A^P \to S(\gamma)$ be the canonical map. Consider the multiplicity module $V(\gamma)$ with its module structure over the twisted group algebra $k_\sharp\widehat{\overline{N}}_G(P_\gamma)$.*

(a) The homomorphism $\pi_\gamma r^G_P : A^G \to S(\gamma)^{\overline{N}_G(P_\gamma)}$ is surjective. In particular we have $\pi_\gamma r^G_P(J(A^G)) = J(S(\gamma)^{\overline{N}_G(P_\gamma)})$.

(b) The $\overline{N}_G(P_\gamma)$-algebra $S(\gamma)$ is primitive. In other words the multiplicity module $V(\gamma)$ is an indecomposable $k_\sharp\widehat{\overline{N}}_G(P_\gamma)$-module.

(c) The $\overline{N}_G(P_\gamma)$-algebra $S(\gamma)$ is projective. In other words the multiplicity module $V(\gamma)$ is a projective $k_\sharp\widehat{\overline{N}}_G(P_\gamma)$-module.

Proof. Since A is primitive, there is a unique point $\alpha = \{1_A\}$ of A^G and A^G is a local ring. Since P is a defect group of G_α, the point α is contained in the ideal $t_P^G(A^P) = A_P^G$. It follows that $A_P^G = A^G$. By Proposition 14.7 and Remark 14.9, the image of $\pi_\gamma r_P^G$ is equal to $S(\gamma)_1^{\overline{N}_G(P_\gamma)}$ and contains $1_{S(\gamma)}$. Therefore $S(\gamma)_1^{\overline{N}_G(P_\gamma)} = S(\gamma)^{\overline{N}_G(P_\gamma)}$ and so $\pi_\gamma r_P^G$ is surjective. Since A^G is a local ring, so is its image $S(\gamma)^{\overline{N}_G(P_\gamma)}$, and we have $\pi_\gamma r_P^G(J(A^G)) = J(S(\gamma)^{\overline{N}_G(P_\gamma)})$. Thus (a) is proved.

Now $S(\gamma)^{\overline{N}_G(P_\gamma)}$ is isomorphic to a quotient of A^G, hence is a local ring too. This means that $S(\gamma)$ is a primitive $\overline{N}_G(P_\gamma)$-algebra. Thus $1_{S(\gamma)}$ is a primitive idempotent of $S(\gamma)^{\overline{N}_G(P_\gamma)}$ and this means that the corresponding $k_\sharp\widehat{\overline{N}}_G(P_\gamma)$-module $V(\gamma)$ is indecomposable (because any direct sum decomposition of $V(\gamma)$ corresponds to a decomposition of $1_{S(\gamma)}$ as an orthogonal sum of idempotents of $S(\gamma)^{\overline{N}_G(P_\gamma)}$). This completes the proof of (b). Finally we have seen that $S(\gamma)_1^{\overline{N}_G(P_\gamma)} = S(\gamma)^{\overline{N}_G(P_\gamma)}$. This means that the $\overline{N}_G(P_\gamma)$-algebra $S(\gamma)$ is projective and by Corollary 17.8, this is equivalent to the projectivity of the $k_\sharp\widehat{\overline{N}}_G(P_\gamma)$-module $V(\gamma)$. □

In the situation of Theorem 19.2 above (that is, if A is a primitive G-algebra), the projective primitive $\overline{N}_G(P_\gamma)$-algebra $S(\gamma)$ is called a *defect multiplicity algebra* of A. Also the projective indecomposable $k_\sharp\widehat{\overline{N}}_G(P_\gamma)$-module $V(\gamma)$ is called a *defect multiplicity module* of A. Both concepts depend on the choice of a defect pointed group P_γ.

The Puig correspondence is a bijection between two singletons when A is a primitive G-algebra. The general case can be reduced in some sense to this one by localization: if G_α is a pointed group on an arbitrary G-algebra A, with defect P_γ having multiplicity algebra $S(\gamma)$, then the localization A_α is a primitive G-algebra whose defect multiplicity algebra is precisely the localization $S(\gamma)_\delta$, where δ is the Puig correspondent of α under the correspondence within the algebra A (Exercise 19.1).

In the case of a primitive G-algebra, we also note that the Puig correspondence yields the following important characterization of the defect.

(19.3) COROLLARY. *Let A be a primitive G-algebra, let P_γ be a local pointed group on A, and let $V(\gamma)$ be the corresponding multiplicity module (with its $k_\sharp\widehat{\overline{N}}_G(P_\gamma)$-module structure). The following conditions are equivalent.*
(a) P is a defect group of A.
(b) P_γ is a defect pointed group of A.
(c) $V(\gamma)$ is indecomposable projective.
(d) $V(\gamma)$ is projective.
(e) $V(\gamma)$ has a non-zero projective direct summand.

Proof. (b) implies (a) by definition. Let Q_δ be a maximal local pointed group on A with $P_\gamma \leq Q_\delta$. By Corollary 18.6, Q_δ is a defect of A. Thus if (a) holds, we must have $P = Q$, hence $P_\gamma = Q_\delta$, proving (b).

By the definition of the defect multiplicity module, (b) implies (c) (see Theorem 19.2). It is clear that (c) implies (d) and that (d) implies (e).

Assume now that (e) holds, and let W be an indecomposable projective direct summand of $V(\gamma)$. Thus W corresponds to a projective point δ of $S(\gamma)^{\overline{N}_G(P_\gamma)}$. By the Puig correspondence, δ corresponds to a point α of A^G such that G_α has defect P_γ. But since A is primitive, $\{1_A\}$ is the unique point of A^G, so that $\alpha = \{1_A\}$ and P_γ is a defect of A, proving (b). □

We emphasize that the last condition in Corollary 19.3 can be restated as follows. If A is a primitive G-algebra, if Q_δ is a local pointed group which is not maximal, and if $V(\delta)$ is the corresponding multiplicity module, then no non-zero direct summand of $V(\delta)$ is projective over $k_\sharp \widehat{\overline{N}}_G(Q_\delta)$.

Exercises

(19.1) Let G_α be a pointed group on a G-algebra A, let P_γ be a defect of G_α, and let $S(\gamma)$ be the multiplicity algebra of γ. Let δ be the Puig correspondent of α. Prove that $S(\gamma)_\delta$ is isomorphic to the defect multiplicity algebra of the primitive G-algebra A_α.

(19.2) Let P_γ be a local pointed group on a G-algebra A. Let H_α and K_β be two pointed groups on A with defect P_γ, and let $\overline{N}_H(P_\gamma)_{\overline{\alpha}}$, respectively $\overline{N}_K(P_\gamma)_{\overline{\beta}}$, be their Puig correspondents (with respect to P_γ). Prove that $H_\alpha \geq K_\beta$ if and only if $\overline{N}_H(P_\gamma)_{\overline{\alpha}} \geq \overline{N}_K(P_\gamma)_{\overline{\beta}}$.

Notes on Section 19

The Puig correspondence is only implicit in Puig [1981]. The full statement and a sketch of proof appears in Puig [1988a]. The defect multiplicity module is introduced in Puig [1988a].

§ 20 THE GREEN CORRESPONDENCE

One important consequence of the Puig correspondence is another bijection called the *Green correspondence*, due to J.A. Green in the case of modules.

(20.1) THEOREM (Green correspondence). *Let A be a G-algebra, let P_γ be a local pointed group on A, and let H be a subgroup of G containing $N_G(P_\gamma)$.*

(a) If α is a point of A^G such that P_γ is a defect of G_α, then there exists a unique point β of A^H such that $G_\alpha \geq H_\beta \geq P_\gamma$.

(b) The correspondence defined by (a) is a bijection between the sets

$$\{\,\alpha \in \mathcal{P}(A^G) \mid P_\gamma \text{ is a defect of } G_\alpha\} \quad \text{and}$$
$$\{\,\beta \in \mathcal{P}(A^H) \mid P_\gamma \text{ is a defect of } H_\beta\,\}\,.$$

(c) The bijection of part (b) has the following properties. Let $\beta \in \mathcal{P}(A^H)$ be the image of $\alpha \in \mathcal{P}(A^G)$ under this bijection, and let $\mathfrak{m}_\beta$ and $\mathfrak{m}_\alpha$ be the corresponding maximal ideals of A^H and A^G respectively. Then

(i) $\mathfrak{m}_\alpha = (r^G_H)^{-1}(\mathfrak{m}_\beta) = A^G \cap \mathfrak{m}_\beta$.

(ii) r^G_H induces an isomorphism between the multiplicity algebras

$$S(\alpha) = A^G/\mathfrak{m}_\alpha \xrightarrow{\sim} S(\beta) = A^H/\mathfrak{m}_\beta\,.$$

In particular the multiplicities of α and β are equal.

(iii) $G_\alpha\, pr\, H_\beta$.

Proof. (b) Since we have $H \geq N_G(P_\gamma)$ by assumption, the subgroups $N_H(P_\gamma)$ and $N_G(P_\gamma)$ are equal and we set

$$\overline{N} = \overline{N}_H(P_\gamma) = \overline{N}_G(P_\gamma)\,.$$

Let $S(\gamma)$ be the multiplicity algebra of γ. Instead of working with points, it is here more convenient to work with the corresponding maximal ideals. Consider the following sets:

$$X = \{\,\mathfrak{m}_\alpha \in \mathrm{Max}(A^G) \mid P_\gamma \text{ is a defect of } G_\alpha\,\}\,,$$
$$Y = \{\,\mathfrak{m}_\beta \in \mathrm{Max}(A^H) \mid P_\gamma \text{ is a defect of } H_\beta\,\}\,,$$
$$Z = \{\,\mathfrak{m}_\delta \in \mathrm{Max}(S(\gamma)^{\overline{N}}) \mid \overline{N}_\delta \text{ is projective }\,\}\,.$$

By the Puig correspondence, X is in bijection with Z via $(\pi_\gamma\, r^G_P)^{-1}$ and similarly Y is in bijection with Z via $(\pi_\gamma\, r^H_P)^{-1}$. Thus it is clear that X

is in bijection with Y via $(r_H^G)^{-1}$. If $\mathfrak{m}_\alpha \in X$ corresponds to $\mathfrak{m}_\beta \in Y$, we have $(r_H^G)^{-1}(\mathfrak{m}_\beta) = \mathfrak{m}_\alpha$ and in particular $G_\alpha \geq H_\beta$ by Lemma 13.3. Thus $G_\alpha \geq H_\beta \geq P_\gamma$, and the proof of (b) will be complete if we prove that (a) holds, since the bijection just constructed then coincides with the one defined by (a).

(a) Let β be the image of α by the bijection constructed above, and let $\beta' \in \mathcal{P}(A^H)$ such that $G_\alpha \geq H_{\beta'}$ and $\beta' \neq \beta$. Since we have the two relations $G_\alpha \geq H_\beta$ and $G_\alpha \geq H_{\beta'}$, then for $i \in \alpha$ there is an orthogonal decomposition $r_H^G(i) = j + j' + e$ where $j \in \beta$, $j' \in \beta'$ and e is some idempotent in A^H. By the construction of the bijection above, we have $\pi_\gamma r_P^G(\alpha) = \delta = \pi_\gamma r_P^H(\beta)$, where $\delta \in \mathcal{P}(S(\gamma)^{\overline{N}})$ is the Puig correspondent of both α and β. Therefore $\pi_\gamma r_P^G(i)$ and $\pi_\gamma r_P^H(j)$ are primitive idempotents. Now the orthogonal decomposition

$$\pi_\gamma r_P^G(i) = \pi_\gamma r_P^H(j) + \pi_\gamma r_P^H(j') + \pi_\gamma r_P^H(e)$$

forces $\pi_\gamma r_P^H(j') = 0 = \pi_\gamma r_P^H(e)$ and the first of these equalities means that $H_{\beta'} \not\geq P_\gamma$. This proves the uniqueness of β.

(c) We have already proved (i) at the end of the proof of (b). It is also clear that r_H^G induces an isomorphism between the multiplicity algebras $S(\alpha)$ and $S(\beta)$, since they are both isomorphic to the multiplicity algebra $S(\delta)$ of the corresponding $\mathfrak{m}_\delta \in Z$, via $\pi_\gamma r_P^G$ and $\pi_\gamma r_P^H$ respectively. We are left with the proof of (iii), that is, we have to prove that $\alpha \subseteq t_H^G(A^H \beta A^H)$. By Corollary 4.11, it suffices to prove that the inclusion $\pi_\gamma r_P^G(\alpha) \subseteq \pi_\gamma r_P^G(t_H^G(A^H \beta A^H))$ holds (because $\pi_\gamma r_P^G(\alpha) \neq \{0\}$). Since P_γ is a defect of H_β, we have in particular $H_\beta \, pr \, P_\gamma$, that is, $A^H \beta A^H \subseteq t_P^H(A^P \gamma A^P)$. Therefore Corollary 14.8 applies and we obtain

$$\pi_\gamma r_P^G(t_H^G(A^H \beta A^H)) = t_{\overline{N}_H(P_\gamma)}^{\overline{N}_G(P_\gamma)} \pi_\gamma r_P^H(A^H \beta A^H) = \pi_\gamma r_P^H(A^H \beta A^H),$$

since $\overline{N}_H(P_\gamma) = \overline{N}_G(P_\gamma)$. Therefore it suffices to prove that the inclusion $\pi_\gamma r_P^G(\alpha) \subseteq \pi_\gamma r_P^H(A^H \beta A^H)$ holds. But we have $\pi_\gamma r_P^G(\alpha) = \delta$ and $\pi_\gamma r_P^H(\beta) = \delta$, where δ is the Puig correspondent of both α and β. Thus we have to prove the inclusion $\delta \subseteq (\pi_\gamma r_P^H(A^H))\, \delta \, (\pi_\gamma r_P^H(A^H))$, which is trivial since $1 \in (\pi_\gamma r_P^H(A^H))$. □

The bijection of part (b) in Theorem 20.1 is called the *Green correspondence*. If α corresponds to β under this bijection, then β is called the *Green correspondent* of α. We also say that the pointed group H_β is the Green correspondent of G_α.

(20.2) REMARK. It should be noted that the Green correpondence depends on the choice of a local pointed group P_γ , and may differ for the choice of a conjugate of P_γ . A consequence of this observation is that a pointed group G_α may have several distinct Green correspondents for a given subgroup H . Indeed for two distinct defect pointed groups P_γ and ${}^g(P_\gamma)$ of G_α , it may happen for instance that $N_G(P_\gamma) = N_G({}^g(P_\gamma))$, with P_γ and ${}^g(P_\gamma)$ not conjugate in this subgroup (Exercise 20.1). If H denotes this subgroup, then G_α has a Green correspondent H_β for the Green correspondence with respect to P_γ and another correspondent $H_{\beta'}$ for the correspondence with respect to ${}^g(P_\gamma)$. In particular we see that for a given G_α , the pointed group H_β is not uniquely determined by the two properties $G_\alpha \geq H_\beta$ and $G_\alpha \, pr \, H_\beta$. This last problem does not arise with the inverse bijection: if H_β is given, the corresponding G_α is uniquely determined by the two properties $G_\alpha \geq H_\beta$ and $G_\alpha \, pr \, H_\beta$ (Exercise 20.2).

(20.3) REMARK. In Theorem 20.1, $(r_H^G)^{-1}$ induces a bijection between maximal ideals, but we emphasize that r_H^G does not induce a map between the corresponding points. If α corresponds to β under the bijection and $i \in \alpha$, then $r_H^G(i)$ is in general not a primitive idempotent in A^H , as we have seen in the proof of (a). Only its image in $S(\gamma)^{\overline{N}}$ under $\pi_\gamma \, r_P^H$ is a primitive idempotent.

Our next result is known as the Burry–Carlson–Puig theorem.

(20.4) THEOREM. *Let P_γ be a local pointed group on a G-algebra A and let H be a subgroup containing $N_G(P_\gamma)$. Let G_α and H_β be pointed groups on A such that $G_\alpha \geq H_\beta \geq P_\gamma$. The following conditions are equivalent.*
(a) P_γ is maximal local in G_α (that is, P_γ is a defect of G_α).
(b) P_γ is maximal local in H_β (that is, P_γ is a defect of H_β).
If these conditions are satisfied, then H_β is the Green correspondent of G_α (with respect to P_γ).

Proof. If P_γ is maximal local such that $G_\alpha \geq P_\gamma$, it is clear that P_γ is also maximal local such that $H_\beta \geq P_\gamma$. Assume conversely that P_γ is a defect of H_β . Since $H \geq N_G(P_\gamma)$, we have $N_H(P_\gamma) = N_G(P_\gamma)$ and we set $\overline{N} = \overline{N}_H(P_\gamma) = \overline{N}_G(P_\gamma)$. Let $\overline{N}_\delta$ be the Puig correspondent of H_β (with respect to P_γ). Then $\overline{N}_\delta$ is the Puig correspondent of a unique pointed group $G_{\alpha'}$ (with defect P_γ), and H_β is the Green correspondent of $G_{\alpha'}$. By Theorem 20.1, the corresponding maximal ideals satisfy $\mathfrak{m}_{\alpha'} = (r_H^G)^{-1}(\mathfrak{m}_\beta)$. But since $G_\alpha \geq H_\beta$ by assumption, we also have $\mathfrak{m}_\alpha \supseteq (r_H^G)^{-1}(\mathfrak{m}_\beta)$. By maximality of $\mathfrak{m}_{\alpha'}$, we obtain $\mathfrak{m}_{\alpha'} = \mathfrak{m}_\alpha$, and so $\alpha = \alpha'$. This completes the proof because we know that P_γ is a defect of $G_{\alpha'}$. □

An important application of this result is the following. Recall that if Q is a proper subgroup of a Sylow p-subgroup P of G, then there exists a p-subgroup R normalizing Q such that $Q < R \leq P$ (in fact we can take $R = N_P(Q)$). We now prove that the same result holds for local pointed groups.

(20.5) COROLLARY. *Let A be a G-algebra and let Q_δ and P_γ be local pointed groups on A such that $Q_\delta < P_\gamma$. Then there exists a local pointed group R_ε such that $Q_\delta < R_\varepsilon \leq P_\gamma$ and $R \leq N_P(Q_\delta)$. In particular $Q < N_P(Q_\delta)$.*

Proof. Let $H = N_P(Q_\delta)$. There exists a point $\alpha \in \mathcal{P}(A^H)$ such that $Q_\delta \leq H_\alpha \leq P_\gamma$ (Exercise 13.5). Since Q_δ is not maximal local in P_γ (because P_γ is local), Q_δ is not maximal local in H_α by Theorem 20.4. Therefore there exists a local pointed group R_ε such that $Q_\delta < R_\varepsilon \leq H_\alpha$. In particular $R_\varepsilon \leq P_\gamma$ and $Q < H$, as was to be shown. □

Our next application of Theorem 20.4 has to do with the poset of pointed groups. Recall that a poset is a partially ordered set. For a G-algebra A, the set $\mathcal{PG}(A)$ of all pointed groups on A is a poset for the partial order $\geq$. Moreover there is an order-preserving action of the group G on this poset by conjugation (Exercise 13.4).

(20.6) COROLLARY. *Let A be a G-algebra, let P_γ be a local pointed group on A, let $N = N_G(P_\gamma)$, and let N_ε be a pointed group with defect P_γ. Let $\mathcal{X}(N_\varepsilon)$ be the poset of all pointed groups H_α on A such that $H_\alpha \geq N_\varepsilon$ and let $\overline{\mathcal{X}}(N_\varepsilon)$ be the G-conjugacy closure of $\mathcal{X}(N_\varepsilon)$ (that is, $H_\alpha \in \overline{\mathcal{X}}(N_\varepsilon)$ if and only if there exists $g \in G$ such that ${}^gH_\alpha \in \mathcal{X}(N_\varepsilon)$).*

(a) For every $H_\alpha \in \mathcal{X}(N_\varepsilon)$, P_γ is a defect of H_α.

(b) For every subgroup $H \geq N$, there exists a unique point $\alpha \in \mathcal{P}(A^H)$ such that $H_\alpha \geq N_\varepsilon$. In other words the poset $\mathcal{X}(N_\varepsilon)$ is isomorphic to the poset of subgroups containing N.

(c) There is no fusion in $\overline{\mathcal{X}}(N_\varepsilon)$ in the following sense: whenever we have $H_\alpha, K_\beta \in \overline{\mathcal{X}}(N_\varepsilon)$, $H_\alpha \geq K_\beta$, and $H_\alpha \geq {}^g(K_\beta)$ for some $g \in G$, then $g \in H$. In particular $N_G(H_\alpha) = H$ for every $H_\alpha \in \overline{\mathcal{X}}(N_\varepsilon)$.

Proof. (a) This is an immediate consequence of Theorem 20.4, because $H_\alpha \geq N_\varepsilon \geq P_\gamma$ and P_γ is a defect of N_ε.

(b) The pointed group N_ε has a Green correspondent H_α. By Theorem 20.4 again, any pointed group $H_{\alpha'}$ such that $H_{\alpha'} \geq N_\varepsilon$ must be the Green correspondent of N_ε. Therefore $\alpha = \alpha'$.

(c) After conjugating the whole situation, we may assume that K_β belongs to $\mathcal{X}(N_\varepsilon)$, so that K_β has defect P_γ by (a). Thus ${}^g(K_\beta)$ has defect ${}^g(P_\gamma)$. Then by (a) again, $H_\alpha \geq K_\beta$ has defect P_γ and $H_\alpha \geq {}^g(K_\beta)$

has defect ${}^g(P_\gamma)$. Since all defect pointed groups are conjugate, there exists $h \in H$ such that ${}^g(P_\gamma) = {}^h(P_\gamma)$. Therefore we have $h^{-1}g \in N_G(P_\gamma) = N$ and since $N \leq K \leq H$, we obtain $g \in H$, as required. The special case follows by taking $H_\alpha = K_\beta$. $\square$

Assume now that the G-algebra A is interior and primitive. Let $\alpha = \{1_A\}$ be the unique point of A^G , let P_γ be a defect of G_α , let $H \geq N_G(P_\gamma)$, and let H_β be the Green correspondent of G_α . By Theorem 20.1, we have both relations $G_\alpha \geq H_\beta$ and $G_\alpha \, pr \, H_\beta$. Therefore by Theorem 17.9, there exists an embedding $\mathcal{F} : A \to \mathrm{Ind}_H^G(A_\beta)$ such that $\mathrm{Res}_H^G(\mathcal{F})\mathcal{F}_\beta = \mathcal{D}_H^G$. Here $\mathcal{F}_\beta : A_\beta \to \mathrm{Res}_H^G(A)$ is an embedding associated with H_β , and $\mathcal{D}_H^G : A_\beta \to \mathrm{Res}_H^G \mathrm{Ind}_H^G(A_\beta)$ is the canonical embedding associated with the interior H-algebra A_β . We let α' , β' and γ' be the images of α , β and γ in $\mathrm{Ind}_H^G(A_\beta)$ under the embedding $\mathcal{F}$. We know that α and β have isomorphic multiplicity algebras (Theorem 20.1). In general multiplicities become larger via embeddings (or more precisely there is an embedding between the corresponding multiplicity algebras, see Proposition 15.3). But we now show that the multiplicities of α' and β' do not grow.

(20.7) PROPOSITION. *Let A be a primitive interior G-algebra, let $\alpha = \{1_A\}$ be the unique point of A^G , let P_γ be a defect of G_α , let $H \geq N_G(P_\gamma)$, and let H_β be the Green correspondent of G_α . Let $\mathcal{F} : A \to \mathrm{Ind}_H^G(A_\beta)$ be the embedding defined above and let α' and β' denote the images of α and β under $\mathcal{F}$. Then α' and β' have multiplicity one.*

Proof. Let γ' be the image of γ under $\mathcal{F}$. Since embeddings preserve containment and defect (Propositions 15.1 and 18.7), we have $G_{\alpha'} \geq H_{\beta'} \geq P_{\gamma'}$ and $P_{\gamma'}$ is a defect of $G_{\alpha'}$. Therefore $H_{\beta'}$ is the Green correspondent of $G_{\alpha'}$ and consequently α' and β' have the same multiplicity (Theorem 20.1). Thus it suffices to show that β' has multiplicity one.

Let $B = A_\beta$ and write $\mathcal{D} = \mathcal{D}_H^G : B \to \mathrm{Res}_H^G \mathrm{Ind}_H^G(B)$. Since $P_\gamma \leq H_\beta$, we can view γ as a point of B^P , that is, we identify the point γ of A^P with its preimage under the embedding $\mathcal{F}_\beta : A_\beta \to \mathrm{Res}_H^G(A)$. Since $\mathrm{Res}_H^G(\mathcal{F})\mathcal{F}_\beta = \mathcal{D}$, we have $\mathcal{D}(\gamma) = \gamma'$. By Proposition 15.3, we know that $\mathcal{D}$ induces an embedding of $\overline{N}$-algebras $\overline{\mathcal{D}}(\gamma) : S(\gamma) \to S(\gamma')$, where $N = N_G(P_\gamma) = N_H(P_\gamma)$ and $\overline{N} = N/P$. We are going to show that $\overline{\mathcal{D}}(\gamma)$ is an exo-isomorphism.

Assuming this, it follows that $S(\gamma')$ is a primitive and projective $\overline{N}$-algebra. Indeed, since B is a primitive H-algebra with defect P_γ , the $\overline{N}$-algebra $S(\gamma)$ is primitive and projective by Theorem 19.2. Thus $S(\gamma')^{\overline{N}}$ has a unique projective point δ' with multiplicity one. The Puig correspondence reduces to a bijection between the singleton δ' and a point of $\mathrm{Ind}_H^G(B)^H$ which can only be β', since $H_{\beta'}$ has defect $P_{\gamma'}$. Since the Puig correspondence preserves multiplicities, β' has multiplicity one, as required.

Now we prove that $\overline{\mathcal{D}}(\gamma)$ is an exo-isomorphism. Let $d \in \mathcal{D}$, where $d = d_H^G : B \to \mathrm{Res}_H^G \mathrm{Ind}_H^G(B)$ is defined by $d(b) = 1 \otimes b \otimes 1$. Then d induces $\overline{d} \in \overline{\mathcal{D}}(\gamma)$ and there is a commutative diagram

$$\begin{array}{ccc} B^P & \xrightarrow{\ d\ } & \mathrm{Ind}_H^G(B)^P \\ \big\downarrow{\scriptstyle \pi_\gamma} & & \big\downarrow{\scriptstyle \pi_{\gamma'}} \\ S(\gamma) & \xrightarrow{\ \overline{d}\ } & S(\gamma') \end{array}$$

(see Proposition 15.3). Since $\overline{d}$ belongs to an embedding, it suffices to show that $\overline{d}(1_{S(\gamma)}) = 1_{S(\gamma')}$ to deduce that $\overline{d}$ is an isomorphism. By construction of induced algebras, we have $1_{\mathrm{Ind}_H^G(B)} = t_H^G(1 \otimes 1_B \otimes 1)$. Moreover since $B = A_\beta$ is a primitive H-algebra with defect P_γ, there exists $a \in B^P \gamma B^P$ such that $t_P^H(a) = 1_B$. Therefore, by Proposition 14.7, we have

$$\begin{aligned} \overline{d}(1_{S(\gamma)}) &= \overline{d}\,\pi_\gamma(1_B) = \pi_{\gamma'}\, d(1_B) = \pi_{\gamma'}\, r_P^H\, t_P^H(1 \otimes a \otimes 1) \\ &= t_1^{\overline{N}}\, \pi_{\gamma'}(1 \otimes a \otimes 1) = \pi_{\gamma'}\, r_P^G\, t_P^G(1 \otimes a \otimes 1) = \pi_{\gamma'}\, r_P^G(1_{\mathrm{Ind}_H^G(B)}) \\ &= 1_{S(\gamma')}\,, \end{aligned}$$

as required. □

Once again we specialize to the case of $\mathcal{O}G$-modules and we give a second form of the Green correspondence, which will be an overall correspondence between modules rather than a correspondence within a fixed G-algebra. Let L be an indecomposable $\mathcal{O}G$-module with vertex P and source X. We know that L is isomorphic to a direct summand of $\mathrm{Ind}_P^G(X)$ (Proposition 17.11). Let $H \geq N_G(P,X)$, where $N_G(P,X)$ denotes the inertial subgroup of the module X. Recall that $N_G(P,X) = N_G(P_\gamma)$ where P_γ is the pointed group on $\mathrm{End}_{\mathcal{O}}(\mathrm{Ind}_P^G(X))$ corresponding to the $\mathcal{O}P$-direct summand X. An indecomposable $\mathcal{O}H$-module M with vertex P and source X is isomorphic to a direct summand of $\mathrm{Ind}_P^H(X)$, hence also to a direct summand of $\mathrm{Res}_H^G \mathrm{Ind}_P^G(X)$, since $\mathrm{Ind}_P^H(X)$ is isomorphic to a direct summand of $\mathrm{Res}_H^G \mathrm{Ind}_H^G(\mathrm{Ind}_P^H(X)) = \mathrm{Res}_H^G \mathrm{Ind}_P^G(X)$. Thus for both G and H, the indecomposable modules with vertex P and source X correspond to pointed groups on $A = \mathrm{End}_{\mathcal{O}}(\mathrm{Ind}_P^G(X))$ with defect P_γ. Applying Theorem 20.1 to the G-algebra A, we obtain the following result, which is the first form of the Green correspondence for modules.

(20.8) PROPOSITION. *Let P be a p-subgroup of G, let X be an indecomposable $\mathcal{O}P$-module with vertex P, and let $H \geq N_G(P,X)$.*

(a) *If L is an indecomposable $\mathcal{O}G$-module with vertex P and source X, then $\mathrm{Res}^G_H(L)$ has a unique isomorphism class of direct summands M with vertex P and source X.*

(b) *The correspondence in (a) induces a bijection between the set of isomorphism classes of indecomposable $\mathcal{O}G$-modules L with vertex P and source X, and the set of isomorphism classes of indecomposable $\mathcal{O}H$-modules M with vertex P and source X.*

(c) *If M corresponds to L under this bijection, then M is isomorphic to a direct summand of $\mathrm{Res}^G_H(L)$ and L is isomorphic to a direct summand of $\mathrm{Ind}^G_H(M)$.*

Proof. The result follows from Theorem 20.1 applied to the G-algebra $A = \mathrm{End}_{\mathcal{O}}(\mathrm{Ind}^G_P(X))$. If L corresponds to a point α of A^G and M corresponds to a point β of A^H, then $G_\alpha \geq H_\beta$ and $G_\alpha \, pr \, H_\beta$. These properties mean respectively that M is isomorphic to a direct summand of $\mathrm{Res}^G_H(L)$ (Example 13.4) and L is isomorphic to a direct summand of $\mathrm{Ind}^G_H(M)$ (Proposition 17.11). □

The bijection of part (b) in Proposition 20.8 is called the *Green correspondence* (for modules). The indecomposable $\mathcal{O}H$-module M (up to isomorphism) corresponding to the indecomposable $\mathcal{O}G$-module L is called the *Green correspondent* of L. More properties of the Green correspondence for modules are given in Exercise 20.4. If we keep the p-subgroup P fixed but allow the source X to vary, we can choose for H any subgroup containing $N_G(P)$ and we obtain the second form of the Green correspondence for modules.

(20.9) COROLLARY. *Let P be a p-subgroup of G and let H be a subgroup containing $N_G(P)$. The Green correspondence induces a bijection between the set of isomorphism classes of indecomposable $\mathcal{O}G$-modules L with vertex P, and the set of isomorphism classes of indecomposable $\mathcal{O}H$-modules M with vertex P. Moreover corresponding modules have a source in common.*

Proof. Since a source is only defined up to $N_G(P)$-conjugation (for a fixed P), we have to choose one module X in each $N_G(P)$-conjugacy class of indecomposable $\mathcal{O}P$-modules with vertex P. Then the disjoint union of the bijections of the last proposition (one for each X) yields the result. □

(20.10) REMARK. There is also a Green correspondence between isomorphism classes of primitive interior G-algebras with defect group P and source algebra B, and isomorphism classes of primitive interior H-algebras with defect group P and source algebra B, provided $H \geq N_G(P,B)$ where $N_G(P,B)$ is the inertial subgroup of the P-algebra B. The proof is similar to that of Proposition 20.8, but more elaborate, because distinct points of $\mathrm{Ind}_P^G(B)^G$ may have isomorphic localizations, so that a primitive interior G-algebra with defect group P and source algebra B may correspond to several points of $\mathrm{Ind}_P^G(B)^G$. However, one can obtain a correspondence which is induced by the Green correspondence between points described in Theorem 20.1.

Exercises

(20.1) Construct explicitly an example of a pointed group G_α having two distinct Green correspondents H_β and $H_{\beta'}$, as explained in Remark 20.2. [Hint: Take G to be the alternating group on 4 letters; the three conjugate subgroups P of order 2 have the same normalizer.]

(20.2) Let H_β be a pointed group on a G-algebra A and assume that $H \geq N_G(P_\gamma)$ for some defect pointed group P_γ of H_β. Prove that there exists a unique pointed group G_α satisfying the two properties $G_\alpha \geq H_\beta$ and $G_\alpha \, pr \, H_\beta$. Moreover H_β is the Green correspondent of G_α.

(20.3) Let N be the normalizer of a Sylow p-subgroup of G. Show that there is no fusion in the poset of all subgroups H containing a conjugate of N, and that in particular $N_G(H) = H$ for any such subgroup H.

(20.4) Let L be an indecomposable $\mathcal{O}G$-module with vertex P and source X. Let H be a subgroup containing $N_G(P,X)$ and let the indecomposable $\mathcal{O}H$-module M be the Green correspondent of L.

(a) Prove that in a decomposition of $\mathrm{Res}_H^G(L)$ into indecomposable summands, there is a unique summand isomorphic to M.

(b) Prove that in a decomposition of $\mathrm{Ind}_H^G(M)$ into indecomposable summands, there is a unique summand isomorphic to L. [Hint: Use Proposition 20.7.]

(c) Prove that any indecomposable direct summand of $\mathrm{Ind}_H^G(M)$ not isomorphic to L has vertex strictly contained in P.

(d) Use Exercise 20.1 to show that the property of $\mathrm{Res}_H^G(L)$ analogous to (c) may fail to hold. Prove however that a vertex of an indecomposable direct summand of $\mathrm{Res}_H^G(L)$ not isomorphic to M cannot contain P.

(20.5) Let L be an indecomposable $\mathcal{O}G$-module, let P be a p-subgroup of G, let X be an indecomposable direct summand of $\mathrm{Res}^G_P(L)$ which is its own source, let $H \geq N_G(P,X)$, and let M be an indecomposable direct summand of $\mathrm{Res}^G_H(L)$. Prove that L has vertex P and source X if and only if M has vertex P and source X. [Hint: This is the Burry–Carlson–Puig theorem in the case of modules.]

Notes on Section 20

The Green correspondence is due to Green [1964] for $\mathcal{O}G$-modules. The version with points is not explicitly stated in Puig's work. The version of the correspondence for primitive interior algebras (mentioned in Remark 20.10) appears in Thévenaz [1993]. The Burry–Carlson–Puig theorem 20.4 was proved by Puig [1981], and independently by Burry and Carlson [1982] in the case of $\mathcal{O}G$-modules.

CHAPTER 4

Further results on G-algebras

In this chapter we prove various results on G-algebras. Some of them will be useful in applications. The first section is concerned with some specific results about p-groups. Then we prove a theorem on lifting idempotents which is used in the case of p-groups to establish some results about primitive idempotent decompositions and induction of primitive interior algebras. Finally we introduce the notion of covering exomorphism and its local characterizations. We continue with our assumption that G is a finite group and that $\mathcal{O}$ is a commutative complete local noetherian ring with an algebraically closed residue field k of characteristic p.

§ 21 BASIC RESULTS FOR p-GROUPS

In this section we prove two results connected with a p-group P. Of course p denotes as before the characteristic of the field $k = \mathcal{O}/\mathfrak{p}$ (which need not be algebraically closed throughout this section). First we prove that the group algebra $\mathcal{O}P$ is a local ring and that the trivial module k is the only simple $\mathcal{O}P$-module. The second result asserts that any twisted group algebra for a p-group is isomorphic in a canonical way to the ordinary group algebra (provided k is perfect).

Let $\mathcal{O}G$ be the group algebra of G. The *augmentation homomorphism* is the map $\varepsilon : \mathcal{O}G \to \mathcal{O}$ defined on the basis of $\mathcal{O}G$ by $\varepsilon(g) = 1$ for every $g \in G$. It is a homomorphism of $\mathcal{O}$-algebras. In particular $\mathcal{O}$ is endowed via ε with an $\mathcal{O}G$-module structure, called the *trivial* $\mathcal{O}G$-module. The *augmentation ideal* of $\mathcal{O}G$ is the kernel of ε and is written $I(\mathcal{O}G)$. It is freely generated as an $\mathcal{O}$-module by the elements $g-1$ for $g \in G - \{1\}$. The composition of ε with the map $\pi : \mathcal{O} \to \mathcal{O}/\mathfrak{p} = k$ is a ring homomorphism with kernel $\mathfrak{m} = I(\mathcal{O}G) + \mathfrak{p} \cdot \mathcal{O}G$, which is a maximal ideal of $\mathcal{O}G$. These definitions also apply if $\mathcal{O}$ is replaced by k.

(21.1) PROPOSITION. *Let P be a p-group.*
(a) The trivial kP-module k is the only simple kP-module up to isomorphism.
(b) The augmentation ideal $I(kP)$ of kP is the Jacobson radical of kP. It is the unique maximal ideal of kP and it is nilpotent.
(c) The ideal $\mathfrak{m} = I(\mathcal{O}P) + \mathfrak{p} \cdot \mathcal{O}P$ is the Jacobson radical of $\mathcal{O}P$. It is the unique maximal ideal of $\mathcal{O}P$ and it is nilpotent modulo $\mathfrak{p} \cdot \mathcal{O}P$.
(d) The only idempotents of $\mathcal{O}P$ are 0 and 1.
(e) Every (finitely generated) projective $\mathcal{O}P$-module is free.

Proof. (a) Since k has characteristic p, it contains the prime field $\mathbb{F}_p$ with p elements. Let V be a simple kP-module, let $v \in V$ with $v \neq 0$ and let W be the $\mathbb{F}_p$-vector subspace of V generated by all the elements $g \cdot v$ for $g \in P$. Then W is finite and is invariant under the action of P by construction. We decompose W as a disjoint union of orbits. The orbit of an element w reduces to $\{w\}$ if and only if w is fixed under P. Therefore the union of all the orbits with one element is the subspace W^P of P-fixed elements in W. If the orbit of w is non-trivial, the stabilizer Q of w is a proper subgroup of P and the cardinality of the orbit is $|P : Q|$, which is a power of p since P is a p-group. Therefore W is the disjoint union of W^P and of orbits of cardinality divisible by p. Since $|W|$ is a power of p (because W is a vector space over $\mathbb{F}_p$), it follows that $|W^P|$ is divisible by p. Now W^P contains 0, hence must contain at least one other element w . Thus we have proved that the kP-module V always contains a non-zero element w fixed under P . The one-dimensional k-subspace generated by w is a kP-submodule of V , hence equal to the whole of V by simplicity of V . Therefore V is one-dimensional and is isomorphic to the trivial kP-module since P acts trivially on it.

(b) We apply Theorem 1.13. Since, by (a), $\mathrm{Irr}(kP)$ has a single element and since $\mathrm{Max}(kP)$ is in bijection with $\mathrm{Irr}(kP)$, the maximal ideal $I(kP)$ is the unique maximal ideal of kP . Therefore $I(kP)$ is equal to the Jacobson radical $J(kP)$, which is nilpotent (Theorem 1.13).

(c) By Theorem 2.7, $\mathfrak{p}{\cdot}\mathcal{O}P \subseteq J(\mathcal{O}P)$. Since $\mathcal{O}P/\mathfrak{p}{\cdot}\mathcal{O}P \cong kP$ and since the image of $I(\mathcal{O}P)$ in kP is $I(kP)$, the inverse image in $\mathcal{O}P$ of $J(kP) = I(kP)$ is the ideal $\mathfrak{m}$ and is the Jacobson radical of $\mathcal{O}P$. Also by Theorem 2.7, we have $J(\mathcal{O}P)^n \subseteq \mathfrak{p}{\cdot}\mathcal{O}P$ for some integer n .

(d) By (c), the semi-simple quotient of $\mathcal{O}P$ is $\mathcal{O}P/\mathfrak{m} \cong k$, whose only idempotents are 0 and 1. Since one can lift idempotents (Theorem 3.1), the same holds for $\mathcal{O}P$.

(e) By Proposition 5.1, any projective indecomposable $\mathcal{O}P$-module is isomorphic to $\mathcal{O}Pe$ where e is a primitive idempotent of $\mathcal{O}P$. But $e = 1$ by (d) and it follows that any projective $\mathcal{O}P$-module is isomorphic to a direct sum of copies of $\mathcal{O}P$, hence free. □

(21.2) COROLLARY. *Let P be a normal p-subgroup of G and let $\tau : \mathcal{O}G \to \mathcal{O}(G/P)$ be the quotient map.*

(a) We have $\mathrm{Ker}(\tau) \subseteq J(\mathcal{O}G)$.

(b) The subgroup P acts trivially on every simple $\mathcal{O}G$-module, so that $\mathrm{Irr}(\mathcal{O}G) = \mathrm{Irr}(kG)$ *can be identified with* $\mathrm{Irr}(\mathcal{O}(G/P)) = \mathrm{Irr}(k(G/P))$.

Proof. (a) Since $\mathfrak{p} \cdot \mathcal{O}G \subseteq J(\mathcal{O}G)$, it suffices to work over k . The ideal $\mathrm{Ker}(\tau)$ is generated over k by the elements $(u-1)g$ where $g \in G$ and $u \in P$. In other words, as an ideal, it is generated by $I(kP)$. Moreover for $g, g' \in G$ and $u, u' \in P$, we have

$$(u-1)g(u'-1)g' = (u-1)({}^{g}u'-1)gg' \, .$$

It follows by induction that $\mathrm{Ker}(\tau)^n$ is generated as an ideal by $I(kP)^n$. Since $I(kP)$ is nilpotent by Proposition 21.1, so is $\mathrm{Ker}(\tau)$ and therefore $\mathrm{Ker}(\tau) \subseteq J(kG)$ (Theorem 1.13).

(b) Since $u-1 \in \mathrm{Ker}(\tau)$ for $u \in P$, it belongs to $J(\mathcal{O}G)$ by (a) and hence annihilates every simple $\mathcal{O}G$-module. In other words u acts as the identity. □

Now we prove that the only twisted group algebra for a p-group is the ordinary group algebra. The proof follows essentially the same line as that of Proposition 10.5. But as the present result also involves a uniqueness statement, we repeat the argument for simplicity. The result holds for a *perfect* field k of characteristic p (this means that any element of k is a p-th power), thus in particular if k is finite or algebraically closed.

(21.3) PROPOSITION. *Let P be a p-group and let k be a perfect field of characteristic p. Then any central extension $1 \to k^* \to \widehat{P} \to P \to 1$ splits in a unique way. Therefore the corresponding twisted group algebra $k_\sharp \widehat{P}$ is isomorphic to kP.*

Proof. Let $q = |P|$, a power of p. Since the characteristic of k is p, the only element $\lambda \in k^*$ such that $\lambda^q = 1$ is $\lambda = 1$. Therefore the map $\lambda \mapsto \lambda^q$ is an injective group homomorphism $\phi : k^* \to k^*$ and it is also surjective because k is perfect. We use some standard facts from the cohomology theory of groups, which are recalled in Proposition 1.18. Consider the cohomology group $H^n(P, k^*)$, where $n \geq 1$ and k^* is viewed as a trivial P-module. The automorphism ϕ induces an automorphism of $H^n(P, k^*)$, which is multiplication by the group order. Since the order of the group annihilates $H^n(P, k^*)$, we deduce that $H^n(P, k^*) = 0$. Now $H^2(P, k^*)$ classifies the central extensions with kernel k^* and quotient group P (the extensions are central because the action of P on k^* is trivial). Thus $H^2(P, k^*) = 0$ means that any such extension splits. Moreover $H^1(P, k^*) = 0$ means that there is a single conjugacy class of splittings. But conjugacy by the central subgroup k^* is trivial, so that the conjugacy class consists of a single splitting. □

We leave to the reader the task of stating the exact condition on the isomorphism $k_\sharp \widehat{P} \cong kP$ to guarantee its uniqueness.

(21.4) COROLLARY. *Let k be a perfect field of characteristic p, let P be a p-group, and let $S = \mathrm{End}_k(M)$ be a simple P-algebra (where M is a k-vector space). Then there is a unique interior P-algebra structure on S inducing the given P-algebra structure. In other words M becomes a kP-module in a unique way.*

Proof. We know from Example 10.8 that the P-algebra structure on S lifts uniquely to a group homomorphism $\widehat{P} \to S^*$. The unique splitting of the central extension of the previous proposition yields a unique group homomorphism $P \to S^*$. □

If one works over $\mathcal{O}$ rather than k, the situation is slightly more complicated but can be completely described when the dimension is prime to p. As we need roots of unity, we return for simplicity to our usual assumption that k is algebraically closed.

(21.5) PROPOSITION. *Let P be a p-group and let $S = \mathrm{End}_{\mathcal{O}}(M)$ be an $\mathcal{O}$-simple P-algebra (where M is a free $\mathcal{O}$-module). Assume that the dimension of M is prime to p.*

(a) *There exists an interior P-algebra structure on S inducing the given P-algebra structure. Explicitly there exists a group homomorphism $\phi : P \to S^*$, such that ${}^u s = \phi(u)s\phi(u)^{-1}$ for all $u \in P$ and $s \in S$. In other words M becomes an $\mathcal{O}P$-lattice via ϕ.*

(b) *If $\phi' : P \to S^*$ is another group homomorphism as in (a), then there exists a group homomorphism $\lambda : P \to \mathcal{O}^*$ (that is, a linear character) such that $\phi'(u) = \lambda(u)\phi(u)$ for all $u \in P$.*

(c) *There exists a unique group homomorphism ϕ as in (a) with the additional property that $\det(\phi(u)) = 1$ for all $u \in P$.*

Proof. It is clear that (a) is a consequence of the more precise statement (c). For the proof of (b), we note that since $\phi(u)$ and $\phi'(u)$ induce the same action by conjugation on S, there exists a central element $\lambda(u) \in \mathcal{O}^*$ such that $\phi'(u) = \lambda(u)\phi(u)$. It is elementary to check that λ is a group homomorphism.

It remains to prove (c). Let $GL(M) = S^*$, let $PGL(M) = S^*/\mathcal{O}^*$, let $SL(M) = \mathrm{Ker}\big(\det : GL(M) \to \mathcal{O}^*\big)$, and let $PSL(M)$ be the image of $SL(M)$ in $PGL(M)$. We first prove that $PSL(M) = PGL(M)$. Let $\overline{a} \in PGL(M)$, let $a \in GL(M)$ be an arbitrary lift of $\overline{a}$ and let $\lambda = \det(a) \in \mathcal{O}^*$. Since $n = \dim(M)$ is prime to p, λ has an n-th root $\mu \in \mathcal{O}^*$ by Corollary 4.8. Then $\det(\mu^{-1}a) = \mu^{-n}\det(a) = 1$ and $\overline{a}$ is still the image of $\mu^{-1}a$ in $PGL(M)$. Therefore $\overline{a} \in PSL(M)$.

By the Skolem–Noether theorem, the action of $u \in P$ on S is equal to some inner automorphism $\mathrm{Inn}(\rho(u))$ and since $\rho(u)$ is only defined up to a central element, this defines a group homomorphism

$$\rho : P \to PGL(M) = PSL(M).$$

Let $K = \mathrm{Ker}(SL(M) \to PSL(M))$. Then K consists of scalars λ such that $\lambda^n = 1$, hence is a (cyclic) group of order n (because $t^n - 1$ has n distinct roots in $\mathcal{O}^*$ by Corollary 4.8). Consider now the pull-back X of the two maps $\rho : P \to PSL(M)$ and $SL(M) \to PSL(M)$. We obtain a diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K & \longrightarrow & X & \xrightarrow{\pi} & P & \longrightarrow & 1 \\ & & \big\downarrow{\scriptstyle id} & & \big\downarrow & & \big\downarrow{\scriptstyle \rho} & & \\ 1 & \longrightarrow & K & \longrightarrow & SL(M) & \longrightarrow & PSL(M) & \longrightarrow & 1 \end{array}$$

in which both rows are exact. By definition of a pull-back, ρ lifts to a homomorphism $\phi : P \to SL(M)$ if and only if π has a section $\sigma : P \to X$. Moreover ϕ is unique if and only if σ is unique. Thus we are left with the proof of the existence and uniqueness of σ. Since K has order prime to p, multiplication by $|P|$ is an automorphism of $H^*(P, K)$ and is also zero because the order of a group annihilates its cohomology. Therefore $H^*(P, K) = 0$ and the argument used at the end of the proof of Proposition 21.3 shows the existence and uniqueness of the required section σ. □

Corollary 21.2 can be generalized to the case of a twisted group algebra over k.

(21.6) PROPOSITION. *Let $k_\sharp \widehat{G}$ be a twisted group algebra of G and suppose that G has a normal p-subgroup P.*

(a) There is a canonical surjection $\tau : k_\sharp \widehat{G} \to k_\sharp(\widehat{G/P})$ onto a twisted group algebra of the quotient group G/P.

(b) We have $\mathrm{Ker}(\tau) \subseteq J(k_\sharp \widehat{G})$. In particular $\mathrm{Ker}(\tau)$ annihilates every simple $k_\sharp \widehat{G}$-module M, so that M can be viewed as a simple $k_\sharp(\widehat{G/P})$-module.

Proof. (a) On restriction to P, we have $k_\sharp \widehat{P} \cong kP$ by Proposition 21.3, and kP has a canonical basis $\{ u \mid u \in P \}$. Choose a transversal $[G/P]$ and, for each $g \in [G/P]$, let $\widehat{g} \in \widehat{G}$ be an element mapping onto g. Then the set $\{ u\widehat{g} \mid u \in P, g \in [G/P] \}$ is a basis of $k_\sharp \widehat{G}$. The ideal I generated by $I(kP)$ is generated over k by the elements $(u-1)\widehat{g}$. Thus the images of the elements $\widehat{g}$ for $g \in [G/P]$ form a k-basis of $(k_\sharp \widehat{G})/I$ and it is clear that $(k_\sharp \widehat{G})/I$ is a twisted group algebra of G/P. Since the isomorphism $k_\sharp \widehat{P} \cong kP$ is unique, the ideal I is canonically associated with the data, and therefore we obtain a canonical surjection $\tau : k_\sharp \widehat{G} \to (k_\sharp \widehat{G})/I \cong k_\sharp(\widehat{G/P})$.

(b) As in the proof of part (a) of Corollary 21.2, we have

$$(u-1)\widehat{g}(u'-1)\widehat{g}' = (u-1)({}^{g}u'-1)\widehat{g}\widehat{g}',$$

and it follows by induction that I^n is generated as an ideal by $I(kP)^n$. Since $I(kP)$ is nilpotent by Proposition 21.1, so is I. Therefore we have $I \subseteq J(k_\sharp \widehat{G})$. □

Exercises

(21.1) Prove the converse of Proposition 21.1: if the augmentation ideal $I(kG)$ is the Jacobson radical of kG, then G is a p-group. [Hint: Raise $g-1$ to the power p^n, where $g \in G$.]

(21.2) Let P be a Sylow p-subgroup of G.

(a) Prove that the dimension of a projective kG-module is a multiple of $|P|$. [Hint: Consider the restriction of the module to P. This result will be improved in Exercise 23.2.]

(b) Let $\widehat{G}$ be a central extension of G by k^* and let $k_\sharp \widehat{G}$ be the corresponding twisted group algebra. Prove that the dimension of a projective $k_\sharp \widehat{G}$-module is a multiple of $|P|$. [Hint: Restrict the module to P and use Proposition 21.3.]

(21.3) Let $\widehat{G}$ be a central extension of G by k^* and let $k_\sharp \widehat{G}$ be the corresponding twisted group algebra. If $k_\sharp \widehat{G}$ is semi-simple, prove that p does not divide $|G|$. [Hint: Use the previous exercise to show that the dimension of every module is a multiple of $|P|$, where P is a Sylow p-subgroup of G. Then find a module of dimension prime to p, for instance the module $\mathrm{Ind}_P^G(k) = k_\sharp \widehat{G} \otimes_{kP} k$, where k denotes the trivial kP-module. The result of this exercise is the converse of Exercise 17.3.]

(21.4) Let P_γ be a local pointed group on a G-algebra A and suppose that $\overline{N}_G(P_\gamma)$ is a p-group. If P_γ is the defect of some pointed group G_α (for instance if P_γ is maximal) prove that for every subgroup H with $P \leq H \leq G$, there exists a unique pointed group H_α with defect P_γ. [Hint: Use the Puig correspondence and show that for every H there is a unique projective pointed group $\overline{N}_H(P_\gamma)_\delta$ on the multiplicity algebra $S(\gamma)$.]

(21.5) Assume that G has a normal p-subgroup P. Prove that any vertex of a simple kG-module contains P. [Hint: Let Q be a vertex of a simple kG-module M and assume that $Q < QP$. In $\mathrm{End}_k(M)$, the relative trace map t_Q^{QP} is zero because P acts trivially on M.]

Notes on Section 21

The results of this section are standard.

§ 22 LIFTING IDEMPOTENTS WITH A REGULAR GROUP ACTION

In this section we prove a version of the theorem on lifting idempotents which involves a regular action of G on idempotents.

(22.1) THEOREM. *Let A be a G-algebra and let I be an ideal of A contained in $J(A)$. Let $\overline{A} = A/I$ and denote by $\overline{a}$ the image of an element $a \in A$ in $\overline{A}$. Assume that I is invariant under the action of G, so that $\overline{A}$ is also a G-algebra. If there exists an idempotent $\overline{e} \in \overline{A}$ such that $1_{\overline{A}} = t_1^G(\overline{e})$ and ${}^g\overline{e} \cdot \overline{e} = 0$ for every $g \in G - \{1\}$ (so that $1_{\overline{A}} = \sum_{g\in G} {}^g\overline{e}$ is an orthogonal decomposition), then $\overline{e}$ lifts to an idempotent e of A such that $1_A = t_1^G(e)$ and ${}^g e \cdot e = 0$ for every $g \in G - \{1\}$.*

Proof. Since $I \subseteq J(A)$, the algebra A is complete in the I-adic topology, that is, $A \cong \varprojlim A/I^n$. Thus it suffices to prove the result when I is nilpotent, since the idempotent e can then be constructed as a limit of idempotents of A/I^n having the required property. Details are left to the reader (Exercise 22.1). We assume now that $I^n = 0$ and argue by induction on n. Thus $\overline{e}$ lifts to an idempotent of A/I^{n-1} with the required property, and since $(I^{n-1})^2 = 0$, we are left with the problem of lifting the idempotent when the ideal has square equal to zero. Thus we assume now that $I^2 = 0$.

Write $\overline{e}_g = {}^g\overline{e}$ for every $g \in G$. By Theorem 3.1, we can lift the orthogonal idempotents $\overline{e}_g$ to orthogonal idempotents e_g of A satisfying $\sum_{g\in G} e_g = 1_A$. Since ${}^g(\overline{e}_h) = \overline{e}_{gh}$ for all $g, h \in G$, we have

$$ {}^g(e_h) = e_{gh} + a_{g,h} \qquad \text{for some } a_{g,h} \in I\,. $$

Since $1_A = {}^g(1_A) = {}^g(\sum_h e_h) = \sum_h e_{gh} + \sum_h a_{g,h} = 1_A + \sum_h a_{g,h}$, we have

(22.2) $$ \sum_{h\in G} a_{g,h} = 0 \qquad \text{for every } g \in G\,. $$

Now $e_{ghk} + a_{gh,k} = {}^{gh}(e_k) = {}^{g}(e_{hk} + a_{h,k}) = e_{ghk} + a_{g,hk} + {}^{g}(a_{h,k})$ and therefore

$$(22.3) \qquad {}^{g}(a_{h,k}) = a_{gh,k} - a_{g,hk} \qquad \text{for all } g, h, k \in G\,.$$

Since ${}^{g}(e_h)^2 = {}^{g}(e_h^2) = {}^{g}(e_h)$ and since $I^2 = 0$, we obtain

$$e_{gh}a_{g,h} + a_{g,h}e_{gh} = a_{g,h} \qquad \text{for all } g, h \in G\,.$$

Multiplying this relation by e_x on the left where $x \neq gh$, we obtain $e_x a_{g,h} e_{gh} = e_x a_{g,h}$, and multiplying this by e_y on the right where $gh \neq y$, we get $e_x a_{g,h} e_y = 0$. Thus for $g, h, x, y \in G$, we have

$$(22.4) \qquad e_x a_{g,h} e_y = \begin{cases} e_x a_{g,h} & \text{if } x \neq gh = y, \\ 0 & \text{if } x \neq gh \neq y. \end{cases}$$

Finally since ${}^{g}(e_h)\,{}^{g}(e_k) = {}^{g}(e_h e_k) = 0$ if $h \neq k$ and since $I^2 = 0$, we obtain $e_{gh}a_{g,k} + a_{g,h}e_{gk} = 0$. Taking in particular $k = 1$ and $h = g^{-1}z$, we get

$$(22.5) \qquad e_z a_{g,1} + a_{g,g^{-1}z} e_g = 0 \qquad \text{if } g \neq z\,.$$

Now define

$$f_g = e_g + \sum_{y \in G} a_{y,y^{-1}g} e_y \qquad \text{for all } g \in G\,.$$

Then $\overline{f}_g = \overline{e}_g$ and moreover

$$(22.6) \qquad \begin{aligned} \sum_{g \in G} f_g &= \sum_{g \in G} e_g + \sum_{g \in G} \sum_{y \in G} a_{y,y^{-1}g} e_y \\ &= 1_A + \sum_{y \in G} \Big(\sum_{g \in G} a_{y,y^{-1}g}\Big) e_y = 1_A\,, \end{aligned}$$

using 22.2. Now if $g \neq h$, we have

$$f_g f_h = \sum_{y \in G} e_g a_{y,y^{-1}h} e_y + \sum_{y \in G} a_{y,y^{-1}g} e_y e_h\,,$$

using $e_g e_h = 0$ and $I^2 = 0$. Clearly the only non-zero term in the second sum appears for $y = h$. Moreover the same holds for the first sum by 22.4. Therefore

$$(22.7) \qquad f_g f_h = (e_g a_{h,1} + a_{h,h^{-1}g} e_h) e_h = 0$$

by 22.5. It now follows from 22.6 and 22.7 that each f_g is an idempotent, because

$$f_g = f_g \cdot 1_A = f_g \sum_{h \in G} f_h = f_g^2 \,.$$

Thus we are left with the proof of the additional property we are looking for, namely that G permutes the idempotents f_g regularly. Using 22.3 and $I^2 = 0$, we have

$$\begin{aligned} {}^g(f_h) &= (e_{gh} + a_{g,h}) + \sum_{y \in G} (a_{gy,y^{-1}h} - a_{g,h})(e_{gy} + a_{g,y}) \\ &= \big(e_{gh} + \sum_{z \in G} a_{z,z^{-1}gh} e_z\big) + a_{g,h}(1 - \sum_{y \in G} e_{gy}) = f_{gh} \,, \end{aligned}$$

as required. □

Exercises

(22.1) Complete the details of the beginning of the proof of Theorem 22.1 (namely the reduction to the case where I is nilpotent).

(22.2) Let A be a primitive G-algebra, let H be a normal subgroup of G, and let β be a point of A^H. Assume that A is projective relative to H and that $N_G(H_\beta) = H$. Prove that there exists $j \in \beta$ such that $t_H^G(j) = 1_A$ and ${}^g j \cdot j = 0$ for all $g \in G - H$ (so that $1_A = \sum_{g \in [G/H]} {}^g j$ is an orthogonal decomposition). In particular prove that β has multiplicity one. [Hint: Replace A by A^H to reduce to the case $H = 1$. Show that the map $A \to A/J(A)$ remains surjective on G-fixed elements. Prove that G acts regularly on the simple factors of $A/J(A)$ and lift the information to A.]

Notes on Section 22

The theorem of this section is due to Thévenaz [1983a]. For a more general version involving a transitive action on idempotents, see Thévenaz [1983b].

§ 23 PRIMITIVITY THEOREMS FOR p-GROUPS

The main theorem of this section is about primitive idempotents in a P-algebra where P is a p-group. The result implies in particular the Green indecomposability theorem.

(23.1) THEOREM. *Let P be a p-group and let A be a P-algebra. Let j be a primitive idempotent of A^P such that $j \in A_Q^P$ for some subgroup Q of P. Then there exists a primitive idempotent $i \in A^Q$ such that $j = t_Q^P(i)$ and ${}^g i \cdot i = 0$ for every $g \in P - Q$. In other words $j = \sum_{g\in[P/Q]} {}^g i$ is an orthogonal decomposition in A.*

Proof. We use a series of reductions. First it suffices to solve the problem in the P-algebra jAj which has unity element j. Thus we can assume that $j = 1_A$, so that A is a primitive P-algebra.

Next we can use induction on $|P : Q|$. The result is trivial if $Q = P$, so we assume $Q < P$. Let R be a maximal subgroup of P containing Q. Since P is a p-group, R is a normal subgroup of P of index p. We claim that it suffices to prove the result for P and R. Indeed if this is proved, then there exists a primitive idempotent f of A^R such that $1_A = t_R^P(f)$ and ${}^g f \cdot f = 0$ for every $g \in P - R$. Thus $1_A = \sum_{g\in[P/R]} {}^g f$ is a primitive decomposition in A^R because R is a normal subgroup of P, and hence each ${}^g f$ is a primitive idempotent of A^R. By assumption there exists $a \in A^Q$ such that $t_Q^P(a) = 1_A$ and so

$$1_A = \sum_{g\in[P/R]} {}^g(t_Q^R(a)) = \sum_{g\in[P/R]} (t_{{}^gQ}^R({}^g a)) .$$

Therefore $A^R = \sum_{g\in[P/R]} A_{{}^gQ}^R$. By Rosenberg's lemma (Porposition 4.9), the primitive idempotent f belongs to one of the ideals $A_{{}^gQ}^R$, so that ${}^{g^{-1}} f \in A_Q^R$. Replacing f by ${}^g f$ (this does not change the primitive decomposition $1_A = \sum_{g\in[P/R]} {}^g f$), we can assume that $f \in A_Q^R$. Since $|R : Q| < |P : Q|$, there exists by the induction hypothesis a primitive idempotent $i \in A^Q$ such that $f = t_Q^R(i)$ and ${}^x i \cdot i = 0$ for every $x \in R - Q$. Thus we obtain an orthogonal decomposition

$$1_A = \sum_{g\in[P/R]} {}^g f = \sum_{g\in[P/R]} \sum_{x\in[R/Q]} {}^{gx} i = \sum_{y\in[P/Q]} {}^y i ,$$

proving the result. This establishes the claim above and reduces the problem to the case of a normal subgroup R of index p.

Now we consider the algebra A^R, which is a (P/R)-algebra, and for which 1_A is a primitive idempotent of $(A^R)^{P/R} = A^P$ such that $1_A \in (A^R)_1^{P/R}$. It suffices to prove the theorem for the (P/R)-algebra A^R. In other words we can assume that $R = 1$. Thus we are left with a P-algebra which is primitive (1_A is a primitive idempotent of A^P) and projective ($1_A \in A_1^P$). Moreover P is cyclic of order p, but this will not play any role.

We reduce modulo the Jacobson radical $J(A)$, which is necessarily invariant under the action of P, so that $\overline{A} = A/J(A)$ is again a P-algebra and the canonical homomorphism $\pi : A \to \overline{A}$ is a homomorphism of P-algebras. We show that the two properties of A which we need are inherited by $\overline{A}$. First the image under π of the relation $1_A \in A_1^P$ shows that $\overline{A}$ is projective. To show that $\overline{A}$ remains primitive, it suffices to prove that $A^P \to \overline{A}^P$ is surjective, because then $\overline{A}^P$ is again a local ring with residue field k. To show the surjectivity, let $\overline{a} \in \overline{A}^P$. By projectivity, there exists $\overline{b} \in \overline{A}$ such that $t_1^P(\overline{b}) = \overline{a}$. Lift $\overline{b}$ to $b \in A$ and let $a = t_1^P(b)$. Then $a \in A^P$ and clearly $\pi(a) = \overline{a}$.

Assume that the result holds for the P-algebra $\overline{A}$. Then there exists a primitive idempotent $\overline{i} \in \overline{A}$ such that $t_1^P(\overline{i}) = 1_{\overline{A}}$ and ${}^g\overline{i} \cdot \overline{i} = 0$ for $1 \neq g \in P$. Thus there is a regular group action of P on orthogonal idempotents as in Theorem 22.1. By that theorem, there exists an idempotent $i \in A^P$ lifting $\overline{i}$ such that $1_A = t_1^P(i)$ and ${}^gi \cdot i = 0$ for $1 \neq g \in P$. Moreover i is primitive in A since $\overline{i}$ is primitive in $\overline{A}$. This proves that it suffices to establish the result for $\overline{A}$.

We assume now that A is a semi-simple k-algebra endowed with an action of P such that A is a P-algebra which is primitive and projective. We have

$$A \cong S_1 \times \ldots \times S_m$$

where each S_r is a simple k-algebra ($1 \le r \le m$) and we identify A with this direct product. Let e_r be the primitive idempotent of the centre $Z(A)$ of A corresponding to S_r, that is, all components of e_r are zero except the r-th which is equal to 1_{S_r}. As the group P acts via algebra automorphisms, it necessarily stabilizes $Z(A)$ and therefore it must permute the central idempotents e_r. The sum of all idempotents in one orbit is an idempotent f of A fixed under P. But as 1_A is primitive in A^P, this idempotent f must be 1_A and this proves that P acts transitively on the idempotents e_r, hence also on the simple factors S_r. If H is the stabilizer of e_1, we obtain $1_A = t_H^P(e_1)$ and ${}^ge_1 \cdot e_1 = 0$ for $g \in P - H$.

This proves the theorem if $H = 1$, while if $H = P$, then $A = S_1$ is a simple k-algebra. Since P can be assumed to be cyclic of order p, this reduces to the case of a simple k-algebra. But we are reduced to this case even without this assumption on P, because S_1 is an H-algebra which is primitive ($1_A = t_H^P(e_1)$ is primitive in A^P and so e_1 is primitive in S_1^H) and projective (we have $A^P = A_1^P$, hence $A^H = A_1^H$, and therefore $(S_1)^H = (S_1)_1^H$). If the theorem is proved for the H-algebra S_1, then it also holds for the P-algebra A by the argument above.

Thus we can now assume that S is a primitive projective P-algebra which is simple as a k-algebra, so that $S = \mathrm{End}_k(V)$ for some k-vector space V. We note that the assumption that k is algebraically closed is used here in an essential way. From Example 10.8, the action of P on S lifts to a group homomorphism $\widehat{P} \to S^*$ where $\widehat{P}$ is a central extension of P with central subgroup k^*. By Proposition 21.3, the central extension splits uniquely so that we obtain a unique group homomorphism $P \to S^*$ lifting the given action. In other words S carries a unique interior P-algebra structure inducing the given P-algebra structure. Therefore V becomes a module over the group algebra kP. The assumption that S is primitive means that V is an indecomposable kP-module and the projectivity assumption means that V is a projective kP-module by Corollary 17.4. It follows now fom Proposition 21.1 that V must be a free kP-module of dimension one.

Let v be a free generator of V over kP. Then the set $\{g \cdot v \mid g \in P\}$ is k-basis of V. Let i be the projection of V onto $k \cdot v$ with kernel $\oplus_{g \neq 1} k \cdot gv$. Then i is a primitive idempotent of S (by Proposition 1.14) and ${}^g i$ is the projection onto $k \cdot gv$. Thus $1_S = \sum_{g \in P} {}^g i$ is an orthogonal primitive decomposition of 1_S, proving the theorem. □

Theorem 23.1 above has several consequences, some of them being just other forms of the main result.

(23.2) COROLLARY. *Let P be a p-group, let A be a P-algebra, let P_α be a pointed group on A and let Q_γ be a defect of P_α. Then for every $j \in \alpha$ there exists $i \in \gamma$ such that $j = t_Q^P(i)$ and ${}^g i \cdot i = 0$ for every $g \in P - Q$.*

Proof. This is an easy exercise which is left to the reader. □

(23.3) COROLLARY. *Let N be a normal subgroup of G of index a power of p. Let A be a G-algebra and let j be a primitive idempotent of A^G such that $j \in A_H^G$ for some subgroup H of G containing N. Then there exists a primitive idempotent i of A^H such that $j = t_H^G(i)$ and ${}^g i \cdot i = 0$ for every $g \in G - H$.*

Proof. Since G/N is a p-group, we can apply the theorem to the (G/N)-algebra A^N and to the subgroup $Q = H/N$. □

Of course the main theorem is just the case $N=1$ in this corollary. We use again this more general setting for the statement of the next result.

(23.4) PROPOSITION. *Let N be a normal subgroup of G of index a power of p and let H be a subgroup of G containing N. Let A be a G-algebra and let i be a primitive idempotent of A^H such that ${}^g i \cdot i = 0$ for every $g \in G - H$. Then $j = t_H^G(i)$ is a primitive idempotent of A^G.*

Proof. It is clear that $j = \sum_{g\in[G/H]} {}^g i$ is an orthogonal decomposition in A, so that j is an idempotent of A^G. We prove that j is primitive by induction on $|G:H|$. If M is a maximal subgroup of G containing H, then $f = t_H^M(i)$ is primitive in A^M by induction. Since G/N is a p-group, the maximal subgroup M/N is normal in G/N and so $M \triangleleft G$. This implies that $j = \sum_{g\in[G/M]} {}^g f$ is an orthogonal decomposition in A^M, which is primitive since each ${}^g f$ is primitive. Let $j = \sum_{\lambda=1}^m j_\lambda$ be a primitive decomposition of j in A^G. Since $j \in A_M^G$, we have $j_\lambda = j_\lambda j \in A_M^G$ and by Corollary 23.3, there exists a primitive idempotent $i_\lambda \in A^M$ such that $j_\lambda = t_M^G(i_\lambda) = \sum_{g\in[G/M]} {}^g i_\lambda$ is an orthogonal decomposition. Thus we obtain two primitive decompositions of j in A^M:

$$j = \sum_{g\in[G/M]} {}^g f = \sum_{\lambda=1}^m \sum_{g\in[G/M]} {}^g i_\lambda .$$

For reasons of cardinality, it follows that $m=1$. This means that j is primitive in A^G, as required. □

Recall that a subgroup H of G is called *subnormal* if there exists a series of subgroups

$$H = H_0 < H_1 < \ldots < H_{r-1} < H_r = G$$

such that H_i is a normal subgroup of H_{i+1} for each $i \le r-1$. It is well-known that any subgroup of a p-group is subnormal. As a corollary of Proposition 23.4, we obtain Green's indecomposability theorem (generalized to the case of interior algebras).

(23.5) COROLLARY (Green's indecomposability theorem). *Let H be a subnormal subgroup of G of index a power of p and let B be a primitive interior H-algebra. Then the interior G-algebra $\mathrm{Ind}_H^G(B)$ is primitive. In particular if P is a p-group and if B is a primitive interior Q-algebra for some subgroup Q of P, then $\mathrm{Ind}_Q^P(B)$ is primitive.*

Proof. Let $H = H_0 < H_1 < \ldots < H_{r-1} < H_r = G$ be a series of subgroups with $H_i \triangleleft H_{i+1}$ for each i. By induction it suffices to prove the result for each successive quotient H_{i+1}/H_i. In other words we can assume that H is normal in G. The image of 1_B under the canonical embedding $d_H^G : B \to \mathrm{Res}_H^G \mathrm{Ind}_H^G(B)$ is the primitive idempotent $i = 1 \otimes 1_B \otimes 1$ of $\mathrm{Ind}_H^G(B)^H$. By the construction of induced algebras, we have $1_{\mathrm{Ind}_H^G(B)} = \sum_{g \in [G/H]} {}^g i$ and ${}^g i \cdot i = 0$ for every $g \in G - H$. By Proposition 23.4 above, $1_{\mathrm{Ind}_H^G(B)}$ is a primitive idempotent of $\mathrm{Ind}_H^G(B)^G$, as was to be shown. □

In particular, for $\mathcal{O}G$-modules, we deduce the classical indecomposability theorem of Green.

(23.6) COROLLARY. *Let H be a subnormal subgroup of G of index a power of p and let M be an indecomposable $\mathcal{O}H$-module. Then $\mathrm{Ind}_H^G(M)$ is an indecomposable $\mathcal{O}G$-module. In particular if P is a p-group and if M is an indecomposable $\mathcal{O}Q$-module for some subgroup Q of P, then $\mathrm{Ind}_Q^P(M)$ is indecomposable.*

Proof. We can apply the previous result to the interior H-algebra $B = \mathrm{End}_{\mathcal{O}}(M)$ and the interior G-algebra $\mathrm{Ind}_H^G(B) \cong \mathrm{End}_{\mathcal{O}}(\mathrm{Ind}_H^G(M))$ (see Example 16.4). The indecomposability of a module is equivalent to the primitivity of the corresponding interior algebra. □

Exercises

(23.1) Prove Corollary 23.2.

(23.2) Let M be an indecomposable $\mathcal{O}G$-lattice with vertex Q and let P be a Sylow p-subgroup containing Q. Show that the index $|P : Q|$ divides the dimension of M over $\mathcal{O}$. [Hint: Reduce to the case of a p-group by showing that every indecomposable summand of $\mathrm{Res}_P^G(M)$ has a vertex contained in some conjugate of Q.]

Notes on Section 23

The Green indecomposability theorem appears in Green [1959]. The generalization 23.1 is due to Puig [1979], but the proof we have given is different. Yet another proof appears in Külshammer [1994]. The result of Exercise 23.2 is due to Green [1959].

§ 24 INVARIANT IDEMPOTENT DECOMPOSITIONS FOR p-GROUPS

In this section, we express the main result of the previous section in a different form, namely as an existence result for idempotent decompositions which are invariant under the action of a p-group. In addition we prove a uniqueness result for such decompositions.

Let P be a p-group, let A be a P-algebra, and let I be an orthogonal idempotent decomposition of 1_A. The decomposition I is called *P-invariant* if ${}^x i \in I$ for every $i \in I$ and $x \in P$. In other words P acts on the idempotents in the decomposition. If P_i denotes the stabilizer of i, the sum of all idempotents of the orbit of i is equal to $t_{P_i}^P(i)$. Thus we obtain in A^P an orthogonal decomposition $1_A = \sum_{i \in [P\backslash I]} t_{P_i}^P(i)$, where $[P\backslash I]$ denotes a set of representatives of the P-orbits in I. If in addition each i is primitive in A^{P_i} and belongs to a local point of A^{P_i} (that is, $br_{P_i}(i) \neq 0$), the P-invariant decomposition I will be called *local*. Since a conjugate of a local point is local, it suffices to require that $br_{P_i}(i) \neq 0$ for some i in each orbit.

The existence of P-invariant decompositions which are local is a special feature of p-groups (Exercise 24.1). We prove now their existence and main properties. We say that a decomposition I of 1_A is a *refinement* of a decomposition J of 1_A if every $j \in J$ can be written $j = \sum_{i \in I_j} i$ for some subset I_j of I (and then I is the disjoint union of the subsets I_j for $j \in J$). We also say that J can be refined to the decomposition I.

(24.1) THEOREM. *Let P be a p-group and let A be a P-algebra.*

(a) *There exists a P-invariant local decomposition of 1_A.*

(b) *For every P-invariant local decomposition of 1_A and for every idempotent i in this decomposition, the sum of all idempotents in the orbit of i is a primitive idempotent of A^P.*

(c) *Any P-invariant orthogonal decomposition of 1_A can be refined to a P-invariant local decomposition. In other words a P-invariant decomposition is maximal (in cardinality) if and only if it is local.*

(d) *All P-invariant local decompositions of 1_A are conjugate under the group $(A^P)^*$.*

Proof. (a) Let E be a primitive decomposition of 1_A in A^P. For each $e \in E$, choose a minimal subgroup Q_e such that $e \in A_{Q_e}^P$ (namely a defect group of the point containing e). By Theorem 23.1, we obtain a primitive idempotent $i_e \in A^{Q_e}$ and an orthogonal decomposition $e = t_{Q_e}^P(i_e) = \sum_{x \in [P/Q_e]} {}^x i_e$. Therefore

$$\{ {}^x i_e \mid e \in E\,,\, x \in [P/Q_e]\}$$

is a P-invariant decomposition of 1_A. By construction, i_e belongs to a source point of the point containing e, and in particular i_e is local. Therefore this is a P-invariant local decomposition.

(b) The sum of all idempotents in the orbit of i is equal to $e = t_Q^P(i)$ where Q is the stabilizer of i. Since i is primitive in A^Q by definition of a local decomposition, e is a primitive idempotent of A^P by Proposition 23.4.

We prove (c) and (d) together by establishing the following statement: if I is a given P-invariant local decomposition of 1_A, then any P-invariant decomposition of 1_A can be refined to a conjugate of I (by an element of $(A^P)^*$). For the given local decomposition I, each idempotent $e_i = t_{P_i}^P(i)$ is primitive in A^P by (b). Thus

$$E = \{ e_i \mid i \in [P\backslash I] \}$$

is a primitive decomposition of 1_A in A^P. Let J be any P-invariant decomposition of 1_A, and for each $j \in [P\backslash J]$, let $f_j = t_{P_j}^P(j)$, where P_j is the stabilizer of j. Since each f_j belongs to A^P, the orthogonal decomposition

$$F = \{ f_j \mid j \in [P\backslash J] \}$$

in A^P can be refined to a primitive decomposition of 1_A in A^P. By Theorem 4.1, any two primitive decompositions of 1_A are conjugate under $(A^P)^*$. Thus replacing the given decomposition I by a conjugate, we can assume that E is a refinement of F. Thus each f_j decomposes as an orthogonal sum of some of the primitive idempotents e_i, namely $f_j = \sum_{e_i \in E_j} e_i$. Here we have decomposed E as a disjoint union $E = \bigcup_{j \in [P\backslash J]} E_j$.

Now we claim that it suffices to prove the result when there is a single orbit in the decomposition J. Indeed suppose that this is proved and, for each $f_j \in F$, apply the result to the P-algebra $f_j A f_j$, the P-invariant decomposition $\{ {}^x j \mid x \in [P/P_j] \}$ of f_j (with one orbit), and the local P-invariant decomposition I_j, where $i \in I_j$ if and only if i appears in the decomposition of f_j (that is, $i = f_j i f_j$). Note that the sum of the orbit of i (namely $t_{P_i}^P(i)$) belongs to E_j, and that we have decomposed I as the disjoint union of the subsets I_j for $j \in [P\backslash J]$. Now, if the result holds in $f_j A f_j$, there exists an invertible element $u_j \in (f_j A f_j)^P$ such that I_j is a refinement of the conjugate decomposition of f_j

$$\{ u_j \, {}^x j u_j^{-1} \mid x \in [P/P_j] \}.$$

But the elements u_j for $j \in [P\backslash J]$ are orthogonal (because $u_j = f_j u_j f_j$) and clearly $u = \sum_{j \in [P\backslash J]} u_j$ is an invertible element of A^P (with inverse

$\sum_j u_j^{-1}$). The conjugations by u and by u_j are equal on f_jAf_j . Therefore the decomposition I (which is the union of all the decompositions I_j) is a refinement of the conjugate decomposition

$$uJu^{-1} = \{\, u_j\, {}^x\! j u_j^{-1} \mid j \in [P\backslash J]\,,\, x \in [P/P_j]\,\}\,.$$

This establishes the claim above.

From now on we assume that there is a single orbit in the decomposition J . Then F is a singleton and $f_j = 1_A$. In particular the equation $1_A = t_{P_j}^P(j)$ implies that the P-algebra A is projective relative to the subgroup P_j . Each primitive idempotent $e_i = t_{P_i}^P(i)$ of A^P belongs to a point α_i with defect group P_i and source point containing i , because $br_{P_i}(i) \neq 0$ by assumption. On the other hand P_{α_i} is projective relative to the subgroup P_j since A is projective relative to P_j . Therefore by Proposition 18.5 and the fact that all defect groups are P-conjugate, we have ${}^xP_i \leq P_j$ for some $x \in P$ (depending on i). According to our needs in some of the arguments below, we shall change the choice of the orbit representatives $[P\backslash I]$, and this will have the effect of replacing P_i by some conjugate.

We proceed by induction on $|P : P_j|$. There is nothing to prove when $P_j = P$ (because $J = \{1_A\}$ in that case), so suppose that $P_j < P$. Let R be a maximal subgroup of P containing P_j . Since P is a p-group, R is a normal subgroup of index p . Consider the idempotent $g = t_{P_j}^R(j) \in A^R$, so that we have $1_A = t_R^P(g)$. Choose a primitive decomposition H of g in A^R and let $h \in H$. Since the idempotents $\{\, {}^xg \mid x \in [P/R]\,\}$ are orthogonal, so are the idempotents $\{\, {}^xh \mid x \in [P/R]\,\}$, because we have ${}^xh = {}^xh\, {}^xg = {}^xg\, {}^xh$. Therefore, by Proposition 23.4, $t_R^P(h) = e_h$ is a primitive idempotent of A^P , for every $h \in H$. Applying t_R^P to g we obtain that $E' = \{\, e_h \mid h \in H\,\}$ is a primitive decomposition of 1_A in A^P . By Theorem 4.1, any two primitive decompositions of 1_A are conjugate under $(A^P)^*$. Thus replacing the given decomposition I by a conjugate, we can assume that $E' = E$. In other words H is in bijection with $[P\backslash I]$, we can write h_i for the element of H corresponding to $i \in [P\backslash I]$, and then $t_R^P(h_i) = e_i$.

Since a conjugate of P_i is contained in P_j , hence in R , we have $P_i \leq R$ because R is a normal subgroup of P . For each $i \in [P\backslash I]$, we set $k_i = t_{P_i}^R(i)$, so that we have $e_i = t_R^P(k_i)$. By Proposition 23.4 again, k_i is a primitive idempotent of A^R , and since R is a normal subgroup, ${}^xk_i$ is also a primitive idempotent of A^R , for every $x \in P$. Thus $\{\, {}^xk_i \mid x \in [P/R]\,\}$ is a primitive decomposition of e_i in A^R . On the other hand $\{\, {}^xh_i \mid x \in [P/R]\,\}$ is also a primitive decomposition of e_i in A^R , and we can view both decompositions as primitive decompositions of the unity element of $e_iA^Re_i$. By Theorem 4.1, they are conjugate by an element $c_i \in (e_i A^R e_i)^*$. Thus $c_i h_i c_i^{-1} = {}^x k_i$ for some $x \in [P/R]$. Changing the choice of the orbit representatives $[P\backslash I]$ (that is, replacing i by ${}^x i$, hence k_i by ${}^x k_i$), we can assume that $c_i h_i c_i^{-1} = k_i$ for every $i \in [P\backslash I]$.

Now the elements c_i are orthogonal (because $c_i = e_i c_i e_i$) and clearly $c = \sum_{i \in [P\backslash I]} c_i$ is an invertible element of A^R (whose inverse is equal to $c^{-1} = \sum_{i \in [P\backslash I]} c_i^{-1}$). Since the conjugations by c and c_i are equal on $e_i A^R e_i$, we have

$$cgc^{-1} = \sum_{i \in [P\backslash I]} ch_i c^{-1} = \sum_{i \in [P\backslash I]} k_i \qquad \text{and}$$
$$t_R^P(cgc^{-1}) = \sum_{i \in [P\backslash I]} t_R^P(k_i) = \sum_{i \in [P\backslash I]} e_i = 1_A .$$

But since the idempotents $\{ {}^x g \mid x \in [P/R] \}$ are orthogonal, it follows that

$$t_R^P(cg) t_R^P(gc^{-1}) = \sum_{x \in [P/R]} \sum_{y \in [P/R]} {}^x(cg)\, {}^y(gc^{-1}) = \sum_{x \in [P/R]} {}^x(cggc^{-1})$$
$$= t_R^P(cgc^{-1}) = 1_A .$$

Thus $b = t_R^P(cg)$ is invertible with inverse $b^{-1} = t_R^P(gc^{-1})$ (because $b^{-1}b = 1_A$ by a similar computation or because of Exercise 3.3). Now since h_i appears in a decomposition of g, it is orthogonal to ${}^x g$ for $x \notin R$, and we have

$$bh_i b^{-1} = \sum_{x \in [P/R]} \sum_{y \in [P/R]} {}^x(cg) h_i\, {}^y(gc^{-1}) = ch_i c^{-1} = k_i .$$

This proves that one can conjugate by $b \in (A^P)^*$ instead of $c \in (A^R)^*$. Thus replacing the given decomposition I by its conjugate under b, we can assume that $k_i = h_i$ for every $i \in [P\backslash I]$, that is, $t_{P_i}^R(i) = h_i$.

We are now in the situation where we have an R-invariant decomposition of g

$$\{ {}^y j \mid y \in [R/P_j] \}$$

with a single orbit and a local R-invariant decomposition of g

$$\{ {}^y i \mid i \in [P\backslash I] ,\, y \in [R/P_i] \} \tag{24.2}$$

(for which the sum of one orbit is $t_{P_i}^R(i) = h_i$). These decompositions lie in the R-algebra gAg with unity element g. Since $|R : P_j| < |P : P_j|$, the induction hypothesis implies that there exists $d \in (gA^R g)^*$ such that the decomposition 24.2 is a refinement of the conjugate decomposition of g

$$\{\, d\,{}^y j d^{-1} \mid y \in [R/P_j]\,\}\,. \tag{24.3}$$

This implies in fact that $djd^{-1} = \sum_{i\in[P\backslash I]} t_{P_i}^{P_j}(i)$ for a suitable choice of orbit representatives $[P\backslash I]$ (Exercise 24.3), but we do not need this explicit statement. The argument used above when we replaced c by $b = t_R^P(cg)$ works again. Thus we can replace $d \in (gA^R g)^*$ by $a = t_R^P(d) \in (A^P)^*$, having inverse $a^{-1} = t_R^P(d^{-1})$ (note that $d = gdg$). Indeed we have $aja^{-1} = djd^{-1}$ by an easy computation. Taking the union of the conjugates under P/R of both decompositions 24.2 and 24.3, we obtain that the decomposition I is a refinement of the conjugate decomposition of 1_A

$$aJa^{-1} = \{\, a\,{}^x j a^{-1} \mid x \in [P/P_j]\,\}\,,$$

as required.

There is a slightly subtle point which remains to be checked. We have made successive assumptions by replacing I by a suitable conjugate, but we have not verified that each previous assumption remained unchanged by the next conjugation. This is left as an exercise for the reader. □

Exercises

(24.1) Show that Theorem 24.1 only holds for p-groups by finding an example of a G-algebra A in which there is no local G-invariant decomposition of 1_A.

(24.2) Let P be a p-group and let A be a primitive P-algebra. Show that all P-invariant local decompositions of 1_A are conjugate under the multiplicative group $1 + J(A^P)$.

(24.3) Prove the statement appearing just after 24.3 in the above proof, namely that $djd^{-1} = \sum_{i\in[P\backslash I]} t_{P_i}^{P_j}(i)$ for a suitable choice of orbit representatives $[P\backslash I]$.

(24.4) Prove the statement appearing at the end of the above proof, namely that each successive conjugation of I has not influenced the previous assumptions.

(24.5) Let P be a p-group, let A be a P-algebra, and let I be a P-invariant decomposition of 1_A. Prove that the following statements are equivalent.

(a) The number of orbits is maximal.

(b) i is primitive in A^{P_i} for every $i \in I$.

(c) $t_{P_i}^P(i)$ is primitive in A^P for every $i \in I$.

Notes on Section 24

Theorem 24.1 is due to Puig [1979]. A generalization appears as Lemma 8.9 in Puig [1988a], for groups having a normal Sylow p-subgroup.

§ 25 COVERING EXOMORPHISMS

We consider in this section G-algebra exomorphisms $\mathcal{F} : A \to B$ which are "essentially surjective" on all subalgebras of fixed elements. This condition allows us to lift pointed groups from B to A and will be essential in some applications for relating the defect theory in A with that of B. Finally we prove an important theorem which gives a local characterization of such exomorphisms.

First we work with $\mathcal{O}$-algebras. A homomorphism of $\mathcal{O}$-algebras $f : A \to B$ is called a *covering homomorphism* if the homomorphism

$$A \xrightarrow{f} B \xrightarrow{\pi_B} B/J(B)$$

is surjective, or equivalently if $B = f(A) + J(B)$. Here $\pi_B : B \to B/J(B)$ is the canonical map onto the semi-simple quotient of B. In particular any surjective homomorphism is a covering homomorphism.

(25.1) LEMMA. *Let $f : A \to B$ be a covering homomorphism of $\mathcal{O}$-algebras.*

(a) f is unitary.

(b) $f(J(A)) \subseteq J(B)$.

(c) f induces a surjective homomorphism $\overline{f} : A/J(A) \to B/J(B)$ such that $\overline{f}\,\pi_A = \pi_B\, f$.

Proof. (a) Note first that a surjective homomorphism $f : A \to B$ is necessarily unitary, because $1_B - f(1_A) = f(a)$ for some $a \in A$ and so $1_B - f(1_A) = f(a{\cdot}1_A) = (1_B - f(1_A))f(1_A) = 0$ since $f(1_A)$ is an idempotent. Now if f is a covering homomorphism, then $\pi_B\, f(1_A) = 1_{B/J(B)}$ by the surjectivity of $\pi_B\, f$. The two idempotents $f(1_A)$ and 1_B have the same image in $B/J(B)$ and are therefore conjugate, hence equal.

(b) Since $\pi_B\, f : A \to B/J(B)$ is surjective onto a semi-simple algebra, the kernel contains $J(A)$. This means that $f(J(A)) \subseteq J(B)$.

(c) This follows immediately from (b). □

Let $f : A \to B$ be a covering homomorphism. The surjective ring homomorphism $\pi_B\, f$ induces an injective map $\mathrm{Max}(B/J(B)) \to \mathrm{Max}(A)$ (via inverse images). But since the map $\mathrm{Max}(B/J(B)) \to \mathrm{Max}(B)$ induced by π_B is always a bijection, we obtain an injective map

$$\mathrm{Max}(B) \longrightarrow \mathrm{Max}(A)\,, \qquad \mathfrak{m} \mapsto f^{-1}(\mathfrak{m})\,.$$

In terms of points, using the canonical bijection between points and maximal ideals (Theorem 4.3), we obtain an injective map

$$f^* : \mathcal{P}(B) \longrightarrow \mathcal{P}(A)$$

such that for $\beta \in \mathcal{P}(B)$, the point $\alpha = f^*(\beta)$ is characterized by the property $\alpha \not\subseteq f^{-1}(\mathfrak{m}_\beta)$, or in other words $f(\alpha) \not\subseteq \mathfrak{m}_\beta$. But for every $i \in \alpha$, the idempotent $\pi_B f(i)$ is primitive in $B/J(B)$, because $\pi_B f$ is surjective (Theorem 3.2), and therefore $f(i)$ is primitive in B (Theorem 3.1). Thus $f(\alpha)$ consists of primitive idempotents, so that the relation $f(\alpha) \not\subseteq \mathfrak{m}_\beta$ is equivalent to the inclusion $f(\alpha) \subseteq \beta$. Also $\pi_B\, f(\alpha) = \overline{\beta}$, where $\overline{\beta} = \pi_B(\beta) \in \mathcal{P}(B/J(B))$, but without passing to the semi-simple quotient, the relation $f(\alpha) \subseteq \beta$ need not be an equality. Thus β is the conjugacy closure of $f(\alpha)$.

If $\overline{f} : A/J(A) \to B/J(B)$ denotes the surjective ring homomorphism induced by f and if we let again $\alpha = f^*(\beta)$, then we have $\overline{f}(\overline{\alpha}) = \overline{\beta}$, where $\overline{\alpha} = \pi_A(\alpha) \in \mathcal{P}(A/J(A))$. If we write $A/J(A) = \prod_{\alpha \in \mathcal{P}(A)} S(\alpha)$ with $S(\alpha)$ simple, then $\mathrm{Ker}(\overline{f}) = \prod_{\alpha \in I} S(\alpha)$ for some subset I of $\mathcal{P}(A)$, and $\overline{f}$ induces an isomorphism $\prod_{\alpha \in \mathcal{P}(A) - I} S(\alpha) \cong B/J(B)$. The set $\mathcal{P}(A) - I$ is exactly the image of f^*, while for every $\alpha \in I$, we have $\pi_B\, f(\alpha) = \{0\}$, hence $f(\alpha) = \{0\}$. If we map further onto multiplicity algebras, then for every $\beta \in \mathcal{P}(B)$, the surjection $\pi_\beta\, f : A \to S(\beta)$ induces an isomorphism $f_\beta : S(\alpha) \xrightarrow{\sim} S(\beta)$, where $\alpha = f^*(\beta)$. In particular the multiplicities m_β and m_α are equal. By Lemma 4.13, the image of $B\beta B$ in $B/J(B)$ is equal to the minimal ideal isomorphic to $S(\beta)$, and similarly for $A\alpha A$. Since $f(A\alpha A) \subseteq B\beta B$ and because of the isomorphism f_β, we deduce that $f(A\alpha A)$ has the same image in $B/J(B)$ as $B\beta B$. Therefore $f(A\alpha A) + J(B) = B\beta B + J(B)$. We record these facts for later use.

(25.2) LEMMA. *Let* $f : A \to B$ *be a covering homomorphism of* $\mathcal{O}$*-algebras, let* $f^* : \mathcal{P}(B) \to \mathcal{P}(A)$ *be the associated injective map, and let* $\alpha \in \mathcal{P}(A)$ *. Then*

$$\begin{array}{ll} f(\alpha) = \{0\} & \textit{if } \alpha \notin \mathrm{Im}(f^*), \\ f(\alpha) \subseteq \beta & \textit{if } \alpha = f^*(\beta). \end{array}$$

In the latter case f *induces an isomorphism* $f_\beta : S(\alpha) \xrightarrow{\sim} S(\beta)$ *(so that in particular* $m_\alpha = m_\beta$ *) and moreover* $f(A\alpha A) + J(B) = B\beta B + J(B)$ *.*

If $f : A \to B$ is a covering homomorphism such that $\mathrm{Ker}(f) \subseteq J(A)$, then f is called a *strict* covering homomorphism. This corresponds to the requirement that the map $\overline{f} : A/J(A) \to B/J(B)$ be an isomorphism, or equivalently, that the subset I above be empty. This in turn is equivalent to the condition that the induced map $f^* : \mathcal{P}(B) \to \mathcal{P}(A)$ is a bijection.

We now show that the existence of an induced map f^* which preserves multiplicities characterizes covering homomorphisms.

(25.3) PROPOSITION. *Let* $f : A \to B$ *be a homomorphism of* $\mathcal{O}$*-algebras. The following conditions are equivalent.*
(a) f *is a covering homomorphism.*
(b) There exists a map $f^* : \mathcal{P}(B) \to \mathcal{P}(A)$ *such that if* $\beta \in \mathcal{P}(B)$ *and* $\alpha = f^*(\beta)$ *, then* $f(\alpha) \subseteq \beta$ *and* $m_\alpha = m_\beta$ *.*
Moreover f *is strict if and only if* f^* *is a bijection.*

Proof. We have already seen that (a) implies (b). Assume conversely that f^* exists. Let $\beta \in \mathcal{P}(B)$ and $\alpha = f^*(\beta)$. In a primitive decomposition of 1_A , choose one idempotent $i \in \alpha$ and write all of the other idempotents in α as conjugates of i . Thus

$$1_A = \sum_{u \in U} i^u + e \,,$$

where U is a finite set of invertible elements of A (of cardinality m_α) and e is the sum of all idempotents in the decomposition which do not belong to α . As in the proof of Theorem 7.3, the elements $u^{-1}iv$ for $u, v \in U$ satisfy the orthogonality relations 7.4

$$t^{-1}iu \cdot v^{-1}iw = \begin{cases} t^{-1}iw & \text{if } u = v, \\ 0 & \text{otherwise,} \end{cases}$$

and span a subalgebra which is mapped onto the multiplicity algebra $S(\alpha)$. By assumption $f(i^u) \in \beta$ for every $u \in U$ and so $\pi_\beta\, f(i^u)$ is a primitive idempotent of $S(\beta)$. Since the decomposition $\sum_{u \in U} \pi_\beta\, f(i^u)$ is orthogonal and since by assumption $|U| = m_\alpha = m_\beta$, we must have $\sum_{u\in U} \pi_\beta\, f(i^u) = 1_{S(\beta)}$ (otherwise $1_{S(\beta)} - \sum_{u\in U} \pi_\beta\, f(i^u)$ is non-zero and we obtain a decomposition of $1_{S(\beta)}$ of size $> m_\beta$). It follows in particular that $\pi_\beta\, f(1_A) = 1_{S(\beta)}$ (and $\pi_\beta\, f(e) = 0$), and so $\pi_\beta\, f(u)$ is invertible in $S(\beta)$. Therefore we have a primitive decomposition

$$1_{S(\beta)} = \sum_{u\in U} (\pi_\beta\, f(i))^{\pi_\beta\, f(u)}\,,$$

and, as above, the elements $\pi_\beta\, f(u)^{-1} \pi_\beta\, f(i)\, \pi_\beta\, f(v)$ (where $u, v \in U$) span the whole matrix algebra $S(\beta)$. This proves that $\pi_\beta\, f$ is surjective.

This argument works for every point $\beta \in \mathcal{P}(B)$ and we therefore obtain a surjective map

$$\Big(\prod_{\beta\in\mathcal{P}(B)} \pi_\beta\, f \Big) : A \longrightarrow \prod_{\beta\in\mathcal{P}(B)} S(\beta) \;\cong\; B/J(B)\,.$$

This completes the proof that f is a covering homomorphism because this map is the canonical map $\pi_B\, f : A \to B/J(B)$. The other assertion about strict covering homomorphisms has already been proved. $\square$

It happens in practice that one knows in advance that f is unitary. In that case, one can ignore multiplicities and use the following characterization of covering homomorphisms.

(25.4) COROLLARY. *Let $f : A \to B$ be a unitary homomorphism of $\mathcal{O}$-algebras. The following conditions are equivalent.*

(a) f is a covering homomorphism.

(b) For every $\alpha \in \mathcal{P}(A - \mathrm{Ker}(f))$, there exists $\beta \in \mathcal{P}(B)$ such that $f(\alpha) \subseteq \beta$, and whenever two points $\alpha, \alpha' \in \mathcal{P}(A - \mathrm{Ker}(f))$ satisfy $f(\alpha) \subseteq \beta$ and $f(\alpha') \subseteq \beta$, then $\alpha = \alpha'$.

Moreover f is strict if and only if no point of A is contained in $\mathrm{Ker}(f)$.

Proof. By Lemma 25.2, (a) implies (b). Assume conversely that (b) holds. In a primitive decomposition of 1_A, choose one idempotent $i_\alpha \in \alpha$ for each $\alpha \in \mathcal{P}(A)$ and write all of the other idempotents in α as conjugates of i_α. Thus

$$1_A = \sum_{\alpha\in\mathcal{P}(A)} \sum_{u\in U_\alpha} i_\alpha^u\,,$$

where U_α is a finite set of invertible elements of A (of cardinality m_α). By assumption each $f(i_\alpha^u) = f(i_\alpha)^{f(u)}$ is either zero or belongs to the corresponding point $\beta \in \mathcal{P}(B)$. Therefore the decomposition

$$1_B = f(1_A) = \sum_{\alpha\in\mathcal{P}(A-\mathrm{Ker}(f))} \sum_{u\in U_\alpha} f(i_\alpha)^{f(u)}$$

is a primitive decomposition of 1_B. Since $f(i_\alpha)$ and $f(i_{\alpha'})$ belong to distinct points if $\alpha \neq \alpha'$, the multiplicity of the point β containing $f(\alpha)$ is equal to the multiplicity of α. Thus there is a map $f^* : \beta \mapsto \alpha$ which preserves multiplicities, and by Proposition 25.3, f is a covering homomorphism.

The additional statement about strict covering homomorphisms follows from the observation that f^* is a bijection if and only if we have $\mathcal{P}(A - \mathrm{Ker}(f)) = \mathcal{P}(A)$. □

Since inner automorphisms are harmless, there is a clear extension of the above notions to exomorphisms. An exomorphism of $\mathcal{O}$-algebras $\mathcal{F} : A \to B$ is called a *covering exomorphism* (respectively a *strict covering exomorphism*) if some $f \in \mathcal{F}$ (or equivalently every $f \in \mathcal{F}$) is a covering homomorphism (respectively a strict covering homomorphism). In that case the injective map $f^* : \mathcal{P}(B) \to \mathcal{P}(A)$ is clearly independent of the choice of f and we write $\mathcal{F}^* = f^*$.

We now move to the case of G-algebras. Recall that an exomorphism of G-algebras $\mathcal{F} : A \to B$ induces for each subgroup H an exomorphism of $\mathcal{O}$-algebras $\mathcal{F}^H : A^H \to B^H$ (namely $\mathcal{F}^H$ contains the restriction f^H of f for every $f \in \mathcal{F}$). An exomorphism of G-algebras $\mathcal{F} : A \to B$ is called a *covering exomorphism* (respectively a *strict covering exomorphism*) if, for every subgroup H of G, the exomorphism of $\mathcal{O}$-algebras $\mathcal{F}^H : A^H \to B^H$ is a covering exomorphism (respectively a strict covering exomorphism). Thus for every subgroup H there is an injective map $(\mathcal{F}^H)^* : \mathcal{P}(B^H) \to \mathcal{P}(A^H)$ mapping β to α if and only if $\mathcal{F}(\alpha) \subseteq \beta$. Moreover each $(\mathcal{F}^H)^*$ is a bijection if $\mathcal{F}$ is strict. Note that, in order that $\mathcal{F}$ be strict, it suffices to require the single inclusion $\mathrm{Ker}(f) \subseteq J(A)$ (where $f \in \mathcal{F}$), because the inclusions $\mathrm{Ker}(f^H) \subseteq J(A^H)$ follow by intersecting with A^H (thanks to Exercise 2.1).

We are going to show that the maps $\mathcal{F}^H$ behave well with respect to the notions attached to pointed groups. We first need a lemma.

(25.5) LEMMA. *Let A be a G-algebra and let $Q \leq P \leq G$.*
(a) If Q is normal in P, then $t_Q^P(J(A^Q)) \subseteq J(A^P)$.
(b) If P is a p-subgroup of G, then $t_Q^P(J(A^Q)) \subseteq J(A^P)$.

Proof. (a) The algebra A^Q is invariant under the action of P, hence so is its Jacobson radical $J(A^Q)$. Therefore

$$t_Q^P(J(A^Q)) = \sum_{g \in [P/Q]} {}^g(J(A^Q)) \subseteq J(A^Q).$$

By Exercise 2.1 it follows that $t_Q^P(J(A^Q)) \subseteq J(A^Q) \cap A^P \subseteq J(A^P)$.

(b) By induction on $|P:Q|$, it suffices to prove the result when Q is a maximal subgroup of P. But as P is a p-group, Q is normal in P and (a) applies. □

(25.6) PROPOSITION. *Let $\mathcal{F} : A \to B$ be a covering exomorphism of G-algebras.*

(a) *For every subgroup H of G, $\mathcal{F}$ induces an injective map*

$$(\mathcal{F}^H)^* : \mathcal{P}(B^H) \longrightarrow \mathcal{P}(A^H)\,, \qquad \alpha \mapsto \alpha^*\,,$$

where α^* is characterized by the property $\mathcal{F}(\alpha^*) \subseteq \alpha$. Thus the family of maps $(\mathcal{F}^H)^*$ induces an injection $\mathcal{F}^* : \mathcal{PG}(B) \to \mathcal{PG}(A)$, defined by $\mathcal{F}^*(H_\alpha) = H_{\alpha^*}$.

(b) *Let H_α and K_β be pointed groups on B. Then $H_\alpha \geq K_\beta$ if and only if $H_{\alpha^*} \geq K_{\beta^*}$. Moreover if $H_{\alpha'} \geq K_{\beta^*}$ for some pointed group $H_{\alpha'}$ on A, then $\alpha' = \alpha^*$ for some α (and so $H_\alpha \geq K_\beta$).*

(c) *Let P_γ be a pointed group on B. Then P_γ is local if and only if P_{γ^*} is local.*

(d) *Let H_α and P_γ be pointed groups on B. Then P_γ is a defect of H_α if and only if P_{γ^*} is a defect of H_{α^*}.*

(e) *If $g \in G$, then the image of ${}^g(H_\alpha)$ under $\mathcal{F}^*$ is equal to ${}^g(H_{\alpha^*})$. In particular $N_G(H_{\alpha^*}) = N_G(H_\alpha)$.*

Proof. (a) is a restatement of the definitions. For the rest of this proof, we choose $f \in \mathcal{F}$ and we let $f^H : A^H \to B^H$ be the restriction of f. Thus we have $f^H(\alpha^*) \subseteq \alpha$ and there is an induced isomorphism $f_\alpha : S(\alpha^*) \to S(\alpha)$.

(b) We have $H_{\alpha^*} \geq K_{\beta^*}$ if and only if $\pi_{\beta^*}\, r_K^H(\alpha^*) \neq \{0\}$. Composing these maps with the isomorphism $f_{\beta^*} : S(\beta^*) \to S(\beta)$ and using $f_{\beta^*}\, \pi_{\beta^*} = \pi_\beta\, f^K$ as well as $f^K\, r_K^H = r_K^H\, f^H$, we see that $H_{\alpha^*} \geq K_{\beta^*}$ is equivalent to $\pi_\beta\, r_K^H\, f^H(\alpha^*) \neq \{0\}$. But since α is the conjugacy closure of $f^H(\alpha^*)$, this holds if and only if $\pi_\beta\, r_K^H(\alpha) \neq \{0\}$, that is, $H_\alpha \geq K_\beta$. For the second assertion in (b), we have by assumption $H_{\alpha'} \geq K_{\beta^*}$, that is, $\pi_{\beta^*}\, r_K^H(\alpha') \neq \{0\}$. It follows as above that $\pi_\beta\, r_K^H\, f^H(\alpha') \neq \{0\}$, forcing $f^H(\alpha') \neq \{0\}$. By Lemma 25.2, α' is in the image of $(f^H)^*$, as required.

(c) If either P_γ or P_{γ^*} is local, then P is necessarily a p-group (Lemma 14.4). Thus we can assume that P is a p-subgroup of G. Let us first prove that we have $B_Q^P + J(B^P) = f^P(A_Q^P) + J(B^P)$ for every subgroup Q of P. This follows from the definition of a covering homomorphism and Lemma 25.5 above, because

$$\begin{aligned} B_Q^P = t_Q^P(B^Q) = t_Q^P(f^Q(A^Q) + J(B^Q)) &= f^P(t_Q^P(A^Q)) + t_Q^P(J(B^Q)) \\ \subseteq f^P(A_Q^P) + J(B^P) \subseteq B_Q^P + J(B^P)\,. \end{aligned}$$

Summing over all proper subgroups of P, it follows that there is an equality of ideals

$$(\sum_{Q<P} B_Q^P) + J(B^P) = f^P(\sum_{Q<P} A_Q^P) + J(B^P)\,.$$

Now P_γ is local if and only if $\gamma \not\subseteq (\sum_{Q<P} B_Q^P) + J(B^P)$, thanks to Rosenberg's lemma (Proposition 4.9) and the fact that $\gamma \not\subseteq J(B^P)$. Since γ is the conjugacy closure of $f^P(\gamma^*)$ and by Rosenberg's lemma again, this is equivalent to the condition $f^P(\gamma^*) \not\subseteq f^P(\sum_{Q<P} A_Q^P)$, that is, $\gamma^* \not\subseteq (\sum_{Q<P} A_Q^P) + \mathrm{Ker}(f^P)$. By Rosenberg's lemma once again (and the fact that $\gamma^* \not\subseteq \mathrm{Ker}(f^P)$), this holds if and only if $\gamma^* \not\subseteq \sum_{Q<P} A_Q^P$, which means that γ^* is local.

(d) Suppose first that P_{γ^*} is a defect of H_{α^*}. Let Q_δ be a local pointed group on B such that $P_\gamma \leq Q_\delta \leq H_\alpha$. Then $P_{\gamma^*} \leq Q_{\delta^*} \leq H_{\alpha^*}$ by (b), and Q_{δ^*} is local by (c). By the maximality of P_{γ^*} (Theorem 18.3), $P_{\gamma^*} = Q_{\delta^*}$ and therefore $P_\gamma = Q_\delta$. This proves that P_γ is a maximal local pointed group contained in H_α, that is, P_γ is a defect of H_α.

Assume conversely that P_γ is a defect of H_α and let Q_{δ_0} be a local pointed group on A such that $P_{\gamma^*} \leq Q_{\delta_0} \leq H_{\alpha^*}$. By the second assertion in (b) (applied to $P_{\gamma^*} \leq Q_{\delta_0}$), there exists $\delta \in \mathcal{P}(B^Q)$ whose image in $\mathcal{P}(A^Q)$ is $\delta^* = \delta_0$. Then $P_\gamma \leq Q_\delta \leq H_\alpha$ by (b) and Q_δ is local by (c). Therefore $P_\gamma = Q_\delta$ by maximality of P_γ, and so $P_{\gamma^*} = Q_{\delta^*}$. This proves that P_{γ^*} is a defect of H_{α^*}.

(e) The proof is straightforward and is left to the reader. □

Another useful observation is that a covering exomorphism induces a covering exomorphism between localizations.

(25.7) PROPOSITION. *Let $\mathcal{G} : A \to B$ be a covering exomorphism of G-algebras, let H_α be a pointed group on B, and let $\mathcal{F}_\alpha : B_\alpha \to \mathrm{Res}_H^G(B)$ be an embedding associated with H_α. Let $\alpha^* \in \mathcal{P}(A^H)$ be the image of α (characterized by the property $\mathcal{G}(\alpha^*) \subseteq \alpha$), and let $\mathcal{F}_{\alpha^*} : A_{\alpha^*} \to \mathrm{Res}_H^G(A)$ be an embedding associated with H_{α^*}.*

(a) There exists a unique exomorphism of H-algebras $\mathcal{G}_\alpha : A_{\alpha^*} \to B_\alpha$ such that $\mathcal{F}_\alpha \mathcal{G}_\alpha = \mathrm{Res}_H^G(\mathcal{G})\mathcal{F}_{\alpha^*}$.

(b) $\mathcal{G}_\alpha$ is a covering exomorphism of H-algebras. Moreover $\mathcal{G}_\alpha$ is strict if $\mathcal{G}$ is strict.

Proof. (a) Choose $g \in \mathcal{G}$, let $j \in \alpha^*$, and let $i = g(j) \in \alpha$. Then we can assume that $B_\alpha = iBi$ and that $\mathcal{F}_\alpha$ is the exomorphism containing the inclusion. Similarly $A_{\alpha^*} = jAj$ and $\mathcal{F}_{\alpha^*}$ contains the inclusion. Since $g(j) = i$, it is obvious that g induces a homomorphism of H-algebras $g_\alpha : jAj \to iBi$. Then the exomorphism $\mathcal{G}_\alpha$ containing g_α satisfies $\mathcal{F}_\alpha \mathcal{G}_\alpha = \mathrm{Res}_H^G(\mathcal{G})\mathcal{F}_{\alpha^*}$. Moreover by Proposition 12.2 and since $\mathcal{F}_\alpha$ is an embedding, $\mathcal{G}_\alpha$ is the unique exomorphism satisfying this equation.

(b) The proof is easy and is left as an exercise for the reader (see Exercise 25.2). □

Recall from 11.6 that, for every p-subgroup P of G, a homomorphism of G-algebras $f : A \to B$ induces a homomorphism of k-algebras $\overline{f}(P) : \overline{A}(P) \to \overline{B}(P)$ such that $\overline{f}(P)\, br_P^A = br_P^B f^P$. As usual, the maps $br_P^A : A^P \to \overline{A}(P)$ and $br_P^B : B^P \to \overline{B}(P)$ denote the respective Brauer homomorphisms. Also an exomorphism of G-algebras $\mathcal{F} : A \to B$ induces an exomorphism of k-algebras $\overline{\mathcal{F}}(P) : \overline{A}(P) \to \overline{B}(P)$, where $\overline{\mathcal{F}}(P)$ contains $\overline{f}(P)$ if $f \in \mathcal{F}$. If $\mathcal{F}$ is a covering exomorphism of G-algebras, then $\overline{\mathcal{F}}(P)$ is a covering exomorphism of k-algebras, because of the commutativity of the following diagram:

$$\begin{array}{ccccc} A^P & \xrightarrow{f^P} & B^P & \longrightarrow & B^P/J(B^P) \\ {\scriptstyle br_P^A}\downarrow & & \downarrow{\scriptstyle br_P^B} & & \downarrow \\ \overline{A}(P) & \xrightarrow{\overline{f}(P)} & \overline{B}(P) & \longrightarrow & \overline{B}(P)/J(\overline{B}(P)) \end{array}$$

where $f \in \mathcal{F}$, and the right hand side vertical map is the surjective homomorphism induced by br_P^B. Clearly the surjectivity of the composite map in the first row implies the surjectivity of the composite in the second row.

Our aim is to prove conversely that the condition that $\overline{\mathcal{F}}(P)$ be a covering exomorphism for every P is sufficient to guarantee that $\mathcal{F}$ is a covering exomorphism of G-algebras. This is a typical result of the kind we are interested in, which asserts that "local" information is sufficient to deduce "global" information. We need the following lemma.

(25.8) LEMMA. *Let P_γ be a local pointed group on a G-algebra A and let H be a subgroup of G containing P. Then*

$$t_P^H\big(J(A^P) \cap A^P\gamma A^P\big) \subseteq J(A^H) + \sum_{Q_\delta < P_\gamma} t_Q^H(A^Q\delta A^Q)\,.$$

Proof. Since $I = t_P^H\big(J(A^P) \cap A^P\gamma A^P\big)$ is an ideal of A^H (see 11.1), we have by Proposition 4.14

$$I \subseteq J(A^H) + \sum_{\substack{\alpha \in \mathcal{P}(A^H) \\ \alpha \subseteq I}} A^H\alpha A^H\,.$$

Thus it suffices to show that $A^H\alpha A^H \subseteq \sum_{Q_\delta < P_\gamma} t_Q^H(A^Q\delta A^Q)$ whenever $\alpha \subseteq I$.

Let $\alpha \in \mathcal{P}(A^H)$ such that $\alpha \subseteq t_P^H\big(J(A^P) \cap A^P\gamma A^P\big)$. Then in particular $H_\alpha\, pr\, P_\gamma$. By minimality of defect pointed groups with respect to this relation (Theorem 18.3), there exists a defect Q_δ of H_α such that $Q_\delta \leq P_\gamma$. On the other hand by Proposition 14.7 we have

$$\pi_\gamma\, r_P^H\, t_P^H\big(J(A^P) \cap A^P\gamma A^P\big) = t_1^{\overline{N}_H(P_\gamma)}\, \pi_\gamma\big(J(A^P) \cap A^P\gamma A^P\big) = \{0\}\,,$$

because $\pi_\gamma(J(A^P)) = \{0\}$. In particular $\pi_\gamma\, r_P^H(\alpha) = \{0\}$, which means that $H_\alpha \not\geq P_\gamma$. Since $H_\alpha \geq Q_\delta$, it follows that $Q_\delta \neq P_\gamma$, hence $Q_\delta < P_\gamma$. Therefore, since $H_\alpha\, pr\, Q_\delta$, we obtain

$$\alpha \subseteq t_Q^H(A^Q\delta A^Q) \subseteq \sum_{Q_\delta < P_\gamma} t_Q^H(A^Q\delta A^Q)\,,$$

as was to be shown. □

We now come to the main result.

(25.9) THEOREM. *Let $\mathcal{F} : A \to B$ be an exomorphism of G-algebras. For every p-subgroup P of G, let $\overline{\mathcal{F}}(P) : \overline{A}(P) \to \overline{B}(P)$ be the exomorphism of k-algebras induced by $\mathcal{F}$. The following conditions are equivalent.*

(a) $\mathcal{F}$ is a covering exomorphism of G-algebras.

(b) For every p-subgroup P of G, $\overline{\mathcal{F}}(P)$ is a covering exomorphism of k-algebras.

(c) For all subgroups $K \leq H \leq G$, we have $B_K^H \subseteq f^H(A_K^H) + J(B^H)$ for some (or for every) $f \in \mathcal{F}$.

If moreover these conditions are satisfied, then $\mathcal{F}$ is strict if and only if $\overline{\mathcal{F}}(P)$ is strict for every p-subgroup P of G.

Proof. The fact that (a) implies (b) has already been noted above. It is clear that (c) implies (a) by taking $K = H$. So we are left with the proof that (b) implies (c). Choose $f \in \mathcal{F}$ and suppose that (b) holds. Using induction on $|K|$, assume that (c) holds for every proper subgroup of K. Note that the subsequent argument also holds for $K = 1$, which allows us to start the induction. Since $B^K = \sum_{\beta \in \mathcal{P}(B^K)} B^K\beta B^K$ by Proposition 4.14, it suffices to prove that $t_K^H(B^K\beta B^K) \subseteq f^H(A_K^H) + J(B^H)$, where $\beta \in \mathcal{P}(B^K)$. Let P_γ be a defect of K_β. Since we have inclusions $B^K\beta B^K \subseteq t_P^K(B^P\gamma B^P)$ (that is, $K_\beta\, pr\, P_\gamma$) and $A_P^H \subseteq A_K^H$ (by transitivity of the relative trace map), it suffices to prove that

$$t_P^H(B^P\gamma B^P) \subseteq f^H(A_P^H) + J(B^H)\,. \tag{25.10}$$

Since γ is a local point of B^P, its image $\overline{\gamma} = br_P^B(\gamma)$ is a point of $\overline{B}(P)$, by Lemma 14.5. In fact we use this lemma repeatedly to identify the points of $\overline{B}(P)$ with the local points of B^P. By (b), there exists $\overline{\gamma}^* \in \mathcal{P}(\overline{A}(P))$ such that $\overline{f}(P)(\overline{\gamma}^*) \subseteq \overline{\gamma}$ (Lemma 25.2), and $\overline{\gamma}^* = br_P^A(\gamma^*)$ where γ^* is a local point of A^P.

Writing $\overline{f} = \overline{f}(P)$ for simplicity, we have

$$\overline{f}(\overline{A}(P)\,\overline{\gamma}^*\,\overline{A}(P)) + J(\overline{B}(P)) = \overline{B}(P)\,\overline{\gamma}\,\overline{B}(P) + J(\overline{B}(P))$$

by Lemma 25.2. Since

$$J(\overline{B}(P)) = \sum_{\overline{\delta}\in\mathcal{P}(\overline{B}(P))} \big(\overline{B}(P)\,\overline{\delta}\,\overline{B}(P) \cap J(\overline{B}(P))\big)$$

by Proposition 4.14, we obtain

$$\overline{B}(P)\,\overline{\gamma}\,\overline{B}(P) \;\subseteq\; \overline{f}(\overline{A}(P)\,\overline{\gamma}^*\,\overline{A}(P)) \;+ \sum_{\overline{\delta}\in\mathcal{P}(\overline{B}(P))} \big(\overline{B}(P)\,\overline{\delta}\,\overline{B}(P) \cap J(\overline{B}(P))\big)\,.$$

We want to lift this to B^P. Clearly $br_P^B(B^P\gamma B^P) = \overline{B}(P)\,\overline{\gamma}\,\overline{B}(P)$ and

$$br_P^B(f^P(A^P\gamma^*A^P)) = \overline{f}\,br_P^A(A^P\gamma^*A^P) = \overline{f}(\overline{A}(P)\,\overline{\gamma}^*\,\overline{A}(P))\,.$$

Finally we also have

$$br_P^B\big(B^P\delta B^P \cap J(B^P)\big) = \overline{B}(P)\,\overline{\delta}\,\overline{B}(P) \cap J(\overline{B}(P))\,.$$

Indeed since $\pi_{\delta'}(B^P\delta B^P) = \{0\}$ for $\delta' \neq \delta$, we have $B^P\delta B^P \cap J(B^P) = B^P\delta B^P \cap \mathrm{Ker}(\pi_\delta)$ (and similarly for $\overline{\delta}$), and on restriction to $B^P\delta B^P$, π_δ is the composite surjection

$$B^P\delta B^P \xrightarrow{\;br_P^B\;} \overline{B}(P)\,\overline{\delta}\,\overline{B}(P) \xrightarrow{\;\pi_{\overline{\delta}}\;} S(\overline{\delta}) \cong S(\delta)\,.$$

Now we can lift the inclusion above to B^P. Since the points of $\overline{B}(P)$ lift to the local points of B^P, we obtain

$$B^P\gamma B^P \;\subseteq\; f^P(A^P\gamma^*A^P) \;+ \sum_{\delta\in\mathcal{LP}(B^P)} \big(B^P\delta B^P \cap J(B^P)\big) \;+\; \mathrm{Ker}(br_P^B)\,.$$

We apply t_P^H to this inclusion. First we have

$$t_P^H(f^P(A^P\gamma^*A^P)) = f^H(t_P^H(A^P\gamma^*A^P)) \;\subseteq\; f^H(A_P^H)\,.$$

By Lemma 25.8,

$$t_P^H\big(B^P\delta B^P \cap J(B^P)\big) \subseteq J(B^H) + \sum_{Q_\varepsilon < P_\delta} t_Q^H(B^Q\varepsilon B^Q) \subseteq J(B^H) + \sum_{Q<P} B_Q^H\,.$$

Finally $t_P^H(\mathrm{Ker}(br_P^B)) = t_P^H(\sum_{Q<P} t_Q^P(B^Q)) = \sum_{Q<P} B_Q^H$. Therefore we obtain

$$t_P^H(B^P\gamma B^P) \subseteq f^H(A_P^H) + J(B^H) + \sum_{Q<P} B_Q^H .$$

Since Q is a proper subgroup of P, it is a proper subgroup of K and the induction hypothesis applies. Therefore $B_Q^H \subseteq f^H(A_Q^H) + J(B^H)$ and it follows that

$$t_P^H(B^P\gamma B^P) \subseteq f^H(A_P^H) + \sum_{Q<P} f^H(A_Q^H) + J(B^H) \subseteq f^H(A_P^H) + J(B^H),$$

proving 25.10. □

The theorem gives a local characterization of covering exomorphisms. When $\mathcal{F}$ is known in advance to be unitary, the characterization also has the following form.

(25.11) COROLLARY. *Let $\mathcal{F} : A \to B$ be a unitary exomorphism of G-algebras. The following conditions are equivalent.*
(a) $\mathcal{F}$ is a covering exomorphism of G-algebras.
(b) For every local pointed group P_γ on A such that $\mathcal{F}(\gamma) \neq \{0\}$, there exists a local pointed group P_δ on B such that $\mathcal{F}(\gamma) \subseteq \delta$, and whenever two local pointed groups P_γ and $P_{\gamma'}$ on A satisfy $\mathcal{F}(\gamma) \subseteq \delta$ and $\mathcal{F}(\gamma') \subseteq \delta$, then $\gamma = \gamma'$.

If moreover these conditions are satisfied, then $\mathcal{F}$ is strict if and only if, for every local pointed group P_γ on A, we have $\mathcal{F}(\gamma) \neq \{0\}$.

Proof. Let P be a p-subgroup of G.

(a) ⇒ (b). This is an immediate consequence of Corollary 25.4, applied to the covering exomorphism of $\mathcal{O}$-algebras $\mathcal{F}^P : A^P \to B^P$. Note that by Proposition 25.6, if $\mathcal{F}(\gamma) \subseteq \delta$ (so that $\gamma = \delta^*$ in the notation of that proposition), then γ is local if and only if δ is local.

(b) ⇒ (a). We show that condition (b) of Theorem 25.9 is satisfied. To this end we are going to apply Corollary 25.4. Recall that the Brauer homomorphism br_P^A induces a bijection $\mathcal{LP}(A^P) \to \mathcal{P}(\overline{A}(P))$. Let $\overline{\gamma} \in \mathcal{P}(\overline{A}(P))$ such that $\overline{\mathcal{F}}(P)(\overline{\gamma}) \neq \{0\}$, and lift $\overline{\gamma}$ to $\gamma \in \mathcal{LP}(A^P)$. Since $br_P^B\mathcal{F}^P = \overline{\mathcal{F}}(P)br_P^A$, we have $\mathcal{F}(\gamma) \neq \{0\}$ (recall that the notation $\mathcal{F}(\gamma)$ stands for $\mathcal{F}^P(\gamma)$). By assumption, there is a local point δ of B^P such that $\mathcal{F}(\gamma) \subseteq \delta$, and it follows that

$$\overline{\mathcal{F}}(P)(\overline{\gamma}) = \overline{\mathcal{F}}(P)br_P^A(\gamma) = br_P^B\mathcal{F}^P(\gamma) \subseteq br_P^B(\delta) = \overline{\delta} .$$

Now if $\overline{\mathcal{F}}(P)(\overline{\gamma}) \subseteq \overline{\delta}$ and $\overline{\mathcal{F}}(P)(\overline{\gamma}') \subseteq \overline{\delta}$, then necessarily $\mathcal{F}(\gamma) \subseteq \delta$ and $\mathcal{F}(\gamma') \subseteq \delta$ (because by assumption $\mathcal{F}(\gamma)$ must be contained in a local point of B^P, which can only be δ, and similarly with γ'). Thus it follows from the assumption that $\gamma = \gamma'$, and therefore $\overline{\gamma} = \overline{\gamma}'$. This shows that the conditions of Corollary 25.4 are satisfied, so that $\overline{\mathcal{F}}(P)$ is a covering exomorphism of $\mathcal{O}$-algebras. By Theorem 25.9, $\mathcal{F}$ is a covering exomorphism of G-algebras.

The additional statement about strict covering exomorphisms is also a consequence of Corollary 25.4. □

Exercises

(25.1) Let $\mathcal{F} : A \to B$ and $\mathcal{G} : B \to C$ be two exomorphisms of G-algebras.

(a) If $\mathcal{F}$ and $\mathcal{G}$ are covering exomorphisms, then $\mathcal{GF}$ is also a covering exomorphism. Moreover $(\mathcal{GF})^* = \mathcal{F}^*\mathcal{G}^*$.

(b) If $\mathcal{GF}$ is a covering exomorphism, then $\mathcal{G}$ is also a covering exomorphism.

(c) If $\mathcal{GF}$ is a covering exomorphism and if $\mathcal{G}$ is a strict covering exomorphism, then $\mathcal{F}$ is also a covering exomorphism.

(25.2) Let $\mathcal{E}_A : A' \to A$ and $\mathcal{E}_B : B' \to B$ be two embeddings of G-algebras. Let $\mathcal{F} : A \to B$ and $\mathcal{F}' : A' \to B'$ be exomorphisms of G-algebras such that $\mathcal{F}\mathcal{E}_A = \mathcal{E}_B\mathcal{F}'$. Assume that $\mathcal{F}'$ is unitary. Prove that if $\mathcal{F}$ is a covering exomorphism, then $\mathcal{F}'$ is also a covering exomorphism. Moreover if $\mathcal{F}$ is strict then so is $\mathcal{F}'$.

(25.3) Prove statement (e) in Proposition 25.6.

(25.4) Let $\pi : L \to M$ be a surjective homomorphism of $\mathcal{O}G$-modules with L a projective $\mathcal{O}G$-module. Let A be the subalgebra of $\mathrm{End}_{\mathcal{O}}(L)$ consisting of all endomorphisms leaving $\mathrm{Ker}(\pi)$ invariant. Any $a \in A$ induces an endomorphism $\overline{a} \in \mathrm{End}_{\mathcal{O}}(M)$ such that $\overline{a}\,\pi = \pi\, a$. Prove that this defines a map $A \to \mathrm{End}_{\mathcal{O}}(M)$ which is a strict covering homomorphism. [Hint: Show first that $\mathrm{Res}^G_H(L)$ is a projective $\mathcal{O}H$-module for every subgroup H of G.]

(25.5) Let $\mathcal{F} : A \to B$ be an exomorphism of G-algebras and assume that p does not divide $|G|$. Prove that $\mathcal{F}$ is a covering exomorphism of G-algebras if and only if $\mathrm{Res}^G_1(\mathcal{F})$ is a covering exomorphism of $\mathcal{O}$-algebras.

(25.6) Let $\mathcal{F} : A \to B$ be a covering exomorphism of G-algebras, let H_α be a pointed group on B, let H_{α^*} be the corresponding pointed group on A, and let K be a subgroup of H. Prove that $\alpha \subseteq B_K^H$ if and only if $\alpha^* \subseteq A_K^H$.

Notes on Section 25

Covering exomorphisms have been introduced by Puig [1988b] and all the results of this section are due to him. In fact Puig treated more generally a relative situation where the exomorphism is only required to "cover" the points which are not projective relative to some fixed set of local points.

Lemma 25.5 raises the question of the invariance of the Jacobson radical under the relative trace map (which certainly does not hold in general, see Exercise 11.3). For an arbitrary G-algebra, there is a necessary and sufficient criterion for the inclusion $t_H^G(J(A^H)) \subseteq J(A^G)$, which is proved by Thévenaz [1988b] (in terms of defect multiplicity modules).

CHAPTER 5

Modules and diagrams

An important source of examples of interior G-algebras is provided by modules over group algebras, which we discuss in this chapter. We start with the parametrization of indecomposable modules with three invariants. Then we develop the theory of two important classes of modules: p-permutation modules and endo-permutation modules. For a fixed p-group P, all endo-permutation modules can be organized into an abelian group, called the Dade group of P. We discuss properties of this group. Then we prove that source modules of simple modules are endo-permutation modules when G is a p-soluble group.

As the theory of modules immediately generalizes to the case of diagrams, we discuss this more general concept. Short exact sequences are interesting examples of diagrams and we focus our attention on the important class of almost split sequences. We prove their existence by exhibiting a suitable duality involving the corresponding G-algebras. This duality takes a different form over a field and over a complete discrete valuation ring. We discuss a few properties of almost split sequences related to induction and restriction. Finally we determine a defect group of an almost split sequence and this provides an excellent illustration of the theory of G-algebras in action.

We continue with our assumption that G is a finite group and that $\mathcal{O}$ is a commutative complete local noetherian ring with an algebraically closed residue field k of characteristic p.

§ 26 THE PARAMETRIZATION OF INDECOMPOSABLE MODULES

With any indecomposable $\mathcal{O}G$-lattice L are associated three invariants: a defect group, a source module, and a defect multiplicity module. The purpose of this section is to show essentially that these three invariants characterize L and that any given choice of three such invariants gives rise to an indecomposable $\mathcal{O}G$-lattice. In other words indecomposable $\mathcal{O}G$-lattices can be parametrized by these three invariants. One obtains in this way a reduction to the case of an indecomposable module over a p-group (the source module) and an indecomposable projective module (the defect multiplicity module). At the end of this section, we prove that the third invariant has an interesting property: the defect multiplicity module of a simple module is again simple (and projective).

The parametrization of indecomposable $\mathcal{O}G$-lattices is part of a more general result which describes the parametrization of arbitrary primitive interior G-algebras in terms of their defect group, source algebra, and defect multiplicity module. However, further complications arise and for this reason we only discuss here the easier case of $\mathcal{O}G$-lattices (see Remark 26.6).

We first fix the notation. Let L be an indecomposable $\mathcal{O}G$-lattice and let $A = \mathrm{End}_{\mathcal{O}}(L)$ be the corresponding primitive interior G-algebra. If P_γ is a defect of A, then P is a vertex of L and γ corresponds to an indecomposable direct summand M of $\mathrm{Res}^G_P(L)$ (up to isomorphism), namely a source of L. Let $C = \mathrm{End}_{\mathcal{O}}(\mathrm{Ind}^G_P(M)) \cong \mathrm{Ind}^G_P(\mathrm{End}_{\mathcal{O}}(M))$. By Proposition 18.9 there exists at least one embedding $\mathcal{F} : A \to C$ and by Proposition 12.5 this embedding is unique, because we are dealing with $\mathcal{O}G$-lattices. In terms of modules, this corresponds to the fact that L is isomorphic to a direct summand of $\mathrm{Ind}^G_P(M)$.

If $P_{\gamma'}$ denotes the image of P_γ under this embedding (Proposition 15.1), then γ' corresponds to an indecomposable direct summand M' of $\mathrm{Res}^G_P \mathrm{Ind}^G_P(M)$ (up to isomorphism). In terms of modules, the direct summand M of $\mathrm{Res}^G_P(L)$ is isomorphic to the direct summand M' of $\mathrm{Res}^G_P \mathrm{Ind}^G_P(M)$. We know from Proposition 15.1 that $N_G(P_\gamma) = N_G(P_{\gamma'})$ and in fact this group is simply the inertial subgroup of M (or M'), that is, the subgroup $N_G(P, M)$ of all $x \in N_G(P)$ such that M is isomorphic to the conjugate module ${}^xM$ (see Example 13.4). We shall from now on identify the pointed groups on A with pointed groups on C via the unique embedding $\mathcal{F} : A \to C$. Thus we write $\gamma' = \gamma$.

We let $V_A(\gamma)$ be the multiplicity module of γ viewed as a pointed group on A and we let $V_C(\gamma)$ be the multiplicity module of γ viewed as a pointed group on C. By definition $V_A(\gamma)$ is the defect multiplicity module of A (that is, of L) and is indecomposable projective. But for the moment we shall only work with $V_C(\gamma)$ and we shall come back later to its connection with $V_A(\gamma)$. We let $\widehat{\overline{N}}_G(P_\gamma)$ be the central extension associated with $V_C(\gamma)$, so that $V_C(\gamma)$ has a module structure over the twisted group algebra $k_\sharp\widehat{\overline{N}}_G(P_\gamma)$.

We first prove the crucial fact that the multiplicity module $V_C(\gamma)$ is free of rank one. For this result one does not need to restrict to the case of lattices, so we replace $\mathrm{End}_{\mathcal{O}}(M)$ by a primitive interior P-algebra B and we work with the interior G-algebra $C = \mathrm{Ind}_P^G(B)$. As usual, we also write $\overline{N} = \overline{N}_G(P_\gamma)$ and consequently $\widehat{\overline{N}} = \widehat{\overline{N}}_G(P_\gamma)$.

(26.1) LEMMA. *Let P be a p-subgroup of G and let $C = \mathrm{Ind}_P^G(B)$, where B is a primitive interior P-algebra such that $\{1_B\}$ is a local point of B^P. Let γ be the point of C^P containing $1 \otimes 1_B \otimes 1$ (that is, the image of the unique point $\{1_B\}$ of B^P under the canonical embedding $\mathcal{D}_P^G : B \to \mathrm{Res}_P^G \mathrm{Ind}_P^G(B) = \mathrm{Res}_P^G(C)$). Then the multiplicity module $V_C(\gamma)$ of γ is free of rank one as a module over the twisted group algebra $k_\sharp\widehat{\overline{N}}_G(P_\gamma)$.*

Proof. Let $S(\gamma) \cong \mathrm{End}_k(V_C(\gamma))$ be the multiplicity algebra of γ and let $\pi_\gamma : C^P \to S(\gamma)$ be the canonical map. Let $i = 1 \otimes 1_B \otimes 1 \in \gamma$, so that $\pi_\gamma(i)$ is a primitive idempotent of $S(\gamma)$. By construction of induced algebras, we have $1_C = t_P^G(i)$ and the decomposition $1_C = \sum_{g \in [G/P]} {}^g i$ is orthogonal. Since $\{1_B\}$ is local by assumption, γ is also local (Proposition 15.1) and therefore Proposition 14.7 applies. We obtain

$$1_{S(\gamma)} = \pi_\gamma\, r_P^G(1_C) = \pi_\gamma\, r_P^G(t_P^G(i)) = t_1^{\overline{N}}(\pi_\gamma(i))$$

where $\overline{N} = \overline{N}_G(P_\gamma)$. The decomposition $1_{S(\gamma)} = \sum_{\overline{g} \in \overline{N}} {}^{\overline{g}}(\pi_\gamma(i))$ is primitive and orthogonal, because on the one hand $\pi_\gamma(i)$ is primitive in $S(\gamma)$ and primitivity is preserved by conjugation, and on the other hand ${}^{\overline{g}}(\pi_\gamma(i)) = \pi_\gamma({}^g i)$ and the idempotents ${}^g i$ are orthogonal. Therefore by Proposition 1.14 the multiplicity module $V_C(\gamma)$ decomposes, as k-vector space, as a direct sum of one-dimensional subspaces

$$V_C(\gamma) = \bigoplus_{\overline{g} \in \overline{N}} {}^{\overline{g}}(\pi_\gamma(i)) V_C(\gamma),$$

and so $\pi_\gamma(i)V_C(\gamma) = kw$ for some $w \in (\pi_\gamma(i))V_C(\gamma)$. By definition of the central extension $\widehat{\overline{N}}$ of $\overline{N}$, the action of $\overline{N}$ on $S(\gamma)$ lifts to a group homomorphism $\rho : \widehat{\overline{N}} \to S(\gamma)^*$ such that $\rho(\widehat{\overline{g}})\, s\, \rho(\widehat{\overline{g}}^{-1}) = {}^{\overline{g}}s$ for all $s \in S(\gamma)$; here it is understood that $\widehat{\overline{g}} \in \widehat{\overline{N}}$ maps to $\overline{g} \in \overline{N}$. Thus

$${}^{\overline{g}}(\pi_\gamma(i))V_C(\gamma) = \rho(\widehat{\overline{g}})\pi_\gamma(i)\rho(\widehat{\overline{g}}^{-1})V_C(\gamma) = \rho(\widehat{\overline{g}})\pi_\gamma(i)V_C(\gamma) = \rho(\widehat{\overline{g}})kw,$$

and therefore

$$V_C(\gamma) = \bigoplus_{\overline{g}\in\overline{N}} \rho(\widehat{\overline{g}})kw\,,$$

which proves that $V_C(\gamma)$ is generated as a module over the twisted group algebra $k_\sharp\widehat{\overline{N}}$ by the single element w. Moreover the surjective homomorphism of $k_\sharp\widehat{\overline{N}}$-modules

$$k_\sharp\widehat{\overline{N}} \longrightarrow V_C(\gamma)\,, \qquad \widehat{\overline{g}} \mapsto \rho(\widehat{\overline{g}})w$$

is an isomorphism because both modules are k-vector spaces of the same dimension, namely $|\overline{N}|$. □

(26.2) REMARK. If the $\overline{N}$-algebra $S(\gamma)$ happens to be interior, so that $V_C(\gamma)$ is a module over the ordinary group algebra $k\overline{N}$, then there is another way of viewing Lemma 26.1. Indeed we first proved above that $1_{S(\gamma)} = \sum_{\overline{g}\in\overline{N}} {}^{\overline{g}}(\pi_\gamma(i))$ is a primitive orthogonal decomposition and by Proposition 16.6 this implies that

$$S(\gamma) \cong \mathrm{Ind}_1^{\overline{N}}(\pi_\gamma(i)S(\gamma)\pi_\gamma(i))\,.$$

Now $S(\gamma) \cong \mathrm{End}_k(V_C(\gamma))$ and $\pi_\gamma(i)S(\gamma)\pi_\gamma(i) \cong \mathrm{End}_k(\pi_\gamma(i)V_C(\gamma)) = \mathrm{End}_k(kw)$. Therefore by Example 16.4 we get

$$\mathrm{End}_k(V_C(\gamma)) \cong \mathrm{Ind}_1^{\overline{N}}(\mathrm{End}_k(kw)) \cong \mathrm{End}_k(\mathrm{Ind}_1^{\overline{N}}(kw))\,,$$

which expresses the fact that $V_C(\gamma) \cong \mathrm{Ind}_1^{\overline{N}}(kw)$, that is, $V_C(\gamma)$ is free of rank one over $k\overline{N}$. It is possible to generalize this approach to the more general situation of the lemma: using the notion of interior $\widehat{\overline{N}}$-algebra given in Example 10.4 (so that $S(\gamma)$ becomes interior in that sense), one can define induction for such algebras and then prove the properties of induction used above, following ideas which are entirely similar to the case of ordinary interior algebras.

For a fixed p-subgroup P and a fixed indecomposable $\mathcal{O}P$-lattice M with vertex P, let $\Lambda_\mathcal{O}(G,P,M)$ be the set of isomorphism classes of all $\mathcal{O}G$-lattices L with vertex P and source M. We first consider the problem of parametrizing the set $\Lambda_\mathcal{O}(G,P,M)$. The discussion at the beginning of this section shows that every such lattice L is isomorphic to a direct summand of $\mathrm{Ind}_P^G(M)$, so that we have to work within the interior G-algebra $C = \mathrm{End}_\mathcal{O}(\mathrm{Ind}_P^G(M))$. This shows in particular that $\Lambda_\mathcal{O}(G,P,M)$ is a finite set.

Let γ be the point of C^P corresponding to the direct summand M of $\mathrm{Res}^G_P \mathrm{Ind}^G_P(M)$. We first note that γ is local because M has vertex P by assumption (see Proposition 18.11). Any $\mathcal{O}G$-lattice L with vertex P and source M is isomorphic to a direct summand of $\mathrm{Ind}^G_P(M)$, hence corresponds to a point α_L of C^G. The requirement that L has vertex P and source M is equivalent to the condition that G_{α_L} has defect pointed group P_γ (see Example 13.4 and Proposition 18.11). Via the Puig correspondence with respect to P_γ, the point α_L corresponds to a point $\delta \in \mathcal{P}(S(\gamma)^{\overline{N}_G(P_\gamma)})$ such that $\overline{N}_G(P_\gamma)_\delta$ is projective, or in other words to an indecomposable projective direct summand W_L (up to isomorphism) of the multiplicity module $V_C(\gamma)$. We shall simply refer to W_L as the Puig correspondent of L. We obtain in this way the parametrization of $\Lambda_{\mathcal{O}}(G,P,M)$ we are looking for.

(26.3) PROPOSITION. *Let P be a p-subgroup of G, let M be an indecomposable $\mathcal{O}P$-lattice with vertex P, let $C = \mathrm{End}_{\mathcal{O}}(\mathrm{Ind}^G_P(M))$, and let γ be the (local) point of C^P corresponding to the direct summand M of $\mathrm{Res}^G_P \mathrm{Ind}^G_P(M)$. The Puig correspondence with respect to P_γ induces a bijection $L \mapsto W_L$ between $\Lambda_{\mathcal{O}}(G,P,M)$ and the set $\mathrm{Proj}(k_\sharp \widehat{\overline{N}}_G(P_\gamma))$ of isomorphism classes of indecomposable projective $k_\sharp \widehat{\overline{N}}_G(P_\gamma)$-modules.*

Proof. The map $L \mapsto \alpha_L$ defined above induces a bijection

$$\Lambda_{\mathcal{O}}(G,P,M) \xrightarrow{\sim} \{\alpha \in \mathcal{P}(C^G) \mid P_\gamma \text{ is a defect of } G_\alpha\}.$$

Now the Puig correspondence (Theorem 19.1) is a bijection between the sets

$$\{\alpha \in \mathcal{P}(C^G) \mid P_\gamma \text{ is a defect of } G_\alpha\} \qquad \text{and}$$

$$\{\delta \in \mathcal{P}(S(\gamma)^{\overline{N}_G(P_\gamma)}) \mid \overline{N}_G(P_\gamma)_\delta \text{ is projective}\},$$

and the latter set is in bijection with the set of isomorphism classes of indecomposable projective direct summands of the multiplicity module $V_C(\gamma)$. But since $V_C(\gamma)$ is free of rank one by Lemma 26.1, this set is just the set $\mathrm{Proj}(k_\sharp \widehat{\overline{N}}_G(P_\gamma))$ of all isomorphism classes of indecomposable projective $k_\sharp \widehat{\overline{N}}_G(P_\gamma)$-modules. □

Now we explain the connection between W_L and the defect multiplicity module of L. In terms of interior G-algebras, the fact that L is isomorphic to a direct summand of $\mathrm{Ind}^G_P(M)$ corresponds to the fact that there is an embedding $\mathcal{F} : A \to C$, where $A = \mathrm{End}_{\mathcal{O}}(L)$. Moreover this embedding is unique (Proposition 12.5). Recall that we identify the pointed groups on A with pointed groups on C via the unique embedding $\mathcal{F}$. In particular the defect pointed group P_γ on A is identified with the pointed group P_γ on C appearing in Proposition 26.3. By Proposition 15.3 and Corollary 15.5, the embedding $\mathcal{F} : A \to C$ induces an embedding $\overline{\mathcal{F}}(\gamma)$ of multiplicity algebras as well as an isomorphism $\overline{\mathcal{F}}(\gamma)^*$ of central extensions

$$\overline{\mathcal{F}}(\gamma) : \mathrm{End}_k(V_A(\gamma)) \longrightarrow \mathrm{End}_k(V_C(\gamma)) \, , \qquad \overline{\mathcal{F}}(\gamma)^* : \hat{\overline{N}}_G(P_\gamma) \xrightarrow{\sim} \hat{\overline{N}}{}^A_G(P_\gamma) \, .$$

where $\hat{\overline{N}}{}^A_G(P_\gamma)$ denotes the central extension associated with $\mathrm{End}_k(V_A(\gamma))$ while $\hat{\overline{N}}_G(P_\gamma)$ is the central extension associated with $\mathrm{End}_k(V_C(\gamma))$ as before. The multiplicity module $V_A(\gamma)$ (that is, the defect multiplicity module of A, or of L) is by definition a module over $k_\sharp\hat{\overline{N}}{}^A_G(P_\gamma)$, but it can be viewed as a module over $k_\sharp\hat{\overline{N}}_G(P_\gamma)$ by means of the isomorphism $\overline{\mathcal{F}}(\gamma)^*$. In this way $V_A(\gamma)$ becomes isomorphic (as a $k_\sharp\hat{\overline{N}}_G(P_\gamma)$-module) to a direct summand of $V_C(\gamma)$. Moreover by Exercise 19.1 this direct summand is precisely W_L. Thus W_L is isomorphic to $V_A(\gamma)$, provided we view $V_A(\gamma)$ as a module over $k_\sharp\hat{\overline{N}}_G(P_\gamma)$ rather than a module over $k_\sharp\hat{\overline{N}}{}^A_G(P_\gamma)$.

Since the central extension $\hat{\overline{N}}_G(P_\gamma)$ is constructed from $\mathrm{Ind}_P^G(M)$, we shall say that $\hat{\overline{N}}_G(P_\gamma)$ is the central extension *determined* by $\mathrm{Ind}_P^G(M)$ and that the $k_\sharp\hat{\overline{N}}_G(P_\gamma)$-module structure on $V_A(\gamma)$ is the module structure *determined* by $\mathrm{Ind}_P^G(M)$. Since the embedding $\mathcal{F} : A \to C$ is unique, the isomorphism $\overline{\mathcal{F}}(\gamma)^*$ is uniquely determined and therefore the module structure on $V_A(\gamma)$ determined by $\mathrm{Ind}_P^G(M)$ is also uniquely determined. The distinction between the two isomorphic groups $\hat{\overline{N}}{}^A_G(P_\gamma)$ and $\hat{\overline{N}}_G(P_\gamma)$ is quite important and will be explained after the proof of the main theorem.

Now we introduce the notation for the main result about the parametrization of indecomposable $\mathcal{O}G$-lattices. In order to emphasize that we are dealing with modules, we shall use the notation $N_G(P,M)$ for the inertial subgroup of M, instead of $N_G(P_\gamma)$. Let $\Lambda_\mathcal{O}(G)$ be the set of isomorphism classes of indecomposable $\mathcal{O}G$-lattices. Let $\Pi_\mathcal{O}(G)$ be the set of triples (P,M,V) where P is a p-subgroup of G, M is an isomorphism class of indecomposable $\mathcal{O}P$-modules with vertex P, and V is an isomorphism class of indecomposable projective $k_\sharp\hat{\overline{N}}_G(P,M)$-modules, with respect to the inertial group $N_G(P,M)$ and the twisted group algebra $k_\sharp\hat{\overline{N}}_G(P,M)$ determined by $\mathrm{Ind}_P^G(M)$. For simplicity we view M and V as modules rather than isomorphism classes. The group G acts by conjugation on $\Pi_\mathcal{O}(G)$ and we are interested in the set of orbits $G\backslash\Pi_\mathcal{O}(G)$. Note that the stabilizer of the triple (P,M,V) is the group $N_G(P,M)$ (which is also the stabilizer of the pair (P,M)).

(26.4) THEOREM. *There is a bijection* $\Lambda_{\mathcal{O}}(G) \to G\backslash\Pi_{\mathcal{O}}(G)$ *which is described as follows.*

(a) With an indecomposable $\mathcal{O}G$*-lattice* L *is associated the* G*-orbit of triples* (P, M, V)*, where* P *is a vertex of* L*,* M *is a source of* L *(up to isomorphism), and* V *is a defect multiplicity module of* L *(up to isomorphism) with its module structure determined by* $\mathrm{Ind}_P^G(M)$*.*

(b) With the G*-orbit of a triple* (P, M, V) *is associated the isomorphism class of direct summands of* $\mathrm{Ind}_P^G(M)$ *corresponding to the point of* $\mathrm{End}_{\mathcal{O}G}(\mathrm{Ind}_P^G(M))$ *which is the Puig correspondent of the module* V *(where the Puig correspondence is taken with respect to* (P, M) *).*

Proof. It is clear that the map in (a) is well-defined since we know that the pair (P, M) (corresponding to a defect pointed group P_γ of $\mathrm{End}_{\mathcal{O}}(L)$) is unique up to G-conjugation. To show that the map in (b) is also well-defined, we first note that if $x \in G$, then $\mathrm{Ind}_{^xP}^G({}^xM) \cong \mathrm{Ind}_P^G(M)$. If P_γ is the pointed group on $\mathrm{End}_{\mathcal{O}}(\mathrm{Ind}_P^G(M))$ corresponding to the $\mathcal{O}P$-direct summand M, then ${}^x(P_\gamma)$ corresponds to the $\mathcal{O}({}^xP)$-direct summand ${}^xM$. We have to show that the Puig correspondent of V with respect to P_γ is the same as the Puig correspondent of ${}^xV$ with respect to ${}^x(P_\gamma)$. But the Puig correspondence is induced by $\pi_\gamma\, r_P^G$ and there is a commutative diagram

$$\begin{array}{ccccc}
C^G & \xrightarrow{r_P^G} & C^P & \xrightarrow{\pi_\gamma} & S(\gamma) \\
{\scriptstyle \mathrm{Conj}(x)}\downarrow & & \downarrow{\scriptstyle \mathrm{Conj}(x)} & & \downarrow{\scriptstyle \mathrm{Conj}(x)} \\
C^G & \xrightarrow{r_{^xP}^G} & C^{^xP} & \xrightarrow{\pi_{^x\gamma}} & S({}^x\gamma)
\end{array}$$

where $C = \mathrm{End}_{\mathcal{O}}(\mathrm{Ind}_P^G(M))$; the claim follows since $\mathrm{Conj}(x) = \mathrm{Inn}(x\cdot 1_C)$ induces the identity on $\mathcal{P}(C^G)$.

We choose a set X of representatives of the G-orbits of pairs (P, M), where P is a p-subgroup of G and M is an isomorphism class of indecomposable $\mathcal{O}P$-modules with vertex P. We have

$$\Lambda_{\mathcal{O}}(G) \;=\; \bigcup_{(P,M)\in X} \Lambda_{\mathcal{O}}(G, P, M) \qquad \text{and}$$

$$G\backslash\Pi_{\mathcal{O}}(G) \;\cong\; \bigcup_{(P,M)\in X} \mathrm{Proj}(k_\sharp\widehat{\overline{N}}_G(P, M)) .$$

As noted in the discussion following Proposition 26.3, the defect multiplicity module V of L is isomorphic to the Puig correspondent W_L (appearing in Proposition 26.3), provided V is viewed with its module structure determined by $\mathrm{Ind}_P^G(M)$. It follows that the map $\Lambda_{\mathcal{O}}(G) \to G\backslash\Pi_{\mathcal{O}}(G)$

(which is well-defined by the above observations) is obtained as the disjoint union of the bijections

$$\Lambda_{\mathcal{O}}(G,P,M) \xrightarrow{\sim} \mathrm{Proj}(k_\sharp \widehat{\overline{N}}_G(P,M))$$

of Proposition 26.3. The result follows. □

There is an important but subtle point which has to be underlined and which explains why we have distinguished between two isomorphic central extensions, so that a defect multiplicity module has both a natural structure and a structure determined by the induction of the source. It may happen that two non-isomorphic indecomposable $\mathcal{O}G$-lattices L and L' have the same vertex, the same source, and isomorphic defect multiplicity algebras. One may be tempted to conclude that this contradicts the theorem, because every multiplicity module is uniquely constructed from the corresponding multiplicity algebra, so that the defect multiplicity modules of L and L' should be isomorphic. But one has to remember that with each multiplicity algebra is constructed a central extension, hence a twisted group algebra, and therefore the defect multiplicity modules of L and L' are modules over two distinct twisted group algebras. Thus one has first to find an isomorphism between the central extensions before one can view the multiplicity modules as modules over the same algebra.

The way to achieve this is to view all multiplicity modules as modules over a single central extension, that is, with their module structure determined by the induction of the source. Consequently the vertex, the source and the multiplicity algebra are not sufficient to determine the isomorphism class of an $\mathcal{O}G$-lattice L, but one needs the extra information coming from the embedding of L into $\mathrm{Ind}_P^G(M)$, this information being contained in the defect multiplicity module *with its structure determined by* $\mathrm{Ind}_P^G(M)$. The following simple example illustrates this point as well as another subtlety of the constructions above. The example is small enough to allow us to write down everything explicitly, but the details of the calculations are left to the reader.

(26.5) EXAMPLE. Let $G = S_3$ be the symmetric group on 3 letters, generated by an element u of order 3 and an element s of order 2. We take a field k of characteristic 3. There are two indecomposable kG-modules L and L' of dimension 2. The top composition factor of L is the trivial representation and its socle is the sign representation, while the opposite holds for L'. Both L and L' restrict to the same 2-dimensional module M for $P = < u >$, which is a source of both modules. In matrix terms, we have

$$u \mapsto \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad , \qquad s \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

for L, and the same for L' with a change of sign for the image of s. Let $A = \mathrm{End}_k(L)$ and $A' = \mathrm{End}_k(L')$. In both cases the unique point $\gamma = \{1\}$ of $A^P = A'^P$ (corresponding to the source module M) has a multiplicity algebra $\mathrm{End}_k(V_A(\gamma))$ isomorphic to k, and we have $N_G(P, M) = G$ and $\overline{N}_G(P, M) = C_2$, the cyclic group of order 2. Thus in both cases we have $GL(V_A(\gamma)) = k^*$ and $PGL(V_A(\gamma)) = 1$, so that by Example 10.8 both central extensions are determined by the following pull-back.

$$\begin{array}{ccc} \widehat{C}_2 = k^* \times C_2 & \longrightarrow & C_2 \\ \Big\downarrow{\scriptstyle \widehat{\rho}} & & \Big\downarrow \\ k^* & \longrightarrow & 1 \end{array}$$

Despite the fact that our two one-dimensional multiplicity algebras are canonically isomorphic, we do not identify the corresponding central extensions, but we use two different isomorphisms with the central extension determined by $\mathrm{Ind}_P^G(M)$ (which correspond to the two embeddings $L \to \mathrm{Ind}_P^G(M)$ and $L' \to \mathrm{Ind}_P^G(M)$). With their structure determined by $\mathrm{Ind}_P^G(M)$, the two multiplicity modules are now distinguished by a sign: since the central extension $\widehat{C}_2$ splits, the twisted group algebra $k_\sharp \widehat{C}_2$ is isomorphic to the ordinary group algebra kC_2 and the two possible multiplicity modules are the trivial and the sign representations of C_2 (which are indeed projective modules since the characteristic is 3). One of these corresponds to L and the other one to L'.

There is another subtle point which we want to emphasize. The two kG-modules L and L' now correspond respectively to each of the two distinct one-dimensional representations of $k_\sharp \widehat{C}_2$, in a uniquely determined fashion. However, one cannot say which is the trivial and which is the sign representation, because this depends on the isomorphism $k_\sharp \widehat{C}_2 \cong kC_2$. Indeed the twisted group algebra $k_\sharp \widehat{C}_2$ has no canonical basis and is isomorphic to the ordinary group algebra kC_2 in two different ways, which swap the role of the trivial and the sign representations. This phenomenon is in fact not surprising in view of the complete symmetry between L and L'.

(26.6) REMARK. There is a parametrization of primitive interior G-algebras which is similar to the parametrization of $\mathcal{O}G$-lattices and which contains it as a special case. Let A be a primitive interior G-algebra with defect group P and source algebra B. Then A always embeds into $C = \mathrm{Ind}_P^G(B)$, but the difficulty comes from the fact that there may be several such embeddings. Accordingly the defect multiplicity module of A is endowed with several module structures "determined" by $\mathrm{Ind}_P^G(B)$.

One can show that this family of modules is a single orbit under some natural action of the group $\mathrm{Out}(C)$ of outer automorphisms of C. Thus one obtains a parametrization of primitive interior G-algebras with three invariants $(P, B, \mathcal{V})$ (up to G-conjugation), where P is a defect group, B is a source algebra (up to isomorphism), and $\mathcal{V}$ is an orbit of multiplicity modules. Alternatively, one can also view the parametrization slightly differently, by defining equivalence classes of triples (P, B, V), where V is now a multiplicity module (not an orbit). The equivalence relation involves both isomorphism and G-conjugation.

The parametrization of $\mathcal{O}G$-lattices follows as a special case by considering only those primitive interior G-algebras of the form $\mathrm{End}_{\mathcal{O}}(L)$ where L is an indecomposable $\mathcal{O}G$-lattice (using the fact that $\mathrm{End}_{\mathcal{O}}(L)$ determines L by Lemma 10.7). This case is much easier because C is now $\mathcal{O}$-simple and hence $\mathrm{Out}(C) = 1$ by the Skolem–Noether theorem 7.2, so that there is just a single defect multiplicity module to consider. On the other hand there is a unique embedding $A \to C$ (Proposition 12.5) and this was used in a crucial way in the proof of the main result above.

(26.7) REMARK. The Green correspondence for $\mathcal{O}G$-lattices is a consequence of the parametrization above. Indeed for a fixed vertex P and a fixed source M, consider a subgroup $H \geq N_G(P, M)$. Then there is a bijection between the set of isomorphism classes of indecomposable $\mathcal{O}G$-lattices with vertex P and source M and the set of isomorphism classes of indecomposable $\mathcal{O}H$-lattices with vertex P and source M, because both sets are in bijection with the set of isomorphism classes of indecomposable projective $k_\sharp \widehat{\overline{N}}_G(P, M)$-modules. In short one can say that Green correspondents have the same three invariants. One can check easily that the correspondence obtained in this way coincides with the Green correspondence of Section 20 (Exercise 26.3). For the detailed proof of these facts one needs to identify the central extension $\widehat{\overline{N}}_G(P, M)$ constructed from $\mathrm{Ind}_P^G(M)$ and the central extension constructed from $\mathrm{Ind}_P^H(M)$. In order to achieve this, notice that the embedding

$$\mathrm{End}_{\mathcal{O}}(\mathrm{Ind}_P^H(M)) \longrightarrow \mathrm{End}_{\mathcal{O}}(\mathrm{Res}_H^G \mathrm{Ind}_P^G(M))$$

always induces an embedding between the two multiplicity algebras of the pointed group P_γ corresponding to (P, M), but this embedding is here an *exo-isomorphism*, thanks to Lemma 26.1.

For simple kG-modules, the three invariants appearing in the parametrization have further interesting properties. We shall come back later in Section 30 to sources of simple modules, but we prove now a result about the third invariant of the parametrization. This result asserts that a defect multiplicity module of a simple kG-module is again simple (and projective) over $k_\sharp\widehat{\overline{N}}_G(P,M)$. The defect multiplicity module has either a natural structure or a structure determined by the source, but clearly the property of being simple is independent of the way we view the defect multiplicity module.

If L is a simple kG-module, then $\mathrm{End}_{kG}(L) \cong k$ by Schur's lemma. More generally we consider $\mathcal{O}G$-lattices L such that $\mathrm{End}_{\mathcal{O}G}(L) \cong \mathcal{O}$.

(26.8) PROPOSITION. *Let L be an indecomposable $\mathcal{O}G$-lattice with vertex P and source M, and let V be the defect multiplicity module of L corresponding to (P,M). If $\mathrm{End}_{\mathcal{O}G}(L) \cong \mathcal{O}$, then V is simple (and projective) as a module over $k_\sharp\widehat{\overline{N}}_G(P,M)$.*

Proof. Let $A = \mathrm{End}_{\mathcal{O}}(L)$, so that $A^G \cong \mathcal{O}$ by assumption. Let γ be the point of A^P corresponding to M, so that $V = V(\gamma)$ and $N_G(P,M) = N_G(P_\gamma)$. The homomorphism $\pi_\gamma r_P^G : A^G \to S(\gamma)^{\overline{N}_G(P_\gamma)}$ is surjective by Theorem 19.2. Therefore $S(\gamma)^{\overline{N}_G(P_\gamma)} \cong k$, because k is the only non-zero quotient of $\mathcal{O}$ which is annihilated by $\mathfrak{p}$. In other words

$$\mathrm{End}_{k_\sharp\widehat{\overline{N}}_G(P_\gamma)}(V) \cong k\,.$$

But V is indecomposable projective (Theorem 19.2) and any twisted group algebra is a symmetric algebra (Example 10.4). Therefore, by Proposition 6.8, $\mathrm{Soc}(V) \cong V/J(V)$, and it follows that there exists an endomorphism ϕ of V with kernel $J(V)$ and image $\mathrm{Soc}(V)$. But since the endomorphism ring of V consists only of scalars, ϕ is just multiplication by some scalar, which must be non-zero because $\phi \neq 0$. Therefore ϕ is an isomorphism. It follows that $J(V) = 0$ and that $V = \mathrm{Soc}(V)$ is simple. □

The proposition applies in two cases of interest. Firstly, taking $\mathcal{O} = k$, then any simple kG-module L satisfies the assumption $\mathrm{End}_{kG}(L) \cong k$. Secondly, if $\mathcal{O}$ is a complete discrete valuation ring with field of fractions K, the assumption of the proposition holds for any $\mathcal{O}G$-lattice L such that $K \otimes_{\mathcal{O}} L$ is an absolutely simple KG-module. Indeed by Proposition 1.11, we have $\mathrm{End}_{KG}(K \otimes_{\mathcal{O}} L) \cong K$, so that $\mathrm{End}_{\mathcal{O}G}(L)$ is isomorphic to a subring of K containing $\mathcal{O}$ (because any $\mathcal{O}G$-linear endomorphism of L induces a KG-linear endomorphism of $K \otimes_{\mathcal{O}} L$). But $\mathcal{O}$ is the only possibility since the subring must be finitely generated over $\mathcal{O}$ and $\mathcal{O}$ is integrally closed (because $\mathcal{O}$ is a principal ideal domain). Therefore $\mathrm{End}_{\mathcal{O}G}(L) \cong \mathcal{O}$ and the proposition applies.

As it will be useful to know the existence of projective simple modules for ordinary group algebras (rather than twisted group algebras), we restrict to the normal subgroup $\overline{C}_G(P) = PC_G(P)/P$. Recall from Section 13 that, on restriction to $\overline{C}_G(P)$ and because P is a p-group, the multiplicity module V is endowed with a module structure over the ordinary group algebra $k\overline{C}_G(P)$.

(26.9) COROLLARY. *Under the assumptions of Proposition 26.8, the* $k\overline{C}_G(P)$*-module* $\mathrm{Res}^{\overline{N}_G(P,M)}_{\overline{C}_G(P)}(V)$ *is a direct sum of projective simple submodules.*

Proof. This is an immediate consequence of the following more general lemma. □

(26.10) LEMMA. *Let* H *be a subgroup of* G *, let* $k_\sharp\widehat{G}$ *be a twisted group algebra, and let* M *be a* $k_\sharp\widehat{G}$*-module.*

(a) If M *is projective, then* $\mathrm{Res}^G_H(M)$ *is a projective* $k_\sharp\widehat{H}$*-module.*

(b) If M *is simple and* H *is a normal subgroup of* G *, then* $\mathrm{Res}^G_H(M)$ *is a semi-simple* $k_\sharp\widehat{H}$*-module.*

Proof. (a) Since the restriction commutes with direct sums, it suffices to prove the result if M is free of rank one, that is, $M \cong k_\sharp\widehat{G}$. But any set $[G/H]$ of coset representatives gives rise to a basis of $k_\sharp\widehat{G}$ over $k_\sharp\widehat{H}$, so that the restriction of M is free.

(b) Let $\mathrm{Soc}(\mathrm{Res}^G_H(M))$ be the socle of $\mathrm{Res}^G_H(M)$, that is, the sum of all simple submodules of $\mathrm{Res}^G_H(M)$, or in other words the largest semi-simple submodule of $\mathrm{Res}^G_H(M)$. If L is a simple submodule of $\mathrm{Res}^G_H(M)$ and if $g \in \widehat{G}$, then $g{\cdot}L$ is again a submodule of $\mathrm{Res}^G_H(M)$, because H is a normal subgroup of G . Indeed $\widehat{H} \lhd \widehat{G}$ and for any $h \in \widehat{H}$, we have

$$hg{\cdot}L = g(g^{-1}hg){\cdot}L \subseteq g{\cdot}L \,.$$

In fact $g{\cdot}L$ is isomorphic to the conjugate module ${}^gL$ (Exercise 26.4). Clearly $g{\cdot}L$ is again simple and therefore $g{\cdot}L \subseteq \mathrm{Soc}(\mathrm{Res}^G_H(M))$. This proves that $\mathrm{Soc}(\mathrm{Res}^G_H(M))$ is invariant under $\widehat{G}$ and so is a submodule of M as a $k_\sharp\widehat{G}$-module. Since M is simple, $\mathrm{Soc}(\mathrm{Res}^G_H(M))$ is the whole of M , and this proves that $\mathrm{Res}^G_H(M)$ is semi-simple. □

In fact in case (b), one can say much more about $\mathrm{Res}^G_H(M)$ (Exercise 26.4).

Exercises

(26.1) Let $G = S_3$ be the symmetric group on 3 letters and $p = 3$. Prove all the facts mentioned in Example 26.5. Moreover describe in detail the parametrization of all indecomposable kS_3-modules. More generally describe the case of the dihedral group of order $2p$. [Hint: Use Exercise 17.2 and show that there are $2p$ indecomposable modules up to isomorphism.]

(26.2) Let G be a p-group. Prove that the set of isomorphism classes of indecomposable $\mathcal{O}G$-lattices is parametrized by the set of G-orbits of pairs (P, M), where P is a subgroup of G and M is an isomorphism class of indecomposable $\mathcal{O}P$-lattices with vertex P. Prove that the $\mathcal{O}G$-lattice corresponding to (P, M) is equal to $\mathrm{Ind}_P^G(M)$. [Hint: For each (P, M), show that there is a unique possible defect multiplicity module. Moreover apply Green's indecomposability theorem.]

(26.3) Prove all the details of the facts mentioned in Remark 26.7, namely that Green correspondents have the same three invariants.

(26.4) Let H be a normal subgroup of G, let $k_\sharp\widehat{G}$ be a twisted group algebra, and let M be a simple $k_\sharp\widehat{G}$-module. Choose a simple submodule L of $\mathrm{Res}_H^G(M)$.

(a) For any $g \in \widehat{G}$, prove that $g{\cdot}L \cong {}^gL$, the conjugate module.

(b) Prove that $\sum_{g\in\widehat{G}} g{\cdot}L = \mathrm{Res}_H^G(M)$. Deduce that for some integer e,

$$\mathrm{Res}_H^G(M) \cong \bigoplus_{g\in[\widehat{G}/\widehat{S}]} {}^g(L^e)$$

where $\widehat{S}$ is the inertial subgroup of L and L^e denotes the direct sum of e copies of L.

(c) Prove that L^e is endowed with a $k_\sharp\widehat{S}$-module structure, that L^e is a simple $k_\sharp\widehat{S}$-module, and that $M \cong \mathrm{Ind}_{\widehat{S}}^{\widehat{G}}(L^e)$.

Notes on Section 26

The idea of using the defect multiplicity module as a third invariant for the parametrization of modules (and interior algebras) is due to Puig. Some partial results (for instance the crucial Lemma 26.1) are stated in Puig [1988a] and the full statement appears in Thévenaz [1993]. The generalization to primitive interior G-algebras mentioned in Remark 26.6 appears in Thévenaz [1993], as well as in Puig [1994a] with a slightly different point of view. Proposition 26.8 is due to Puig [1981]. Lemma 26.10

and Exercise 26.4 are instances of the so-called Clifford theory: they are straightforward extensions of classical results of Clifford [1937].

§ 27 *p*-PERMUTATION MODULES

The permutation $\mathcal{O}G$-lattices and the $\mathcal{O}G$-lattices with trivial source $\mathcal{O}$ have some remarkable properties which we discuss in this section.

Given a finite G-set X (that is, a finite set endowed with a left action of the group G), we can construct an $\mathcal{O}$-lattice $\mathcal{O}X$ with $\mathcal{O}$-basis X , and extend linearly the G-action on X to obtain an $\mathcal{O}G$-lattice, called the *permutation $\mathcal{O}G$-lattice* on X . An arbitrary $\mathcal{O}G$-lattice is a permutation lattice precisely when it has a G-invariant $\mathcal{O}$-basis. A decomposition of the basis X as a disjoint union of G-orbits yields a direct sum decomposition of $\mathcal{O}X$ as an $\mathcal{O}G$-lattice. Thus we can assume that X is a transitive G-set, in which case $\mathcal{O}X \cong \mathrm{Ind}_H^G(\mathcal{O})$, where H is the stabilizer of some $x \in X$ and $\mathcal{O}$ denotes the trivial $\mathcal{O}H$-lattice. Indeed we have a direct sum decomposition as an $\mathcal{O}$-lattice

$$\mathcal{O}X = \bigoplus_{g\in[G/H]} \mathcal{O}gx$$

and G acts transitively on the summands, so that $\mathcal{O}X \cong \mathrm{Ind}_H^G(\mathcal{O})$ (Exercise 16.3). Therefore an arbitrary permutation $\mathcal{O}G$-lattice is isomorphic to a direct sum of modules of the form $\mathrm{Ind}_H^G(\mathcal{O})$ for various $H \leq G$. Conversely $\mathrm{Ind}_H^G(\mathcal{O})$ is a permutation $\mathcal{O}G$-lattice with invariant basis

$$\{\, g\otimes 1_{\mathcal{O}} \mid g \in [G/H] \,\} \,.$$

More generally if $\mathcal{O}X$ is a permutation $\mathcal{O}H$-lattice on X, then $\mathrm{Ind}_H^G(\mathcal{O}X)$ is a permutation $\mathcal{O}G$-lattice with invariant basis

$$\{\, g\otimes x \mid g \in [G/H] \,, x \in X \,\} \,.$$

Thus induction preserves permutation lattices. It is obvious that restriction and conjugation also preserve permutation lattices.

We now define a more general notion. An $\mathcal{O}G$-lattice M is called a *p-permutation lattice* if $\mathrm{Res}_Q^G(M)$ is a permutation lattice for every p-subgroup Q of G . Let P be a Sylow p-subgroup of G . Since we have $\mathrm{Res}_{{}^gP}^G(M) \cong {}^g(\mathrm{Res}_P^G(M))$ and since restriction and conjugation preserve permutation lattices, it suffices to require that $\mathrm{Res}^G_P(M)$ is a permutation lattice in order to deduce that M is a p-permutation lattice. In other words an $\mathcal{O}G$-lattice M is a p-permutation lattice if and only if it has a P-invariant $\mathcal{O}$-basis X. Of course X depends on the choice of the Sylow p-subgroup P, but one obtains a ${}^gP$-invariant basis by considering the set $\{\, g{\cdot}x \mid x \in X \,\}$. It is clear that p-permutation lattices are preserved by the following operations: direct sums, tensor products, restriction, conjugation. It is easy to prove directly from the definition that induction also preserves p-permutation lattices (Exercise 27.1), but this follows from another characterization of p-permutation lattices which we are going to give. We first need a lemma.

(27.1) LEMMA. *Let P be a p-group and let Q be a subgroup of P. Then $\mathrm{Ind}^P_Q(\mathcal{O})$ is indecomposable. Moreover Q is a vertex of $\mathrm{Ind}^P_Q(\mathcal{O})$ and the trivial $\mathcal{O}Q$-lattice $\mathcal{O}$ is a source of $\mathrm{Ind}^P_Q(\mathcal{O})$.*

Proof. The indecomposability follows from Green's indecomposability theorem (Corollary 23.6). Alternatively there is the following elementary proof. First one can replace $\mathcal{O}$ by its residue field k because if $\mathrm{Ind}^P_Q(\mathcal{O})$ decomposes, then so does $k \otimes_{\mathcal{O}} \mathrm{Ind}^P_Q(\mathcal{O}) \cong \mathrm{Ind}^P_Q(k)$. Consider the space $\mathrm{Hom}_{kP}(\mathrm{Ind}^P_Q(k), k)$. By construction of induced modules, any kQ-linear homomorphism $f : k \to \mathrm{Res}^P_Q(k) = k$ extends to a kP-linear homomorphism $1 \otimes f : \mathrm{Ind}^P_Q(k) \to k$ and therefore we have isomorphisms

$$\mathrm{Hom}_{kP}(\mathrm{Ind}^P_Q(k), k) \cong \mathrm{Hom}_{kQ}(k, \mathrm{Res}^P_Q(k)) = \mathrm{Hom}_{kQ}(k, k) \cong k\,.$$

Suppose that $\mathrm{Ind}^P_Q(k) = M_1 \oplus M_2$ as a kP-module, with $M_1 \neq 0$ and $M_2 \neq 0$. Since the trivial kP-module k is the only simple kP-module up to isomorphism (Proposition 21.1), M_i must have some top composition factor isomorphic to k, so that there exists a non-zero kP-linear homomorphism $f_i : M_i \to k$, which extends to a kP-linear homomorphism $f_i : \mathrm{Ind}^P_Q(k) \to k$ by requiring f_i to be zero on the other direct summand. Clearly f_1 and f_2 are linearly independent, contradicting the fact that $\mathrm{Hom}_{kP}(\mathrm{Ind}^P_Q(k), k)$ is one-dimensional. Thus $\mathrm{Ind}^P_Q(k)$ cannot decompose.

Finally we prove that Q is a vertex of $\mathrm{Ind}^P_Q(\mathcal{O})$. First note that Q is the vertex of the trivial $\mathcal{O}Q$-module $\mathcal{O}$ (because, for $R < Q$, the image of the trace map t^Q_R in $\mathrm{End}_{\mathcal{O}}(\mathcal{O}) = \mathcal{O}$ is equal to $|Q{:}R|\,\mathcal{O} \subseteq \mathfrak{p}\mathcal{O}$, so that t^R_Q cannot be surjective). Moreover $\mathcal{O}$ is a direct summand of $\mathrm{Res}^P_Q \mathrm{Ind}^P_Q(\mathcal{O})$, so that the conditions of Proposition 18.11 are satisfied. □

(27.2) COROLLARY. *If M is a p-permutation $\mathcal{O}G$-lattice, then any direct summand of M is again a p-permutation $\mathcal{O}G$-lattice. In particular if P is a p-group, any direct summand of a permutation $\mathcal{O}P$-lattice is a permutation $\mathcal{O}P$-lattice.*

Proof. By definition it suffices to work with the restriction to a Sylow p-subgroup P. If M is a permutation $\mathcal{O}P$-lattice, then M is a direct sum

$$M \cong \bigoplus_i \mathrm{Ind}_{Q_i}^P(\mathcal{O})$$

for some subgroups Q_i. By the lemma, each $\mathrm{Ind}_{Q_i}^P(\mathcal{O})$ is indecomposable. Therefore by the Krull–Schmidt theorem 4.4 any direct summand L of M is isomorphic to the direct sum of some of the factors. Thus L is again a permutation $\mathcal{O}P$-lattice. □

There are two other characterizations of p-permutation lattices. We define a *trivial source* $\mathcal{O}G$-lattice to be a direct sum of indecomposable $\mathcal{O}G$-lattices with trivial source $\mathcal{O}$.

(27.3) PROPOSITION. *Let M be an $\mathcal{O}G$-lattice. The following conditions are equivalent.*
(a) M is a p-permutation $\mathcal{O}G$-lattice.
(b) M is isomorphic to a direct summand of a permutation $\mathcal{O}G$-lattice.
(c) M is a trivial source $\mathcal{O}G$-lattice.

Proof. If M is an indecomposable trivial source $\mathcal{O}G$-lattice with vertex Q, then M is isomorphic to a direct summand of $\mathrm{Ind}_Q^G(\mathcal{O})$, which is a permutation $\mathcal{O}G$-lattice. Therefore (c) implies (b). It is clear by Corollary 27.2 that (b) implies (a). To prove that (a) implies (c), we consider each indecomposable direct summand of M (each is still a p-permutation lattice by Corollary 27.2), so that we can assume that M is indecomposable. If Q is a vertex of M, then M is isomorphic to a direct summand of $\mathrm{Ind}_Q^G \mathrm{Res}_Q^G(M)$. But $\mathrm{Res}_Q^G(M)$ is a permutation lattice, hence of the form

$$\mathrm{Res}_Q^G(M) \cong \bigoplus_i \mathrm{Ind}_{R_i}^Q(\mathcal{O}),$$

for some subgroups $R_i \le Q$. Inducing this to G and using the Krull–Schmidt theorem, we deduce that M, being indecomposable, is isomorphic to a direct summand of $\mathrm{Ind}_{R_i}^G(\mathcal{O})$ for some R_i, which we write as R for simplicity. By the minimality criterion for defect pointed groups (Theorem 18.3), it follows that $R = Q$ and that $\mathcal{O}$ must be a source of M, proving that M is a trivial source lattice. Explicitly if $A = \mathrm{End}_{\mathcal{O}}(\mathrm{Ind}_R^G(\mathcal{O}))$, if α denotes the point of A^G corresponding to M, and if γ denotes the point of A^R corresponding to the trivial $\mathcal{O}R$-lattice $\mathcal{O}$, then $G_\alpha \, pr \, R_\gamma$ (see Proposition 17.11). Therefore by the minimality criterion, R_γ contains some defect pointed group of G_α, which is of the form ${}^g(Q_\delta)$, because Q is a defect group by assumption. Since ${}^gQ \leq R \leq Q$, we must have equality, and so ${}^g(Q_\delta) = R_\gamma$. Hence γ is a source point of α and this means that $\mathcal{O}$ is a source of M. □

We shall use the terminology "p-permutation lattice" rather than "trivial source lattice", because the important point is the existence of invariant bases.

(27.4) COROLLARY. *If H is a subgroup of G and if M is a p-permutation $\mathcal{O}H$-lattice, then $\mathrm{Ind}_H^G(M)$ is a p-permutation $\mathcal{O}G$-lattice.*

Proof. Since permutation lattices are preserved by induction, so are their direct summands. □

Our aim now is to define the Brauer homomorphism for an $\mathcal{O}G$-lattice rather than a G-algebra. Let M be an $\mathcal{O}G$-lattice and for every subgroup H of G, denote by M^H the set of H-fixed elements in M. If $K \leq H \leq G$, the *relative trace map* t_K^H is defined to be the map

$$t_K^H : M^K \longrightarrow M^H , \qquad v \mapsto \sum_{h \in [H/K]} h{\cdot}v .$$

As in the case of G-algebras, it is easy to check that t_K^H is independent of the choice of coset representatives $[H/K]$ and that it satisfies the same properties (except the ones involving a multiplicative structure), namely properties (a), (b), (c), (d), and (g) of Proposition 11.4. We also set $M_K^H = t_K^H(M^K)$ and, for every subgroup P of G, we define the *Brauer quotient*

$$\overline{M}(P) = M^P / \big(\sum_{Q<P} M_Q^P + \mathfrak{p}M^P \big) .$$

Since $\mathfrak{p}\overline{M}(P) = 0$, it is clear that $\overline{M}(P)$ is a k-vector space. Moreover the action of $\overline{N}_G(P) = N_G(P)/P$ on M^P preserves $\sum_{Q<P} M_Q^P$ and $\mathfrak{p}M^P$, and therefore induces a $k\overline{N}_G(P)$-module structure on $\overline{M}(P)$. Note that $\overline{M}(1) = M/\mathfrak{p}M \cong k \otimes_{\mathcal{O}} M$. The argument of Lemma 11.7 shows that $\overline{M}(P)$ can be non-zero only if P is a p-subgroup of G.

The canonical surjection $br_P^M : M^P \to \overline{M}(P)$ is called the *Brauer homomorphism* corresponding to the subgroup P, written also br_P when the context is clear. It is clearly a homomorphism of $k\overline{N}_G(P)$-modules. Its restriction to M^H, where $H \geq P$, induces a homomorphism of $\mathcal{O}$-modules $br_P \, r_P^H : M^H \to \overline{M}(P)^{\overline{N}_H(P)}$.

(27.5) PROPOSITION. *Let M be an $\mathcal{O}G$-lattice, let P be a p-subgroup of G, and let H be a subgroup of G containing P. Then for every $v \in M^P$, we have*

$$br_P\, r_P^H\, t_P^H(v) = t_1^{\overline{N}_H(P)}\, br_P(v)\,,$$

where $t_1^{\overline{N}_H(P)} : \overline{M}(P) \to \overline{M}(P)^{\overline{N}_H(P)}$ is the relative trace map in $\overline{M}(P)$.

Proof. The proof of Proposition 11.9 carries over without change. □

If A is a G-algebra which is free as an $\mathcal{O}$-module, then it is in particular an $\mathcal{O}G$-lattice. It is clear that the construction of $\overline{A}(P)$ and br_P for the $\mathcal{O}G$-lattice A coincides with the construction defined in Section 11 for the G-algebra A. But there is more structure in this special case, because $\mathfrak{p}A^P + \sum_{Q<P} A_Q^P$ is an ideal and $\overline{A}(P)$ is a k-algebra.

For a primitive G-algebra A, we know from Corollary 18.6 that a defect group of A is a maximal subgroup P such that $\overline{A}(P) \neq 0$. We warn the reader that the analogous property does not hold for an indecomposable $\mathcal{O}G$-lattice M: a maximal subgroup Q such that $\overline{M}(Q) \neq 0$ is contained in a vertex P of M but may not be equal to P (Exercise 27.2). However, we are going to see that this problem does not arise for p-permutation lattices, so that $\overline{M}(P)$ is a particularly useful construction in that case.

(27.6) PROPOSITION. *Let M be a p-permutation $\mathcal{O}G$-lattice and let X be a P-invariant $\mathcal{O}$-basis of M, where P is a p-subgroup of G. Moreover let $A = \mathrm{End}_{\mathcal{O}}(M)$.*

(a) $\overline{M}(P)$ has a k-basis $br_P(X^P) = \{\, br_P(x) \mid x \in X^P \,\}$, where X^P denotes the set of P-fixed elements in X. Moreover the sum of all elements in a non-trivial P-orbit is in the kernel of br_P.

(b) $\overline{M}(P)$ is a p-permutation $k\overline{N}_G(P)$-module.

(c) There is a natural action of $\overline{A}(P)$ on $\overline{M}(P)$ and this induces an isomorphism of $k\overline{N}_G(P)$-algebras

$$\overline{A}(P) \cong \mathrm{End}_k(\overline{M}(P))\,.$$

(d) The set $\mathcal{LP}(A^P)$ of local points is either empty or is a singleton. It is empty if and only if $X^P = \emptyset$. If $X^P \neq \emptyset$, the unique local point $\gamma \in \mathcal{LP}(A^P)$ has a multiplicity algebra $S(\gamma) = \overline{A}(P)$ and the canonical surjection $\pi_\gamma : A^P \to S(\gamma)$ coincides with the Brauer homomorphism.

Proof. (a) Since the action of P is a left action, we write $[P\backslash X]$ for a set of representatives of P-orbits in X, and for each $x \in [P\backslash X]$ we let P_x be the stabilizer of x. Then a straightforward computation shows that

$$\{\, t_{P_x}^P(x) \mid x \in [P\backslash X] \,\}$$

is an $\mathcal{O}$-basis of M^P. Clearly $t_{P_x}^P(x) \in \sum_{Q<P} M_Q^P$ if $P_x < P$, while $x \in X^P$ otherwise. In order to compute M_Q^P for every proper subgroup Q of P, we first note that similarly $\{\, t_{Q_x}^Q(x) \mid x \in [Q\backslash X] \,\}$ is an $\mathcal{O}$-basis of M^Q. Then we have

$$t_Q^P(t_{Q_x}^Q(x)) = t_{Q_x}^P(x) = t_{P_x}^P(t_{Q_x}^{P_x}(x)) = |P_x : Q_x|\, t_{P_x}^P(x)\,.$$

This belongs to $\mathfrak{p}M^P$ if $Q_x < P_x$ (because $|P_x : Q_x|$ is a power of p and $p{\cdot}1_{\mathcal{O}} \in \mathfrak{p}$), while if $Q_x = P_x$, we obtain $t_{P_x}^P(x)$ which is a basis element of M^P. It follows that

$$M_Q^P \subseteq \mathfrak{p}M^P + \sum_{\substack{x\in[P\backslash X]\\ P_x<P}} \mathcal{O}{\cdot}t_{P_x}^P(x)$$

and therefore

$$\begin{aligned}\mathfrak{p}M^P + \sum_{Q<P} M_Q^P &= \mathfrak{p}M^P + \sum_{\substack{x\in[P\backslash X]\\ P_x<P}} \mathcal{O}{\cdot}t_{P_x}^P(x)\\ &= \Big(\bigoplus_{x\in X^P} \mathfrak{p}{\cdot}x\Big) \oplus \Big(\bigoplus_{\substack{x\in[P\backslash X]\\ P_x<P}} \mathcal{O}{\cdot}t_{P_x}^P(x)\Big)\,.\end{aligned}$$

Hence $\overline{M}(P) = \bigoplus_{x\in X^P} (\mathcal{O}/\mathfrak{p}){\cdot}br_P(x)$, which completes the proof of (a).

(b) Let Q be a Sylow p-subgroup of $N_G(P)$, which necessarily contains P, and let X be a Q-invariant basis of M. Then X is in particular P-invariant and part (a) applies. Since Q normalizes P, the set X^P is invariant under the action of Q. Therefore the k-basis $br_P(X^P)$ of $\overline{M}(P)$ is invariant under the Sylow p-subgroup Q/P of $\overline{N}_G(P)$. This proves that $\overline{M}(P)$ is a p-permutation $k\overline{N}_G(P)$-module.

(c) Let $b_{x,y}$ be the endomorphism of M defined on each basis element $z \in X$ by the formula $b_{x,y}(z) = \delta_{y,z}\, x$ (where $\delta_{y,z}$ is the Kronecker symbol). The set $B = \{\, b_{x,y} \mid x, y \in X \,\}$ is an $\mathcal{O}$-basis of the algebra $A = \mathrm{End}_{\mathcal{O}}(M)$. In matrix terms, $b_{x,y}$ is the matrix having the (x, y)-entry equal to 1 and all other entries zero, and it is clear that these matrices form an $\mathcal{O}$-basis of A. If $u \in P$ and $z \in X$, we have

$$u{\cdot}b_{x,y}{\cdot}u^{-1}(z) = u{\cdot}b_{x,y}(u^{-1}{\cdot}z) = u{\cdot}\delta_{y,u^{-1}\cdot z}\, x = \delta_{u\cdot y,z}\, u{\cdot}x = b_{u\cdot x,u\cdot y}(z)\,,$$

and therefore $u{\cdot}b_{x,y}{\cdot}u^{-1} = b_{u\cdot x,u\cdot y}$.

The G-algebra A is in particular an $\mathcal{O}G$-lattice, with G acting by conjugation. The computation above shows that B is a P-invariant basis of A and that

$$B^P = \{\, b_{x,y} \mid x, y \in X^P \,\}.$$

Thus A is a p-permutation lattice and by part (a), the set $br_P^A(B^P)$ is a k-basis of $\overline{A}(P)$.

The A-module structure on M is given by an $\mathcal{O}$-bilinear map

$$f : A \times M \longrightarrow M\,, \qquad f(a,v) = a{\cdot}v\,,$$

which commutes with the G-action, in the sense that $f({}^g a, g{\cdot}v) = g{\cdot}f(a,v)$ for all $a \in A$, $v \in M$, and $g \in G$. Thus f induces by restriction a bilinear map $f^Q : A^Q \times M^Q \to M^Q$ for every subgroup Q of G. If $Q \leq P$, $a \in A^Q$, and $v \in M^P$, we have the property

$$\begin{aligned} f^P(t_Q^P(a), v) &= f(\sum_{u\in[P/Q]} {}^u a\,, v) = \sum_{u\in[P/Q]} f({}^u a, u{\cdot}v) = \sum_{u\in[P/Q]} u{\cdot}f(a,v) \\ &= t_Q^P(f^Q(a,v))\,. \end{aligned}$$

Similarly $f^P(a, t_Q^P(v)) = t_Q^P(f^Q(a,v))$ if $a \in A^P$ and $v \in M^Q$. From this it follows that f^P induces a k-bilinear map

$$\overline{f}(P) : \overline{A}(P) \times \overline{M}(P) \longrightarrow \overline{M}(P)$$

such that $\overline{f}(P)(br_P^A(a), br_P^M(v)) = br_P^M(a{\cdot}v)$. We shall use the notation $\overline{f}(P)(\overline{a}, \overline{v}) = \overline{a}{\cdot}\overline{v}$, so that we have $br_P^A(a){\cdot}br_P^M(v) = br_P^M(a{\cdot}v)$.

This shows that $\overline{M}(P)$ is a module over $\overline{A}(P)$ and therefore we obtain a k-algebra map

$$\phi : \overline{A}(P) \longrightarrow \mathrm{End}_k(\overline{M}(P))\,,$$

such that $\phi(\overline{a})(\overline{v}) = \overline{a}{\cdot}\overline{v}$. Since the bilinear map f we started with commutes with the action of G, and since the Brauer homomorphism commutes with the action of $\overline{N}_G(P)$ (by definition of its action on $\overline{A}(P)$ and $\overline{M}(P)$), the map ϕ is a homomorphism of $\overline{N}_G(P)$-algebras. To show that ϕ is an isomorphism, we show that the k-basis $br_P^A(B^P)$ of $\overline{A}(P)$ is mapped to a basis of $\mathrm{End}_k(\overline{M}(P))$. To this end we compute the action of an element of $br_P^A(B^P)$ on the basis $br_P^M(X^P)$ of $\overline{M}(P)$. If $x, y, z \in X^P$ (so that $b_{x,y} \in B^P$), we have

$$br_P^A(b_{x,y}){\cdot}br_P^M(z) = br_P^M(b_{x,y}(z)) = \delta_{y,z}\, br_P^M(x)\,.$$

Thus $\phi(br_P^A(b_{x,y}))$ is the elementary matrix having the (x,y)-entry equal to 1 and all other entries zero. It is clear that these matrices form a k-basis of $\mathrm{End}_k(\overline{M}(P))$ for $x,y \in X^P$.

(d) Since $\overline{A}(P) \cong \mathrm{End}_k(\overline{M}(P))$ and $\overline{M}(P)$ has $br_P^M(X^P)$ as a k-basis, it is clear that $\overline{A}(P) = 0$ if and only if X^P is empty. This proves the first assertion since $\mathcal{LP}(A^P) \cong \mathcal{P}(\overline{A}(P))$ (see Lemma 14.5). If $X^P \neq \emptyset$, then $\overline{A}(P)$ is a simple algebra (since it is the endomorphism algebra of a k-vector space), hence has a single point. It is then clear that $br_P^A : A^P \to \overline{A}(P)$ is the canonical surjection onto a simple algebra, corresponding to a point γ of A^P which is the unique local point of A^P. □

(27.7) COROLLARY. *Let M be a p-permutation $\mathcal{O}G$-lattice. If M is indecomposable, then any maximal subgroup P such that $\overline{M}(P) \neq 0$ is a vertex of M.*

Proof. Let $A = \mathrm{End}_{\mathcal{O}}(M)$. By part (c) of Proposition 27.6, we know that $\overline{M}(P) \neq 0$ if and only if $\overline{A}(P) \neq 0$. The result now follows from Corollary 18.6. □

Let M be a p-permutation $\mathcal{O}G$-lattice and let $A = \mathrm{End}_{\mathcal{O}}(M)$. By construction $\overline{M}(P)$ has a $k\overline{N}_G(P)$-module structure and therefore its endomorphism algebra $\mathrm{End}_k(\overline{M}(P)) \cong \overline{A}(P)$ is an interior $\overline{N}_G(P)$-algebra. If $\overline{M}(P) \neq 0$, then $\overline{A}(P) = S(\gamma)$ is the multiplicity algebra of the unique local point γ of A^P, and this multiplicity algebra carries canonically an *interior* $\overline{N}_G(P)$-algebra structure. In other words the multiplicity module of γ is the $k\overline{N}_G(P)$-module $\overline{M}(P)$ and $S(\gamma) \cong \mathrm{End}_k(\overline{M}(P))$. Thus the usual twisted group algebra associated with a multiplicity algebra is here isomorphic to the ordinary group algebra $k\overline{N}_G(P)$. We shall come back to this point at the end of this section.

(27.8) COROLLARY. *Let M be a p-permutation $\mathcal{O}G$-lattice and let $A = \mathrm{End}_{\mathcal{O}}(M)$. If P_γ is a local pointed group on A (so that γ is the unique local point of A^P), then the multiplicity module of γ is a module over the ordinary group algebra $k\overline{N}_G(P)$ and is isomorphic to $\overline{M}(P)$.*

In particular if M is an indecomposable p-permutation $\mathcal{O}G$-lattice with vertex P, the defect multiplicity module of M is $\overline{M}(P)$ and it is an indecomposable projective $k\overline{N}_G(P)$-module. Note that by Corollary 19.3, the converse also holds, as follows.

(27.9) PROPOSITION. *Let* M *be an indecomposable* p*-permutation* $\mathcal{O}G$*-lattice and let* P *be a* p*-subgroup of* G. *Then* P *is a vertex of* M *if and only if* $\overline{M}(P)$ *is non-zero and is a projective* $k\overline{N}_G(P)$*-module.*

Using this explicit description of the defect multiplicity module, we specialize the results of the previous section to the case of p-permutation lattices. In other words we fix the trivial module as source module and we consider the parametrization of trivial source $\mathcal{O}G$-lattices with the remaining two invariants: the vertex and the defect multiplicity module. Let $\Lambda_{\mathcal{O}}(G, \mathrm{triv})$ be the set of isomorphism classes of indecomposable p-permutation $\mathcal{O}G$-lattices (or equivalently with trivial source) and let $\Pi_{\mathcal{O}}(G, \mathrm{triv})$ be the set of pairs (P, V) where P is a p-subgroup of G and V is an isomorphism class of indecomposable projective $k\overline{N}_G(P)$-modules. The group G acts by conjugation on $\Pi_{\mathcal{O}}(G, \mathrm{triv})$. Let $G\backslash\Pi_{\mathcal{O}}(G, \mathrm{triv})$ be the set of orbits. The bijection of Theorem 26.4 restricts immediately to a bijection between $\Lambda_{\mathcal{O}}(G, \mathrm{triv})$ and $G\backslash\Pi_{\mathcal{O}}(G, \mathrm{triv})$. We state the result in full.

(27.10) THEOREM. *There is a bijection* $\Lambda_{\mathcal{O}}(G, \mathrm{triv}) \to G\backslash\Pi_{\mathcal{O}}(G, \mathrm{triv})$ *which is described as follows.*

(a) *With an indecomposable* p*-permutation* $\mathcal{O}G$*-lattice* M *is associated the* G*-orbit of pairs* $(P, \overline{M}(P))$ *where* P *is a vertex of* M.

(b) *With the* G*-orbit of a pair* (P, V) *is associated the isomorphism class of direct summands of* $\mathrm{Ind}_P^G(\mathcal{O})$ *corresponding to the point of* $\mathrm{End}_{\mathcal{O}G}(\mathrm{Ind}_P^G(\mathcal{O}))$ *which is the Puig correspondent of the module* V *(where the Puig correspondence is taken with respect to* $(P, \mathcal{O})$ *).*

Any $\mathcal{O}G$-lattice M determines a kG-module $M/\mathfrak{p}M$, but in general a kG-module may not lift to an $\mathcal{O}G$-lattice. However, this property holds for p-permutation modules.

(27.11) PROPOSITION. *The ring homomorphism* $\mathcal{O} \to \mathcal{O}/\mathfrak{p} = k$ *induces a bijection between* $\Lambda_{\mathcal{O}}(G, \mathrm{triv})$ *and* $\Lambda_k(G, \mathrm{triv})$, *preserving vertex and defect multiplicity module. Thus any* p*-permutation* kG*-module lifts to a* p*-permutation* $\mathcal{O}G$*-lattice.*

Proof. It is clear that if M is a p-permutation $\mathcal{O}G$-lattice, then $M/\mathfrak{p}M$ is a p-permutation kG-module. Indeed if X is a P-invariant $\mathcal{O}$-basis of M for some p-subgroup P, then its image in $M/\mathfrak{p}M$ is a P-invariant k-basis of $M/\mathfrak{p}M$. Moreover both $\overline{M}(P)$ and $\overline{(M/\mathfrak{p}M)}(P)$ are k-vector spaces with basis $br_P(X^P)$, and so reduction modulo $\mathfrak{p}$ induces an isomorphism

$$\overline{M}(P) \cong \overline{(M/\mathfrak{p}M)}(P).$$

If now M is an indecomposable p-permutation $\mathcal{O}G$-lattice with vertex P, then $\overline{M}(P)$ is an indecomposable projective $k\overline{N}_G(P)$-module. Moreover by Corollary 19.3, for any p-subgroup Q not conjugate to P, no indecomposable direct summand of $\overline{M}(Q)$ is a projective $k\overline{N}_G(Q)$-module (using the fact that if $\overline{M}(Q) \neq 0$, then it is the multiplicity module of a local pointed group on $\mathrm{End}_{\mathcal{O}}(M)$, by Proposition 27.6 and Corollary 27.8). It follows that $M/\mathfrak{p}M$ is a p-permutation kG-module such that $\overline{(M/\mathfrak{p}M)}(P)$ is an indecomposable projective $k\overline{N}_G(P)$-module, and such that for any p-subgroup Q not conjugate to P, no indecomposable direct summand of $\overline{(M/\mathfrak{p}M)}(Q)$ is a projective $k\overline{N}_G(Q)$-module. This implies that $M/\mathfrak{p}M$ is indecomposable because an indecomposable direct summand of $M/\mathfrak{p}M$ can be detected by its defect multiplicity module: if L is an indecomposable direct summand of $M/\mathfrak{p}M$ with vertex Q, then $\overline{L}(Q)$ is an indecomposable projective direct summand of $\overline{(M/\mathfrak{p}M)}(Q)$. Thus $M/\mathfrak{p}M$ is indecomposable and the indecomposable projective $k\overline{N}_G(P)$-module $\overline{(M/\mathfrak{p}M)}(P)$ must be its defect multiplicity module, so that P is its vertex by Proposition 27.9. Therefore we have proved that reduction modulo $\mathfrak{p}$ preserves indecomposability, as well as vertex and defect multiplicity module. The result now follows from the parametrization given by Theorem 27.10. □

An indecomposable $\mathcal{O}G$-lattice M with vertex 1 necessarily has trivial source $\mathcal{O}$, because $\mathcal{O}$ is the only indecomposable $\mathcal{O}$-lattice. Thus M is a p-permutation lattice and it is a direct summand of the induced module $\mathrm{Ind}_1^G(\mathcal{O}) = \mathcal{O}G$, the free $\mathcal{O}G$-module of rank one. In other words M is an indecomposable projective $\mathcal{O}G$-module. Conversely an indecomposable projective module is a p-permutation lattice with vertex 1 since it is a direct summand of $\mathcal{O}G = \mathrm{Ind}_1^G(\mathcal{O})$. Note that the defect multiplicity module of M is $\overline{M}(1) = M/\mathfrak{p}M$, an indecomposable projective kG-module. Thus as a special case of Proposition 27.11, we obtain that reduction modulo $\mathfrak{p}$ induces a bijection between the set of isomorphism classes of indecomposable projective $\mathcal{O}G$-modules and the set of isomorphism classes of indecomposable projective kG-modules. Of course this has been proved more directly in Corollary 5.2.

(27.12) REMARK. We mention a few facts about the Green correspondence and we give in particular another point of view explaining why the defect multiplicity module is a module over an untwisted group algebra. Let M be an indecomposable p-permutation $\mathcal{O}G$-lattice with vertex P and let L be its Green correspondent, an $\mathcal{O}H$-lattice where $H = N_G(P)$. Since L has vertex P and trivial source, L is a summand of $\mathrm{Ind}_P^H(\mathcal{O})$, on which P acts trivially because $P \triangleleft H$. Therefore P acts trivially on L and it follows that $C_H(P \cdot 1_A) = H$, where $A = \mathrm{End}_{\mathcal{O}}(L)$. Whereas A^P is in general only viewed as an interior $C_H(P)$-algebra, it is in fact always an interior $C_H(P{\cdot}1_A)$-algebra, and $C_H(P{\cdot}1_A)$ may be larger than $C_H(P)$. This means here that the H-algebra A^P is interior and therefore so is the defect multiplicity algebra which is a quotient of A^P. Consequently the defect multiplicity module of L is a module over the ordinary group algebra $k\overline{H}$, and therefore so is the defect multiplicity module of M, since both defect multiplicity modules coincide. However, this argument does not work directly with M because for $B = \mathrm{End}_{\mathcal{O}}(M)$, the subgroup $C_G(P{\cdot}1_B)$ may not include H.

We also mention that if we work over the field k, then the Green correspondent L is simply equal to $\overline{M}(P)$, viewed as a $kN_G(P)$-module by letting P act trivially (Exercise 27.4). If we work over $\mathcal{O}$, then L is obtained by lifting to $\mathcal{O}N_G(P)$ the $kN_G(P)$-module $\overline{M}(P)$. For an arbitrary p-subgroup Q, working over k again, there is also an interpretation of $\overline{M}(Q)$ as a suitable direct summand of $\mathrm{Res}^G_Q(M)$ (Exercise 27.4).

Exercises

(27.1) Prove directly from the definition that the induction of a p-permutation lattice is again a p-permutation lattice.

(27.2) Let M be an indecomposable $\mathcal{O}G$-lattice with vertex P.

(a) Prove that if $\overline{M}(Q) \neq 0$, then a conjugate of Q is a subgroup of P. [Hint: Prove that $\overline{M}(Q)$ is an $\overline{A}(Q)$-module, where $A = \mathrm{End}_{\mathcal{O}}(M)$.]

(b) Find an example where $\overline{M}(P) = 0$. [Hint: Let $G = GL_3(\mathbb{F}_2)$ be the general linear group over the field $\mathbb{F}_2$ with two elements, and let M be the natural representation of G over $\mathbb{F}_2$, of dimension 3 (given by the identity map), which can be viewed as a representation over any field k of characteristic 2. Let P be the set of upper triangular matrices, which is a Sylow 2-subgroup of G. Then by Exercise 23.2, P is a vertex of M. Let Q be the subgroup of P consisting of the upper triangular matrices whose $(1, 2)$-entry is zero. Prove that, if v_1 and v_2 are the first two basis elements of M, then $M^P = kv_1$, $M^Q = kv_1 \oplus kv_2$, and $t^P_Q(M^Q) = M^P$.]

(27.3) Let P be a p-subgroup of G, let V be an indecomposable projective $k\overline{N}_G(P)$-module, and let $M_{(P,V)}$ be the indecomposable p-permutation $\mathcal{O}G$-lattice with vertex P and defect multiplicity module V. Let L be a p-permutation $\mathcal{O}G$-lattice. Prove that $M_{(P,V)}$ is isomorphic to a direct summand of L if and only if V is a direct summand of $\overline{L}(P)$.

(27.4) Let M be a p-permutation kG-module and let Q be a p-subgroup of G. Choose a decomposition of $\mathrm{Res}^G_{N_G(Q)}(M)$ into indecomposable direct summands and write $\mathrm{Res}^G_{N_G(Q)}(M) = L_1 \oplus L_2$ where L_1 is the direct sum of all the summands on which Q acts trivially and L_2 is the direct sum of all the other summands.

(a) Prove that every indecomposable summand of L_1 has vertex containing Q and that every indecomposable summand of L_2 has vertex not containing Q.

(b) Prove that $\overline{L}_1(Q) = L_1$ and $\overline{L}_2(Q) = 0$. Deduce that $\overline{M}(Q) = L_1$.

(c) In the case where Q is the vertex of M, prove that $L_1 = \overline{M}(Q)$ is indecomposable and is the Green correspondent of M. [Hint: Use Exercise 20.4.]

(27.5) Let P be a p-subgroup of G. The *Scott module* $Sc(P)$ is the indecomposable p-permutation $\mathcal{O}G$-lattice with vertex P and defect multiplicity module V, where V is the projective cover of the trivial $k\overline{N}_G(P)$-module. This is well-defined up to isomorphism.

(a) Prove that if V is the projective cover of the trivial kX-module (where X is any finite group), then $t_1^X(V) = V^X$ has dimension 1, while if W is the projective cover of a non-trivial simple kX-module, then $t_1^X(W) = W^X = 0$. [Hint: Compute t_1^X as well as fixed elements in a free kX-module of rank one.]

(b) Prove that $Sc(P)^G_P = Sc(P)^G$, and that this is a one-dimensional sublattice of $Sc(P)$, hence an $\mathcal{O}G$-sublattice of $Sc(P)$ isomorphic to the trivial $\mathcal{O}G$-lattice $\mathcal{O}$. Prove also that $Sc(P)$ is the only direct summand of $\mathrm{Ind}^G_P(\mathcal{O})$ (up to isomorphism) having an $\mathcal{O}G$-sublattice isomorphic to $\mathcal{O}$. [Hint: The Brauer homomorphism induces a surjection of $Sc(P)^G_P$ onto $V_1^{\overline{N}_G(P)}$, which is one-dimensional by (a). On the other hand show that $Sc(P)^G_P \subseteq Sc(P)^G \cong \mathrm{Hom}_{\mathcal{O}G}(\mathcal{O}, Sc(P)) \subseteq \mathrm{Hom}_{\mathcal{O}G}(\mathcal{O}, \mathrm{Ind}^G_P(\mathcal{O})) \cong \mathrm{Hom}_{\mathcal{O}P}(\mathcal{O}, \mathcal{O}) \cong \mathcal{O}$.]

(c) Prove that $Sc(P) \cong Sc(P)^*$. [Hint: Show that $\overline{M}(P)^* \cong \overline{M^*}(P)$ for any p-permutation $\mathcal{O}G$-lattice M. Moreover show that the projective cover of the trivial module is self-dual.]

(d) Deduce from (b) and (c) that $Sc(P)$ has a quotient $\mathcal{O}G$-lattice isomorphic to the trivial $\mathcal{O}G$-lattice $\mathcal{O}$ and that $Sc(P)$ is the only direct summand of $\mathrm{Ind}^G_P(\mathcal{O})$ (up to isomorphism) having a quotient $\mathcal{O}G$-lattice isomorphic to $\mathcal{O}$.

Notes on Section 27

Trivial source modules have been studied by Conlon [1968], Scott [1973] and others. The approach using invariant bases and the Brauer homomorphism is due to Puig and appears in Broué [1985].

§ 28 ENDO-PERMUTATION MODULES

In this section we study the important class of endo-permutation modules over a p-group, which are generalizations of permutation modules. Their importance stems from the fact that they occur in the description of a source algebra of a nilpotent block (see Section 50). Also, for a p-soluble group G, they appear as sources of simple kG-modules (see Section 30), and also in the description of a source algebra of any block of G.

Let P be a finite p-group. An *endo-permutation* $\mathcal{O}P$-lattice is an $\mathcal{O}P$-lattice M such that $\mathrm{End}_{\mathcal{O}}(M)$ is a permutation $\mathcal{O}P$-module under the conjugation action of P. In other words we require the existence of a P-invariant $\mathcal{O}$-basis of $\mathrm{End}_{\mathcal{O}}(M)$. It is reasonable to work only with lattices since $\mathrm{End}_{\mathcal{O}}(M)$ is in particular required to have an $\mathcal{O}$-basis. If $\mathcal{O} = k$ is a field, an endo-permutation $\mathcal{O}P$-lattice will also be called an endo-permutation $\mathcal{O}P$-module. Clearly the definition uses only the P-algebra structure of $\mathrm{End}_{\mathcal{O}}(M)$, so it is natural to define the following related concept. A *permutation G-algebra* is a G-algebra having a G-invariant basis. Thus an $\mathcal{O}P$-lattice M is an endo-permutation $\mathcal{O}P$-lattice if and only if $\mathrm{End}_{\mathcal{O}}(M)$ is a permutation P-algebra.

If A is an $\mathcal{O}$-simple permutation P-algebra, we have $A \cong \mathrm{End}_{\mathcal{O}}(M)$ for some $\mathcal{O}$-lattice M. Although this resembles the definition of an endo-permutation module, we note that A may not have an interior structure (inducing the given P-algebra structure), so that M may not be an endo-permutation module. In general M is only a module over a twisted group algebra (Exercise 28.2). However, in all cases which we are interested in, we are going to prove that A can in fact be given an interior structure, so that M becomes an endo-permutation $\mathcal{O}P$-lattice. The technical property which allows this is $\overline{A}(P) \neq 0$, and this also implies some other important facts. For this reason we define a *Dade P-algebra* to be an $\mathcal{O}$-simple permutation P-algebra A such that $\overline{A}(P) \neq 0$. If an $\mathcal{O}$-simple permutation P-algebra A is primitive, then $\overline{A}(P) \neq 0$ if and only if P is a defect group of A (Corollary 18.6). Thus a primitive Dade P-algebra has defect group P.

In general two different endo-permutation module structures on an $\mathcal{O}$-lattice M may yield the same P-algebra $A = \mathrm{End}_{\mathcal{O}}(M)$. This occurs precisely when the two module structures are given by two group homomorphisms $\phi, \phi' : P \to A^*$ such that $\phi' = \lambda\phi$ for some group homomorphism $\lambda : P \to \mathcal{O}^*$ (see Exercise 10.1 or Proposition 21.5). However, we have uniqueness over k, because there are no non-trivial p-th roots of unity in k so that such a homomorphism λ is necessarily trivial. This is actually one of the two cases in which we have already seen a proof of the existence of an interior structure on an $\mathcal{O}$-simple P-algebra. We recall the result.

(28.1) LEMMA. *Let A be an $\mathcal{O}$-simple permutation P-algebra and write $A = \mathrm{End}_{\mathcal{O}}(M)$ (where M is an $\mathcal{O}$-lattice).*

(a) If $\mathcal{O} = k$, there exists a unique interior P-algebra structure on A inducing the given P-algebra structure. In other words M becomes in a unique way an endo-permutation kP-module.

(b) If the dimension of M is prime to p, there exists a unique interior P-algebra structure on A inducing the given P-algebra structure and such that $\det(u{\cdot}1_A) = 1$ for all $u \in P$. In other words M becomes in a unique way an endo-permutation $\mathcal{O}P$-lattice of determinant 1.

Proof. This is a restatement of Corollary 21.4 and Proposition 21.5, specialized to the case of permutation P-algebras. □

Thus over k, the concepts of simple permutation P-algebra and endo-permutation kP-module are the same. Note that in case (b), the other interior P-algebra structures are obtained from the unique structure of determinant one by multiplying with a group homomorphism $\lambda : P \to \mathcal{O}^*$. All these structures are distinct since their determinants are distinct (using the fact that, if the dimension n of M is prime to p, then the n-th power of λ cannot be trivial). If $\mathcal{O}$ does not contain non-trivial p-th roots of unity (for instance if $\mathcal{O}$ is an absolutely unramified discrete valuation ring and $p \neq 2$), then λ must be trivial and the interior structure is unique. At the other extreme, if $\mathcal{O}$ is a characteristic zero domain containing primitive $|P|$-th roots of unity, then the number of choices for λ is $|P_{ab}|$, the order of the abelianization of P.

We now prove that the permutation modules considered in the previous section are examples of endo-permutation modules. Note that since P is a p-group, any p-permutation $\mathcal{O}P$-lattice is in fact a permutation $\mathcal{O}P$-lattice. We also show that several operations preserve the class of endo-permutation modules.

(28.2) PROPOSITION. *Let P be a p-group.*

(a) Any permutation $\mathcal{O}P$-lattice is an endo-permutation $\mathcal{O}P$-lattice.

(b) Any direct summand of an endo-permutation $\mathcal{O}P$-lattice is an endo-permutation $\mathcal{O}P$-lattice.

(c) If M is an endo-permutation $\mathcal{O}P$-lattice and Q is a subgroup of P, then $\mathrm{Res}^P_Q(M)$ is an endo-permutation $\mathcal{O}Q$-lattice.

(d) If M and N are endo-permutation $\mathcal{O}P$-lattices, then the dual M^* and the tensor product $M \otimes_{\mathcal{O}} N$ are endo-permutation $\mathcal{O}P$-lattices.

(e) If M is an endo-permutation $\mathcal{O}P$-lattice, then the Heller translates ΩM and $\Omega^{-1} M$ are endo-permutation $\mathcal{O}P$-lattices.

Proof. (a) Let M be a permutation $\mathcal{O}P$-lattice, let X be a P-invariant basis of M, and let $b_{x,y}$ be the endomorphism of M defined on each basis element $z \in X$ by the formula $b_{x,y}(z) = \delta_{y,z}x$. We have already noticed in the proof of part (c) of Proposition 27.6 that the set $B = \{ b_{x,y} \mid x, y \in X \}$ is a P-invariant basis of $\mathrm{End}_{\mathcal{O}}(M)$.

(b) Let M be an endo-permutation $\mathcal{O}P$-lattice, let $A = \mathrm{End}_{\mathcal{O}}(M)$, and let iM be a direct summand of M, where i is an idempotent of A^P. We know from Lemma 12.4 that $\mathrm{End}_{\mathcal{O}}(iM) \cong iAi$. The P-invariant direct sum decomposition

$$A = iAi \;\oplus\; iA(1-i) \;\oplus\; (1-i)Ai \;\oplus\; (1-i)A(1-i)$$

shows that iAi is a direct summand of the permutation $\mathcal{O}P$-lattice A, hence is again a permutation $\mathcal{O}P$-lattice (Corollary 27.2).

(c) It is clear that a P-invariant basis of $\mathrm{End}_{\mathcal{O}}(M)$ is also Q-invariant.

(d) Any P-invariant basis of $A = \mathrm{End}_{\mathcal{O}}(M)$ is also a P-invariant basis of $A^{op} \cong \mathrm{End}_{\mathcal{O}}(M^*)$. On the other hand the tensor product of a P-invariant basis of $\mathrm{End}_{\mathcal{O}}(M)$ and a P-invariant basis of $\mathrm{End}_{\mathcal{O}}(N)$ yields a P-invariant basis of $\mathrm{End}_{\mathcal{O}}(M) \otimes_{\mathcal{O}} \mathrm{End}_{\mathcal{O}}(N) \cong \mathrm{End}_{\mathcal{O}}(M \otimes_{\mathcal{O}} N)$.

(e) Let $0 \to N \to L \to M \to 0$ be a short exact sequence of $\mathcal{O}P$-lattices with L projective (in fact free by Proposition 21.1). We have to show that M is an endo-permutation lattice if and only if N is an endo-permutation lattice. Since the short exact sequence splits over $\mathcal{O}$ (as we are dealing only with free $\mathcal{O}$-modules), the functors $\mathrm{Hom}_{\mathcal{O}}(-, M)$ and $\mathrm{Hom}_{\mathcal{O}}(N, -)$ preserve exactness. Therefore we have two exact sequences of $\mathcal{O}P$-lattices:

$$0 \longrightarrow \mathrm{End}_{\mathcal{O}}(M) \longrightarrow \mathrm{Hom}_{\mathcal{O}}(L, M) \longrightarrow \mathrm{Hom}_{\mathcal{O}}(N, M) \longrightarrow 0\,,$$
$$0 \longrightarrow \mathrm{End}_{\mathcal{O}}(N) \longrightarrow \mathrm{Hom}_{\mathcal{O}}(N, L) \longrightarrow \mathrm{Hom}_{\mathcal{O}}(N, M) \longrightarrow 0\,.$$

By Exercise 17.4, both $\mathrm{Hom}_{\mathcal{O}}(L, M)$ and $\mathrm{Hom}_{\mathcal{O}}(N, L)$ are projective $\mathcal{O}P$-lattices, because L is projective. Therefore by Proposition 5.4, the right hand side surjection in each sequence is the direct sum of a projective cover of $\mathrm{Hom}_{\mathcal{O}}(N, M)$ and some projective $\mathcal{O}P$-lattice. It follows that, up to a projective direct summand, the kernel of each sequence is isomorphic to $\Omega(\mathrm{Hom}_{\mathcal{O}}(N, M))$. Thus there exist two projective $\mathcal{O}P$-lattices F and F' such that

$$\mathrm{End}_{\mathcal{O}}(M) \cong \Omega(\mathrm{Hom}_{\mathcal{O}}(N, M)) \oplus F\,,$$
$$\mathrm{End}_{\mathcal{O}}(N) \cong \Omega(\mathrm{Hom}_{\mathcal{O}}(N, M)) \oplus F'\,.$$

Note that F and F' are permutation $\mathcal{O}P$-lattices because they are free over $\mathcal{O}P$ by Proposition 21.1. Note also that a direct summand of a permutation module is a permutation module by Corollary 27.2. Therefore $\mathrm{End}_{\mathcal{O}}(M)$ is a permutation module if and only if $\Omega(\mathrm{Hom}_{\mathcal{O}}(N, M))$ is a permutation module, and this in turn holds if and only if $\mathrm{End}_{\mathcal{O}}(N)$ is a permutation module. This proves that M is an endo-permutation lattice if and only if N is an endo-permutation lattice. □

It should be noted that the class of endo-permutation $\mathcal{O}P$-lattices is not closed under direct sums (see Corollary 28.10 below), nor under induction (Exercise 28.1).

Apart from permutation modules, the Heller operator provides one of the main tools for constructing endo-permutation modules. One can start from a permutation module for a quotient group P/Q (for instance the trivial module), apply the Heller operator $\Omega^n_{P/Q}$ for the group P/Q, view the result as a module for P with Q acting trivially (the so-called *inflation* procedure), and then apply the Heller operator Ω^m_P for the group P. Repeating such operations yields a large variety of endo-permutation modules. It turns out that any indecomposable endo-permutation module over k for a cyclic p-group is obtained in this way (Exercise 28.3).

We have seen in the last section that if $A = \mathrm{End}_{\mathcal{O}}(M)$ is the endomorphism algebra of a permutation $\mathcal{O}P$-lattice M and if $Q \leq P$, then $\overline{A}(Q)$ is a simple k-algebra if it is non-zero (because it is the k-endomorphism algebra of $\overline{M}(Q)$). This is a very special property of the Brauer quotient and our aim is to show that it also holds for endo-permutation modules. We need some preliminary results.

(28.3) PROPOSITION. *Let A and B be two permutation G-algebras and let Q be a p-subgroup of G. There is an isomorphism of k-algebras $\overline{(A \otimes_{\mathcal{O}} B)}(Q) \cong \overline{A}(Q) \otimes_k \overline{B}(Q)$ mapping $br_Q(a \otimes b)$ to $br_Q(a) \otimes br_Q(b)$ (where $a \in A^Q$ and $b \in B^Q$).*

Proof. If X and Y are G-invariant bases of A and B respectively, then $Z = \{\, x \otimes y \mid x \in X, y \in Y \,\}$ is a G-invariant basis of $A \otimes_{\mathcal{O}} B$. By the first part of Proposition 27.6, $br_Q(X^Q)$ is a k-basis of $\overline{A}(Q)$. Similarly $br_Q(Y^Q)$ is a k-basis of $\overline{B}(Q)$ and $br_Q(Z^Q)$ is a k-basis of $\overline{(A \otimes_{\mathcal{O}} B)}(Q)$. But we clearly have $Z^Q = \{\, x \otimes y \mid x \in X^Q, y \in Y^Q \,\}$, and the result follows. □

Note that any element of $\overline{(A \otimes_{\mathcal{O}} B)}(Q)$ is in the image of $A^Q \otimes_{\mathcal{O}} B^Q$, but the algebra $(A \otimes_{\mathcal{O}} B)^Q$ is usually larger than $A^Q \otimes_{\mathcal{O}} B^Q$. Note also that the isomorphism of Proposition 28.3 is clearly an isomorphism of $\overline{N}_G(Q)$-algebras. Finally it should be mentioned that Proposition 28.3 holds more generally under the weaker assumption that only one of the two G-algebras A and B is a permutation G-algebra, but the proof is more elaborate.

(28.4) COROLLARY. *If A and B are Dade P-algebras, then $A \otimes_{\mathcal{O}} B$ is a Dade P-algebra.*

Proof. It is clear that $A \otimes_{\mathcal{O}} B$ is again a permutation P-algebra and Proposition 28.3 implies that $\overline{(A \otimes_{\mathcal{O}} B)}(Q) \neq 0$. Moreover $A \otimes_{\mathcal{O}} B$ is again $\mathcal{O}$-simple, because if $A \cong \mathrm{End}_{\mathcal{O}}(M)$ and $B \cong \mathrm{End}_{\mathcal{O}}(N)$, then $A \otimes_{\mathcal{O}} B \cong \mathrm{End}_{\mathcal{O}}(M \otimes_{\mathcal{O}} N)$. □

We shall need the following classical result about $\mathcal{O}$-simple algebras and their opposite algebras.

(28.5) LEMMA. *Let A be an $\mathcal{O}$-simple algebra.*
 (a) *There is an isomorphism of algebras $\phi : A \otimes_{\mathcal{O}} A^{op} \xrightarrow{\sim} \mathrm{End}_{\mathcal{O}}(A)$ induced by left and right multiplication.*
 (b) *If A is a P-algebra, then ϕ is an isomorphism of P-algebras (where $\mathrm{End}_{\mathcal{O}}(A)$ is the interior P-algebra associated with the $\mathcal{O}P$-module A).*

Proof. (a) By definition, $\phi(a \otimes b)(x) = axb$ for every $a, b, x \in A$. It is clear that ϕ is a homomorphism of algebras (and it is here that one needs the opposite multiplication). Since A is $\mathcal{O}$-simple, $A \cong M_n(\mathcal{O})$ for some n and we identify A with $M_n(\mathcal{O})$. Let e_{ij} be the basis element of A having the (i,j)-entry equal to 1 and all other entries zero. Then the elements $e_{ij} \otimes e_{kl}$ form a basis of $A \otimes A^{op}$. By a straightforward computation $\phi(e_{ij} \otimes e_{kl}) = E_{ijkl}$ is the $\mathcal{O}$-linear endomorphism of A mapping e_{jk} to e_{il} and all other basis elements to zero. But the elements E_{ijkl} form a basis of $\mathrm{End}_{\mathcal{O}}(A)$ and so ϕ maps a basis to a basis. Therefore ϕ is an isomorphism.

(b) Let $c_u \in \mathrm{End}_{\mathcal{O}}(A)$ be the action of $u \in P$ on A, that is, $c_u(a) = {}^u a$ for $a \in A$. The interior P-algebra structure on $\mathrm{End}_{\mathcal{O}}(A)$ is given by $u \cdot 1 = c_u$. For $a, b, x \in A$ and $u \in P$, we have

$$(\phi({}^u a \otimes {}^u b))(x) = {}^u a\, x\, {}^u b = c_u(a\, c_u^{-1}(x)\, b) = (c_u\, \phi(a \otimes b)\, c_u^{-1})(x),$$

and therefore $\phi({}^u a \otimes {}^u b) = c_u\, \phi(a \otimes b)\, c_u^{-1}$ as required. □

Note that in fact $A^{op} \cong A$ when A is $\mathcal{O}$-simple, the isomorphism being the transpose of matrices. But, in part (a), it is more natural to work with A^{op} because of the direct use of right multiplication. On the other hand, if A has a P-algebra structure, A^{op} need not be isomorphic to A as a P-algebra, so that the use of A^{op} is essential in part (b).

Now we can state the main result on the structure of the endomorphism algebra of an endo-permutation module. For later use we work with the more general case of an $\mathcal{O}$-simple permutation P-algebra.

(28.6) THEOREM. *Let* A *be an* $\mathcal{O}$*-simple permutation* P*-algebra and let* Q *be a subgroup of* P.

(a) *The* k*-algebra* $\overline{A}(Q)$ *is simple if it is non-zero.*

(b) *If* $\overline{A}(Q) \neq 0$, *then* $\overline{A}(R) \neq 0$ *for every subgroup* R *of* Q. *In particular if* A *is a Dade* P*-algebra, then* $\overline{A}(R) \neq 0$ *for every subgroup* R *of* P.

Proof. (a) By Lemma 28.5, there is an isomorphism of P-algebras $\phi : A \otimes_{\mathcal{O}} A^{op} \to \mathrm{End}_{\mathcal{O}}(A)$. The isomorphism ϕ necessarily induces an isomorphism between the Brauer quotients:

$$\overline{A}(Q) \otimes_k \overline{A}(Q)^{op} \cong \overline{(A \otimes_{\mathcal{O}} A^{op})}(Q) \xrightarrow{\sim} \overline{(\mathrm{End}_{\mathcal{O}}(A))}(Q),$$

using the isomorphism of Proposition 28.3 (and the obvious isomorphism $\overline{A^{op}}(Q) \cong \overline{A}(Q)^{op}$). But, since A is a permutation $\mathcal{O}P$-module, we have an isomorphism $\overline{(\mathrm{End}_{\mathcal{O}}(A))}(Q) \cong \mathrm{End}_k(\overline{A}(Q))$ by part (c) of Proposition 27.6. Now $\mathrm{End}_k(\overline{A}(Q))$ is a simple k-algebra (since it is the endomorphism algebra of a k-vector space) and therefore $\overline{A}(Q) \otimes_k \overline{A}(Q)^{op}$ is simple. This immediately implies that $\overline{A}(Q)$ is simple, because if I is a proper ideal of $\overline{A}(Q)$, then $I \otimes_k \overline{A}(Q)^{op}$ is a proper ideal of $\overline{A}(Q) \otimes_k \overline{A}(Q)^{op}$, hence is zero, forcing $I = 0$.

(b) By Proposition 27.6, $\overline{A}(Q)$ has a basis $br_Q(X^Q)$, where X is a P-invariant basis of A. Thus $\overline{A}(Q) \neq 0$ if and only if $X^Q \neq \emptyset$. Clearly $X^Q \neq \emptyset$ implies that $X^R \neq \emptyset$ for every subgroup R of Q. The special case of a Dade P-algebra follows immediately since $\overline{A}(P) \neq 0$ by definition. □

Theorem 28.6 has several important consequences. The first is that we do not leave the class of endo-permutation modules by passing to the Brauer quotient.

(28.7) COROLLARY. *Let* A *be an* $\mathcal{O}$*-simple permutation* P*-algebra and let* Q *be a subgroup of* P *such that* $\overline{A}(Q) \neq 0$.

(a) $\overline{A}(Q)$ *is a simple permutation* $\overline{N}_P(Q)$*-algebra.*

(b) *There exists a unique endo-permutation* $k\overline{N}_P(Q)$*-module* V_Q *(up to isomorphism) such that* $\overline{A}(Q) \cong \mathrm{End}_k(V_Q)$ *as* $\overline{N}_P(Q)$*-algebras.*

Proof. (a) Theorem 28.6 asserts that $\overline{A}(Q)$ is simple. If X is a P-invariant basis of A, then $br_Q(X^Q)$ is a basis of $\overline{A}(Q)$ (Proposition 27.6), which is $\overline{N}_P(Q)$-invariant. Thus $\overline{A}(Q)$ is a permutation $\overline{N}_P(Q)$-algebra.

(b) In view of part (a) and the fact that $\overline{A}(Q)$ is a k-algebra, this is a direct application of Lemma 28.1. □

The second consequence of the theorem is that we control entirely the poset of local points.

(28.8) PROPOSITION. *Let A be an $\mathcal{O}$-simple permutation P-algebra and let Q be a subgroup of P such that $\overline{A}(Q) \neq 0$.*
(a) There exists a unique local point δ of A^Q. Moreover the corresponding simple quotient of A^Q is $S(\delta) = \overline{A}(Q)$ and the multiplicity module of δ is the module V_Q of the previous corollary.
(b) If A is a Dade P-algebra, then the partially ordered set of local pointed groups on A is isomorphic to the partially ordered set of subgroups of P.

Proof. (a) Since $\overline{A}(Q)$ is simple by Theorem 28.6, it has a unique point. Thus A^Q has a unique local point δ since $\mathcal{LP}(A^Q) \cong \mathcal{P}(\overline{A}(Q))$ by Lemma 14.5. Since $\overline{A}(Q)$ is simple, it must be the simple quotient corresponding to δ. The assertion on the multiplicity module follows immediately.

(b) By (a) and by part (b) of Theorem 28.6, the set of local pointed groups on A is in bijection with the set of all subgroups of P. If $R_\delta \leq Q_\gamma$, then $R \leq Q$ by definition. Suppose conversely that $R \leq Q$, let δ be the unique local point of A^R, and let γ be the unique local point of A^Q. We have to prove that $R_\delta \leq Q_\gamma$, that is, $\mathrm{Ker}(br_R) \cap A^Q \subseteq \mathrm{Ker}(br_Q)$, using the fact that $\mathfrak{m}_\delta = \mathrm{Ker}(br_R)$ and $\mathfrak{m}_\gamma = \mathrm{Ker}(br_Q)$ by (a). Let X be a P-invariant basis of A. Let $a \in A^Q$, write $a = \sum_{x\in X} \lambda_x x$ with $\lambda_x \in \mathcal{O}$, and suppose that $a \notin \mathrm{Ker}(br_Q)$. Since $br_Q(X^Q)$ is a k-basis of $\overline{A}(Q)$ and $br_Q(a) \neq 0$, there exists $y \in X^Q$ such that $\lambda_y \notin \mathfrak{p}$. But since $X^Q \subseteq X^R$, the image $br_R(y)$ of y is also part of a basis of $\overline{A}(R)$ and therefore $br_R(a) \neq 0$. This proves the inclusion $\mathrm{Ker}(br_R) \cap A^Q \subseteq \mathrm{Ker}(br_Q)$ and completes the proof. □

We emphasize that for any local pointed group Q_δ on A, the multiplicity module $V(\delta)$, which is equal to the module V_Q, is a module over the ordinary group algebra $k\overline{N}_P(Q)$. Thus the usual twisted group algebra associated with a multiplicity algebra is here isomorphic to the ordinary group algebra.

(28.9) COROLLARY. *Let M be an endo-permutation $\mathcal{O}P$-lattice.*
(a) Let Q be any subgroup of P. If N_1 and N_2 are two indecomposable direct summands of $\mathrm{Res}^P_Q(M)$ with vertex Q, then $N_1 \cong N_2$.
(b) If $\overline{\mathrm{End}_{\mathcal{O}}(M)}(P) \neq 0$ (that is, if $\mathrm{End}_{\mathcal{O}}(M)$ is a Dade P-algebra), there is a unique isomorphism class of indecomposable direct summands of M with vertex P.

Proof. (a) By Example 13.4, the isomorphism class of N_i corresponds to a point δ_i of A^Q where $A = \mathrm{End}_{\mathcal{O}}(M)$. Since N_i has vertex Q , the point δ_i is local (Proposition 18.11). But there is a unique local point of A^Q by Proposition 28.8 above. Therefore $\delta_1 = \delta_2$, and this means that N_1 and N_2 are isomorphic.

(b) The condition $\overline{\mathrm{End}_{\mathcal{O}}(M)}(P) \neq 0$ means that there exists an indecomposable direct summand of M with vertex P . Thus the statement is a special case of (a). □

(28.10) COROLLARY. *Let M_1 and M_2 be two indecomposable endo-permutation $\mathcal{O}P$-lattices with vertex P . Then $M_1 \oplus M_2$ is an endo-permutation $\mathcal{O}P$-lattice if and only if M_1 and M_2 are isomorphic.*

Proof. If $M_1 \oplus M_2$ is an endo-permutation $\mathcal{O}P$-lattice, then $M_1 \cong M_2$ by Corollary 28.9. If $M_1 \cong M_2$, then $M_1 \oplus M_2 \cong M_1 \otimes_{\mathcal{O}} \mathcal{O}^2$, with P acting trivially on $\mathcal{O}^2$. Both M_1 and $\mathcal{O}^2$ are endo-permutation modules (because $\mathcal{O}^2$ is a permutation module) and therefore so is their tensor product by Proposition 28.2. □

Our next use of Theorem 28.6 is a useful result on dimensions.

(28.11) COROLLARY. *If A is a primitive Dade P-algebra, then we have* $\dim_{\mathcal{O}}(A) \equiv 1 \pmod{p}$. *If M is an indecomposable endo-permutation $\mathcal{O}P$-lattice with vertex P , then* $\dim_{\mathcal{O}}(M) \equiv \pm 1 \pmod{p}$.

Proof. Let M be an indecomposable endo-permutation $\mathcal{O}P$-lattice with vertex P and let $A = \mathrm{End}_{\mathcal{O}}(M)$. Since M is indecomposable, A is primitive, and since P is a vertex of M , it is a defect group of A (Proposition 18.11), so that A is a Dade P-algebra. Since $\dim(A) = \dim(M)^2$, it suffices to prove the statement about A .

We now prove the first statement. Since A is primitive, $\gamma = \{1_A\}$ is the unique point of A^P , with multiplicity one, and so the corresponding simple quotient of A^P is isomorphic to k . Since $\overline{A}(P) \neq 0$, the point γ is local. By part (a) of Proposition 28.8, it follows that $\overline{A}(P) \cong k$. If X is a P-invariant basis of A , then we know that $br_P(X^P)$ is a basis of $\overline{A}(P)$, and therefore X^P is a singleton. All the other elements of X belong to non-trivial orbits for the action of P , and since P is a p-group, all these non-trivial orbits have cardinality divisible by p . Therefore $|X| \equiv 1 \pmod{p}$. □

Our last application of Theorem 28.6 is the result announced earlier.

(28.12) PROPOSITION. *Let A be a Dade P-algebra. Then there exists an interior P-algebra structure on A inducing the given P-algebra structure.*

Proof. Since A is $\mathcal{O}$-simple, $A \cong \mathrm{End}_{\mathcal{O}}(M)$ for some $\mathcal{O}$-lattice M, and therefore M has a unique module structure over a twisted group algebra $\mathcal{O}_\sharp \widehat{P}$. We have to show that this twisted group algebra is isomorphic to the ordinary group algebra $\mathcal{O}P$, so that M becomes a module over $\mathcal{O}P$ and A becomes an interior P-algebra. By definition of a Dade P-algebra, $\overline{A}(P) \neq 0$ and therefore there exists a (unique) local point γ of A^P.

We first use localization to reduce to the case of a primitive Dade P-algebra. Let $i \in \gamma$ and let $A_\gamma = iAi \cong \mathrm{End}_{\mathcal{O}}(iM)$. Since A_γ is a direct summand of A as an $\mathcal{O}P$-lattice (see the proof of part (b) of Proposition 28.2), A_γ is an $\mathcal{O}$-simple permutation P-algebra, and $\overline{A}_\gamma(P) \neq 0$ as γ is still a local point of A_γ^P. Therefore A_γ is a Dade P-algebra. There is a twisted group algebra $\mathcal{O}_\sharp \widehat{P}'$ associated with A_γ, but Proposition 15.4 shows that the inclusion $A_\gamma \to A$ induces an isomorphism $\mathcal{O}_\sharp \widehat{P} \cong \mathcal{O}_\sharp \widehat{P}'$. Thus it suffices to show that $\mathcal{O}_\sharp \widehat{P}'$ is isomorphic to the ordinary group algebra. In other words we have reduced to proving the result for A_γ.

Since A_γ is a primitive Dade P-algebra, we know by Corollary 28.11 that $\dim(A_\gamma) \equiv 1 \pmod p$. Therefore, by Lemma 28.1, there exists an interior P-algebra structure on A_γ inducing the given P-algebra structure. This means precisely that the corresponding twisted group algebra is isomorphic to the ordinary group algebra, as was to be shown. □

Exercises

(28.1) Let Q be a normal p-subgroup of a p-group P and let M be an indecomposable endo-permutation $\mathcal{O}Q$-lattice with vertex Q.

(a) Assume that for some $u \in P$, the conjugate module ${}^uM$ is not isomorphic to M. Prove that $\mathrm{Ind}_Q^P(M)$ is not an endo-permutation $\mathcal{O}P$-lattice. [Hint: Show that both M and ${}^uM$ are direct summands of $\mathrm{Res}_Q^P \mathrm{Ind}_Q^P(M)$.]

(b) Construct explicit examples where the assumptions of (a) are satisfied. [Hint: Let Q be the direct product of two cyclic groups of order p and let P be the semi-direct product $Q \rtimes C_p$, where C_p has order p and acts on Q by fixing some subgroup Q_0 of order p and permuting transitively all the other subgroups of order p. Choose for M a non-trivial endo-permutation module for Q/R, where R is a subgroup of order p distinct from Q_0, and view M as a module for Q.]

(28.2) Let P be a p-group, let $\mathcal{O}_\sharp\widehat{P}$ be a twisted group algebra of P, let $M = \mathcal{O}_\sharp\widehat{P}$, viewed as an $\mathcal{O}_\sharp\widehat{P}$-module, and let $A = \mathrm{End}_\mathcal{O}(M)$.

(a) Prove that the action of $\widehat{P}$ on M induces an action of P on A and that A is an $\mathcal{O}$-simple permutation P-algebra.

(b) Prove that A can be given an interior P-algebra structure (inducing the given P-algebra structure) if and only if the central extension $\widehat{P}$ splits (that is, if and only if $\mathcal{O}_\sharp\widehat{P}$ is isomorphic to the ordinary group algebra).

(c) Let $B = \mathrm{End}_\mathcal{O}(\mathcal{O}P)$, constructed in a similar fashion using the ordinary group algebra $\mathcal{O}P$. Prove that $k \otimes_\mathcal{O} A \cong k \otimes_\mathcal{O} B$ as P-algebras; but if $\widehat{P}$ does not split, prove that A and B are not isomorphic as P-algebras.

(d) Construct examples where $\widehat{P}$ does not split. [Hint: Let $p = 2$, let $\mathcal{O}$ be such that $-1 \neq 1$ in $\mathcal{O}$, let Q be the quaternion group of order 8, let z be its central element of order 2, and let C be the quotient of the group algebra $\mathcal{O}Q$ by the ideal generated by $(z+1)$. Then C is a twisted group algebra of the Klein four-group $Q/\langle z \rangle$.]

(28.3) The purpose of this exercise is to classify indecomposable endo-permutation modules over k for a cyclic p-group. Let P be a cyclic group of order p^n generated by g. Recall (Exercises 5.4 and 17.2) that $kP \cong k[X]/(X-1)^{p^n}$, that $M_r = k[X]/(X-1)^r$ is the unique indecomposable kP-module of dimension r (up to isomorphism), and that for $1 \le r \le p^n$ this provides a complete list of indecomposable kP-modules (up to isomorphism).

(a) Write $r = ap^{n-1} + b$ with $0 \le a \le p$ and $0 \le b < p^{n-1}$. Let Q be the cyclic subgroup of P of order p generated by $g^{p^{n-1}}$. Prove that $\mathrm{Res}^P_Q(M_r)$ is isomorphic to the direct sum of b copies of the indecomposable kQ-module of dimension $a+1$ and of $(p^{n-1}-b)$ copies of the indecomposable kQ-module of dimension a. [Hint: Consider the action of $g^{p^{n-1}} - 1 = (g-1)^{p^{n-1}}$ on the basis $\{1, X, \ldots, X^{r-1}\}$ of M_r.]

(b) If $p^{n-1} < r < (p-1)p^{n-1}$, prove that M_r is not an endo-permutation module. [Hint: Deduce from (a) that the dimension of some summand of $\mathrm{Res}^P_Q(M_r)$ does not satisfy the required congruence modulo p.]

(c) If $r \ge (p-1)p^{n-1}$, use the Heller operator to reduce the classification problem to the case $r \le p^{n-1}$. If $r \le p^{n-1}$, prove that Q acts trivially on M_r, so that M_r is an indecomposable module for P/Q.

(d) Let $\mathcal{M}$ be the set of all indecomposable kP-modules obtained from the trivial module by repeated applications of the Heller operator and inflation. Prove that an indecomposable kP-module is an endo-permutation module if and only if it is either free or isomorphic to a module in $\mathcal{M}$.

(e) Prove that M_r is an endo-permutation module if and only if r can be written in the form

$$r = p^{e_0} - p^{e_1} + p^{e_2} - \ldots + (-1)^m p^{e_m}$$

where $n \geq e_0 > e_1 > e_2 > \ldots > e_m \geq 0$ and $0 \leq m \leq n$. Prove that if $p = 2$, then any indecomposable kP-module is an endo-permutation module.

(f) Prove that an endo-permutation module M_r has vertex P if and only if p does not divide r (that is, $e_m = 0$ in the notation of (e)). Prove that the number of isomorphism classes of indecomposable endo-permutation modules with vertex P is equal to 2^n if p is odd and 2^{n-1} if $p = 2$. [Hint: $p - 1 = 1$ if and only if $p = 2$.]

Notes on Section 28

The notion of endo-permutation module was introduced by Dade [1978a, 1978b], who also proved all the main results on their structure. The approach to the concept using Dade P-algebras rather than endo-permutation modules is due to Puig [1990a]. The generalization of Proposition 28.3 to the case in which only one of the two G-algebras is a permutation G-algebra appears in Puig [1988b].

§ 29 THE DADE GROUP OF A p-GROUP

This section is a short discussion of the Dade group of a p-group P. This is an abelian group of equivalence classes of Dade P-algebras.

We first describe the P-algebras which will form the unity element of the Dade group. A Dade P-algebra A is called *neutral* if $A \cong \mathrm{End}_{\mathcal{O}}(M)$ for some permutation $\mathcal{O}P$-lattice M. If M is an arbitrary permutation $\mathcal{O}P$-lattice, the corresponding P-algebra $A = \mathrm{End}_{\mathcal{O}}(M)$ is a Dade P-algebra (hence neutral) if and only if there exists a local point γ of A^P, that is, if and only if there exists an indecomposable direct summand M_γ of M with vertex P. But M_γ is again a permutation $\mathcal{O}P$-lattice, hence isomorphic to the indecomposable $\mathcal{O}P$-lattice $\mathrm{Ind}_Q^P(\mathcal{O})$ for some $Q \leq P$ (by Lemma 27.1 and the Krull–Schmidt theorem). Then Q is a vertex of M_γ (Lemma 27.1), so that $Q = P$ and $M_\gamma \cong \mathcal{O}$, the trivial $\mathcal{O}P$-lattice. Thus, for a permutation $\mathcal{O}P$-lattice M, the argument shows that $A = \mathrm{End}_{\mathcal{O}}(M)$ is a Dade P-algebra if and only if M has a direct summand isomorphic to the trivial $\mathcal{O}P$-lattice $\mathcal{O}$. In other words a neutral Dade P-algebra must be isomorphic to $\mathrm{End}_{\mathcal{O}}(M)$ for some permutation $\mathcal{O}P$-lattice M having at least one trivial direct summand.

The tensor product $A \otimes_{\mathcal{O}} B$ of two neutral Dade P-algebras A and B is again a neutral Dade P-algebra. Indeed on the one hand $A \otimes_{\mathcal{O}} B$ is again a Dade P-algebra (Corollary 28.4); on the other hand if M and N are permutation lattices, then so is $M \otimes_{\mathcal{O}} N$, and we have $\mathrm{End}_{\mathcal{O}}(M) \otimes_{\mathcal{O}} \mathrm{End}_{\mathcal{O}}(N) \cong \mathrm{End}_{\mathcal{O}}(M \otimes_{\mathcal{O}} N)$.

We first give the following important characterization of neutral Dade P-algebras.

(29.1) PROPOSITION. *Let A be a Dade P-algebra, let γ be the unique local point of A^P, and let $\mathcal{O}$ denote the trivial P-algebra of dimension 1. The following conditions are equivalent.*
(a) A is neutral.
(b) $A_\gamma \cong \mathcal{O}$.
(c) There exists an embedding of P-algebras $\mathcal{O} \to A$.

Proof. (a) $\Rightarrow$ (b). If A is neutral, then $A \cong \mathrm{End}_{\mathcal{O}}(M)$ for some permutation $\mathcal{O}P$-module M. The point γ corresponds to an isomorphism class of indecomposable direct summands M_γ of M and we have observed above that M_γ must be the trivial $\mathcal{O}P$-lattice. Therefore we have $A_\gamma \cong \mathrm{End}_{\mathcal{O}}(M_\gamma) \cong \mathrm{End}_{\mathcal{O}}(\mathcal{O}) \cong \mathcal{O}$.

(b) $\Rightarrow$ (c). This is trivial since an embedding associated with γ is an embedding $\mathcal{O} \to A$.

(c) $\Rightarrow$ (a). Let $f : \mathcal{O} \to A$ be a homomorphism of P-algebras belonging to the given embedding and let $i = f(1_{\mathcal{O}})$, so that $iAi \cong \mathcal{O}$. Since the primitivity of idempotents is preserved by embeddings, i is primitive in A. By $\mathcal{O}$-simplicity, $A \cong \mathrm{End}_{\mathcal{O}}(M)$ for some $\mathcal{O}$-lattice M, and by Lemma 7.1, M is the unique indecomposable projective A-module up to isomorphism. Therefore $M \cong Ai$ since i is primitive in A and Ai is indecomposable projective (Proposition 5.1). It follows that $A \cong \mathrm{End}_{\mathcal{O}}(Ai)$, the isomorphism being induced by the left action of A on Ai.

But as i is fixed under P, the decomposition $A = Ai \oplus A(1-i)$ is P-invariant, so that Ai is an $\mathcal{O}P$-lattice. Let $c_u \in \mathrm{End}_{\mathcal{O}}(Ai)$ be the action of $u \in P$ on Ai. Then $\mathrm{End}_{\mathcal{O}}(Ai)$ has an interior P-algebra structure (given by $u{\cdot}1 = c_u$). We check that the isomorphism $\phi : A \to \mathrm{End}_{\mathcal{O}}(Ai)$ induced by left multiplication is an isomorphism of P-algebras. For $a \in A$, $x \in Ai$, and $u \in P$, we have

$$(\phi({}^u a))(x) = {}^u a\, x = {}^u(a\ {}^{u^{-1}}x) = c_u(a\, c_u^{-1}(x)) = (c_u\, \phi(a)\, c_u^{-1})(x)\,,$$

as required. Since A is a permutation $\mathcal{O}P$-module by assumption, so is its direct summand Ai (Corollary 27.2). Therefore $A \cong \mathrm{End}_{\mathcal{O}}(Ai)$ is neutral. □

We can now define the equivalence relation. Two Dade P-algebras A and B are called *similar* if there exist two neutral Dade P-algebras S and T such that $A \otimes S \cong B \otimes T$. If A and B are similar (with S and T as above), and if B and C are similar (so that $B \otimes S' \cong C \otimes T'$ for some neutral Dade P-algebras S' and T'), then

$$A \otimes S \otimes S' \cong B \otimes T \otimes S' \cong B \otimes S' \otimes T \cong C \otimes T' \otimes T\,.$$

It follows that A and C are similar because $S \otimes S'$ and $T' \otimes T$ are neutral by a remark above. Therefore the similarity relation is transitive and it follows easily that it is an equivalence relation. We denote by $\mathcal{D}_{\mathcal{O}}(P)$ the set of equivalence classes.

The tensor product of two Dade P-algebras is again a Dade P-algebra by Corollary 28.4. An argument analogous to the above observations shows that, if A is similar to A' and B is similar to B', then $A \otimes_{\mathcal{O}} B$ is similar to $A' \otimes_{\mathcal{O}} B'$. Therefore the tensor product induces a commutative monoid structure on $\mathcal{D}_{\mathcal{O}}(P)$, with the class of neutral Dade P-algebras as unity element. Moreover the isomorphism $A \otimes_{\mathcal{O}} A^{op} \cong \mathrm{End}_{\mathcal{O}}(A)$ of Lemma 28.5 shows that the class of A^{op} is the inverse of the class of A. Indeed $\mathrm{End}_{\mathcal{O}}(A)$ is neutral since A is a permutation $\mathcal{O}P$-lattice by definition. Therefore $\mathcal{D}_{\mathcal{O}}(P)$ is a group, called the *Dade group* of P. In particular two Dade P-algebras A and B are similar if and only if $A \otimes_{\mathcal{O}} B^{op}$ is neutral.

For a Dade P-algebra A, we have seen in Proposition 29.1 that the property of being neutral can be seen in the localization A_γ, where γ is the unique local point of A^P. We now show that the similarity relation also has this property. The result also gives other characterizations of the equivalence relation.

(29.2) PROPOSITION. *Let A and B be two Dade P-algebras. Let γ (respectively δ) be the unique local point of A^P (respectively B^P). The following conditions are equivalent.*
(a) A and B are similar.
(b) $A_\gamma \cong B_\delta$.
(c) There exist a Dade P-algebra C and two embeddings of P-algebras $A \to C$ and $B \to C$.
(d) There exist a Dade P-algebra D and two embeddings of P-algebras $D \to A$ and $D \to B$.

Proof. (a) ⇒ (c). There exist two neutral Dade P-algebras S and T such that $A \otimes_{\mathcal{O}} S \cong B \otimes_{\mathcal{O}} T$ (by definition). By Proposition 29.1, $\mathcal{O}$ embeds into S and T. Therefore $A \cong A \otimes_{\mathcal{O}} \mathcal{O}$ embeds into $C = A \otimes_{\mathcal{O}} S$ and similarly $B \cong B \otimes_{\mathcal{O}} \mathcal{O}$ embeds into $B \otimes_{\mathcal{O}} T \cong C$.

(c) ⇒ (b). Let ε be the unique local point of C^P . Since there is an embedding $A \to C$, the local point γ of A^P maps to a local point of C^P (Proposition 15.1), which can only be ε . Therefore the localizations A_γ and C_ε are isomorphic (Proposition 15.1). Similarly there is an isomorphism $B_\delta \cong C_\varepsilon$, and it follows that $A_\gamma \cong B_\delta$.

(b) ⇒ (d). It suffices to choose $D = A_\gamma \cong B_\delta$.

(d) ⇒ (a). The given embeddings $D \to A$ and $D \to B$ induce an embedding $D \otimes_{\mathcal{O}} D^{op} \to A \otimes_{\mathcal{O}} B^{op}$. But $\mathcal{O}$ embeds into the neutral Dade P-algebra $D \otimes_{\mathcal{O}} D^{op}$ (Proposition 29.1), hence also into $A \otimes_{\mathcal{O}} B^{op}$. By Proposition 29.1 again, $A \otimes_{\mathcal{O}} B^{op}$ is neutral, and this means that A and B belong to the same class of the Dade group. In other words A and B are similar. □

(29.3) COROLLARY. *Let A and B be two primitive Dade P-algebras. Then A and B are similar if and only if they are isomorphic.*

Proof. The primitivity assumption means that $A = A_\gamma$ and $B = B_\delta$, and the result follows, using part (b) of Proposition 29.2. □

By Proposition 29.2, every similarity class of Dade P-algebras contains a unique primitive P-algebra, namely the localization A_γ , where A belongs to the class and γ is the unique local point of A^P . Therefore $\mathcal{D}_{\mathcal{O}}(P)$ can be reinterpreted (up to isomorphism) as the set of isomorphism classes of primitive Dade P-algebras. With this point of view, the product of two primitive Dade P-algebras A and B is obtained by taking the localization $(A \otimes_{\mathcal{O}} B)_\varepsilon$ of the tensor product, where ε is the unique local point of $(A \otimes_{\mathcal{O}} B)^P$.

If A is a Dade P-algebra, then clearly $k \otimes_{\mathcal{O}} A \cong A/\mathfrak{p}A$ is a Dade P-algebra over k (using the fact that $\overline{(A/\mathfrak{p}A)}(P) \cong \overline{A}(P) \neq 0$). It follows easily that reduction modulo $\mathfrak{p}$ induces a canonical group homomorphism $\mathcal{D}_{\mathcal{O}}(P) \to \mathcal{D}_k(P)$.

(29.4) PROPOSITION. *The group homomorphism* $\mathcal{D}_{\mathcal{O}}(P) \to \mathcal{D}_k(P)$ *is injective.*

Proof. Let A be a Dade P-algebra, let $B = A/\mathfrak{p}A$, let γ be the unique local point of A^P, and let $\overline{\gamma}$ be the image of γ in B. Since A has a P-invariant basis by definition, A^P has a basis consisting of orbit sums. Therefore the homomorphism $A^P \to B^P$ is surjective since it maps an $\mathcal{O}$-basis onto the corresponding k-basis. It follows that $\overline{\gamma}$ is a point of B^P, and it is still local (since $\overline{A}(P) \cong \overline{B}(P)$). Therefore $A_\gamma = iAi$ maps onto $B_{\overline{\gamma}} = \overline{i}B\overline{i}$ (where $i \in \gamma$), so that $B_{\overline{\gamma}} = A_\gamma/\mathfrak{p}A_\gamma$.

Assume now that B is neutral. By Proposition 29.1 (applied with k as a base ring), we have $B_{\overline{\gamma}} \cong k$. But as A_γ is an $\mathcal{O}$-lattice and $A_\gamma/\mathfrak{p}A_\gamma \cong k$, the dimension of A_γ as a free $\mathcal{O}$-module must be 1, and therefore $A_\gamma \cong \mathcal{O}$. By Proposition 29.1 again, A is neutral. This proves the injectivity of the map. □

(29.5) COROLLARY. *Let A and B be two primitive Dade P-algebras. If $A/\mathfrak{p}A \cong B/\mathfrak{p}B$ as P-algebras, then $A \cong B$.*

Proof. The assumption implies in particular that $A/\mathfrak{p}A$ and $B/\mathfrak{p}B$ are similar, so that A and B are similar by Proposition 29.4. But as A and B are primitive, they are isomorphic by Corollary 29.3. □

In fact the same result holds without the primitivity assumption, but the proof requires a little more work. We note that the question of the surjectivity of $\mathcal{D}_{\mathcal{O}}(P) \to \mathcal{D}_k(P)$ is an open problem.

(29.6) REMARK. There is also a version of the Dade group obtained by using capped endo-permutation modules rather than Dade P-algebras. An endo-permutation $\mathcal{O}P$-lattice M is said to be *capped* if $A = \mathrm{End}_{\mathcal{O}}(M)$ is a Dade P-algebra, or in other words if there exists a local point of A^P. This condition means that there exists an indecomposable direct summand of M with vertex P (necessarily unique up to isomorphism since the local point of A^P is unique), and this is called a *cap* of M. Two capped endo-permutation $\mathcal{O}P$-lattices M and N are similar if $M \otimes_{\mathcal{O}} S \cong N \otimes_{\mathcal{O}} T$ for some capped permutation $\mathcal{O}P$-lattices S and T. As in Proposition 29.2, this equivalence relation is equivalent to the condition that the caps of M and N are isomorphic. The equivalence classes again form a group, written $\mathcal{D}'_{\mathcal{O}}(P)$, the multiplication being induced by the tensor product. The unity element is the class of permutation $\mathcal{O}P$-lattices which are capped (that is, having at least one trivial direct summand). Each equivalence class contains (up to isomorphism) a unique indecomposable endo-permutation $\mathcal{O}P$-lattice with vertex P, namely the cap of any element of the class.

To each capped endo-permutation $\mathcal{O}P$-lattice M corresponds the Dade P-algebra $\mathrm{End}_{\mathcal{O}}(M)$, and this induces a canonical group homomorphism

$$d : \mathcal{D}'_{\mathcal{O}}(P) \longrightarrow \mathcal{D}_{\mathcal{O}}(P) .$$

By Proposition 28.12, d is surjective. If a class belongs to the kernel of d, the unique indecomposable endo-permutation $\mathcal{O}P$-lattice M in the class must be a one-dimensional $\mathcal{O}P$-lattice, mapping to the trivial P-algebra $\mathcal{O}$. The $\mathcal{O}P$-module structure of M is given by a group homomorphism $\lambda : P \to \mathcal{O}^*$, called a one-dimensional character of P. It follows that $\mathrm{Ker}(d) \cong \mathcal{X}(P)$, where $\mathcal{X}(P)$ denotes the group of one-dimensional characters of P. Moreover

$$\mathcal{D}'_{\mathcal{O}}(P) \cong \mathcal{X}(P) \times \mathcal{D}_{\mathcal{O}}(P) ,$$

because one can prove that the homomorphism d has a section. When p is odd, the section is obtained by mapping a primitive Dade P-algebra A to the unique indecomposable endo-permutation $\mathcal{O}P$-lattice M of determinant 1 such that $A \cong \mathrm{End}_{\mathcal{O}}(M)$ (Lemma 28.1). Note that this is possible because the dimension of A is prime to p by Corollary 28.11. Note also that it is not obvious that this section is a group homomorphism. Reduction modulo $\mathfrak{p}$ is no longer injective if one works with $\mathcal{D}'_{\mathcal{O}}(P)$. Indeed $\mathcal{X}(P)$ is precisely the kernel, since any one-dimensional module for P must be trivial over k.

(29.7) REMARK. The structure of the Dade group has been completely determined by Dade [1978b] when P is assumed to be abelian. In particular the group is finitely generated and $\mathcal{D}_{\mathcal{O}}(P) \cong \mathcal{D}_k(P)$. The finite generation also holds for arbitrary P by a result of Puig [1990a], but the complete structure of the Dade group is not known. Several interesting invariants in block theory lie in the Dade group and are expected to lie in fact in the torsion subgroup (see Section 50).

Exercises

(29.1) Let P be a cyclic p-group of order p^n . Prove that the Dade group $\mathcal{D}_k(P)$ is isomorphic to an elementary abelian 2-group of order 2^n (respectively 2^{n-1} if $p = 2$). [Hint: Show that every indecomposable kP-module is self-dual and deduce that every element of $\mathcal{D}_k(P)$ has order 2. Then use Exercise 28.3.]

(29.2) Let Q be a subgroup of a p-group P .
(a) Prove that if A is a Dade P-algebra, $\overline{A}(Q)$ is a Dade $\overline{N}_P(Q)$-algebra.
(b) Prove that the correspondence in (a) induces a group homomorphism $sl_Q : \mathcal{D}_\mathcal{O}(P) \to \mathcal{D}_k(\overline{N}_P(Q))$ (called a *slash map*).
(c) An endo-permutation $\mathcal{O}P$-lattice M is called *endo-trivial* if the permutation module $\mathrm{End}_\mathcal{O}(M)$ is the direct sum of a trivial $\mathcal{O}P$-lattice and a projective $\mathcal{O}P$-lattice. Prove that in that case the class of $\mathrm{End}_\mathcal{O}(M)$ is in the kernel of sl_Q for every non-trivial subgroup Q . Prove that the Heller translates $\Omega^n(\mathcal{O})$ of the trivial lattice are endo-trivial.
(d) Prove that if Q is a normal subgroup of P , then the group homomorphism $P \to P/Q$ induces a restriction map (often called inflation) $\mathrm{Inf}_Q : \mathcal{D}_k(P/Q) \to \mathcal{D}_k(P)$. Prove that Inf_Q is a section of sl_Q , and deduce that $\mathcal{D}_k(P) \cong \mathcal{D}_k(P/Q) \times \mathrm{Ker}(sl_Q)$.

(29.3) Prove that Corollary 29.5 may not hold for two primitive $\mathcal{O}$-simple permutation P-algebras A and B (without the condition $\overline{A}(P) \neq 0$ and $\overline{B}(P) \neq 0$). [Hint: Remember Exercise 28.2.]

Notes on Section 29

The Dade group of a p-group is a concept due to Dade [1978a, 1978b] (in the version described in Remark 29.6). The approach given here (using P-algebras rather than modules) is due to Puig [1988d, 1990a], who also extended the definition of the Dade group over k by defining a larger group which incorporates the Brauer group of the field k (in the case of a non-algebraically closed field). An induction argument (involving the slash maps of Exercise 29.2) was used by Dade [1978b] for the explicit description of the Dade group of an abelian p-group. The main point in Dade's argument is the proof that the Heller translates $\Omega^n(\mathcal{O})$ of the trivial lattice are the only endo-trivial $\mathcal{O}P$-lattices when P is abelian. The finite generation of the Dade group was proved by Puig [1990a], with the consequence that there are only finitely many self-dual indecomposable endo-permutation $\mathcal{O}P$-lattices with vertex P . A proof of Corollary 29.5 without the primitivity assumption appears in Puig [1990a].

§ 30 SOURCES OF SIMPLE MODULES FOR p-SOLUBLE GROUPS

The purpose of this section is to show that if G is a p-soluble group, then a source module of a simple kG-module is always an endo-permutation module. Recall that G is called *p-soluble* if there exists a series of normal subgroups

$$1 = H_0 < H_1 < \ldots < H_{n-1} < H_n = G$$

such that H_i/H_{i-1} is either a p-group or a group of order prime to p, for every $i \geq 1$. For instance any soluble group is p-soluble. Recall that $O_p(G)$ (respectively $O_{p'}(G)$) denotes the largest normal subgroup of G of order a power of p (respectively prime to p). If G is p-soluble and $G \neq 1$, then either $O_p(G) \neq 1$ or $O_{p'}(G) \neq 1$. Any quotient of a p-soluble group is p-soluble. In particular $O_{p'}(G/O_p(G)) \neq 1$ since $G/O_p(G)$ is p-soluble and $O_p(G/O_p(G)) = 1$. We shall need the following basic fact about p-soluble groups.

(30.1) LEMMA. *Let G be a p-soluble group. If both $O_p(G)$ and $O_{p'}(G)$ are central subgroups of G, then G is abelian.*

Proof. Let $\overline{G} = G/O_{p'}(G)$ and let $O_{p',p}(G)$ be the inverse image in G of $O_p(\overline{G})$. The central extension

$$1 \longrightarrow O_{p'}(G) \longrightarrow O_{p',p}(G) \longrightarrow O_p(\overline{G}) \longrightarrow 1$$

splits because the cohomology group $H^2(O_p(\overline{G}), O_{p'}(G))$ is trivial (since $O_p(\overline{G})$ and $O_{p'}(G)$ have coprime orders, see Proposition 1.18). Therefore $O_{p',p}(G) \cong O_{p'}(G) \times P$ (a direct product because $O_{p'}(G)$ is central), where P maps isomorphically onto $O_p(\overline{G})$. Since P is a normal Sylow p-subgroup of $O_{p',p}(G)$, it is characteristic, hence normal in G (because $O_{p',p}(G)$ is normal in G). Therefore $P \leq O_p(G)$. But since $O_p(G)$ maps into $O_p(\overline{G})$, it is contained in $O_{p',p}(G)$ and so $O_p(G) = P$. Therefore $O_{p',p}(G) \cong O_{p'}(G) \times O_p(G)$.

Now let $O_{p,p'}(\overline{G})$ be the inverse image in $\overline{G}$ of $O_{p'}(\overline{G}/O_p(\overline{G}))$. Since $O_p(G)$ is central and maps isomorphically onto $O_p(\overline{G})$, we have a central extension

$$1 \longrightarrow O_p(\overline{G}) \longrightarrow O_{p,p'}(\overline{G}) \longrightarrow O_{p'}(\overline{G}/O_p(\overline{G})) \longrightarrow 1\,.$$

Exchanging the role of p and p' in the argument above, we obtain in a similar way that $O_{p,p'}(\overline{G}) \cong O_p(\overline{G}) \times O_{p'}(\overline{G})$. But $O_{p'}(\overline{G}) = 1$ by definition of $\overline{G}$, and therefore $O_{p,p'}(\overline{G}) = O_p(\overline{G})$, or in other words $O_{p'}(\overline{G}/O_p(\overline{G})) = 1$. But we also have $O_p(\overline{G}/O_p(\overline{G})) = 1$ by construction of $\overline{G}/O_p(\overline{G})$. By a remark above, this forces the p-soluble group $\overline{G}/O_p(\overline{G})$ to be trivial. Therefore $\overline{G} = O_p(\overline{G})$, so that $G = O_{p',p}(G)$ and it follows that $G \cong O_{p'}(G) \times O_p(G)$ is abelian. □

We shall often use the following characterization of simple modules.

(30.2) LEMMA. *Let M be a kG-module and let $A = \mathrm{End}_k(M)$. Then M is a simple kG-module if and only if the image of G generates A as a k-vector space.*

Proof. M is a simple kG-module if and only if $\mathrm{End}_k(M)$ is isomorphic to one of the simple factors of $kG/J(kG)$, that is, if and only if $\mathrm{End}_k(M)$ is isomorphic to a quotient of the algebra kG. This holds if and only if the structural map $kG \to \mathrm{End}_k(M)$ is surjective, and this means that the image of G generates $\mathrm{End}_k(M)$ as a k-vector space. □

We shall need below to consider the more general situation of a not necessarily interior G-algebra $\mathrm{End}_k(M)$, in which case M becomes a module over a twisted group algebra $k_\sharp\widehat{G}$. The following simplicity criterion for M has the advantage of being expressed only in terms of the G-algebra structure of $\mathrm{End}_k(M)$ (that is, without mentioning the corresponding central extension $\widehat{G}$). Recall that an idempotent is called trivial if it is equal to either 0 or 1.

(30.3) LEMMA. *Let A be a simple G-algebra and write $A \cong \mathrm{End}_k(M)$ for some k-vector space M, so that M becomes a module over a twisted group algebra $k_\sharp\widehat{G}$. Then M is not a simple $k_\sharp\widehat{G}$-module if and only if there exists a non-trivial idempotent j of A such that jA is G-invariant.*

Proof. Let $\widehat{g}$ be an element of $\widehat{G}$ mapping onto $g \in G$. Recall that A is an interior $\widehat{G}$-algebra and that the action of g is equal to the conjugation by $\widehat{g}\cdot 1_A$. Let j be any idempotent of A. Since $A\cdot\widehat{g}^{-1} = A$, we have ${}^g(jA) \subseteq jA$ if and only if $\widehat{g}\cdot jA \subseteq jA$. Applying endomorphisms to elements $x \in M$, we now show that the latter inclusion holds if and only if $\widehat{g}\cdot jM \subseteq jM$. Indeed if $\widehat{g}\cdot jA \subseteq jA$, then $\widehat{g}\cdot j = ja$ for some $a \in A$ and therefore $\widehat{g}\cdot jx = jax \in jM$ for every $x \in M$. Conversely if $\widehat{g}\cdot jM \subseteq jM$, then for every $x \in M$, there exists $y \in M$ such that $\widehat{g}\cdot jx = jy$, and therefore $\widehat{g}\cdot jx = j^2y = j\cdot\widehat{g}\cdot jx$. It follows that $\widehat{g}\cdot j = j\cdot\widehat{g}\cdot j$, which implies that $\widehat{g}\cdot jA \subseteq jA$.

We have proved that jA is G-invariant if and only if jM is invariant under the action of $\widehat{G}$, which means that jM is a $k_\sharp\widehat{G}$-submodule of M. Now any k-subspace of M is equal to jM for some idempotent j of A, and jM is non-zero and proper if and only if j is a non-trivial idempotent. The result follows. □

In the special case where the idempotent j itself is G-invariant (so that jA is G-invariant), we note that the submodule jM is a direct summand of M.

The following lemma is the main step for the proof of the result on p-soluble groups.

(30.4) LEMMA. *Assume that G is a p-soluble group. Let M be a simple kG-module, let $A = \mathrm{End}_k(M)$, and assume that M is not induced from a proper subgroup of G. Then there exists a finite subgroup L of A^* with the following three properties:*
(a) L has order prime to p.
(b) L is invariant under the action of G.
(c) L generates A as a k-vector space.

Proof. We proceed by induction on the order of $G/Z(G)$, where $Z(G)$ denotes the centre of G. Suppose first that $|G/Z(G)| = 1$, which means that G is abelian. Then the simple algebra A is commutative (because by Lemma 30.2, A is generated by G), and so $A \cong k$. Then the trivial subgroup $L = 1$ has the required properties. Therefore we can assume now that $|G/Z(G)| > 1$, so that G is non-abelian.

Suppose first that $O_{p'}(G)$ is a central subgroup of G. The normal p-subgroup $P = O_p(G)$ is not central by Lemma 30.1. By Corollary 21.2, P acts trivially on M, and M can be viewed as a simple module for $k(G/P)$ (and again M cannot be induced from a proper subgroup of G/P). Since P is not central, $Z(G) < Z(G)P$, so that $Z(G)P/P$ is a central subgroup of G/P of index strictly smaller than $|G/Z(G)|$. Thus the induction hypothesis applies to G/P and there exists a subgroup L with the required properties. Note that L is G/P-invariant, hence G-invariant since P acts trivially on A.

Assume now that $H = O_{p'}(G)$ is not central in G. Consider the structural algebra homomorphism $\phi : kG \to A$, which is surjective by Lemma 30.2. Let S be the image of the subalgebra kH. We want to show that S is a simple algebra, and that S is G-invariant.

Since $\phi(1_{kG}) = 1_A \neq 0$, there exists a primitive idempotent e of the centre $Z(kH)$ of kH such that $\phi(e) \neq 0$. Since H is a normal subgroup of G, the group G acts by conjugation on kH, hence also on the centre $Z(kH)$. Let F be the stabilizer of e in G. If $g \notin F$, then ${}^g e$ is distinct from e, hence orthogonal to e because $Z(kH)$ is commutative (Corollary 4.2), and therefore $t_F^G(e) = \sum_{g\in[G/F]} {}^g e$ is an orthogonal idempotent decomposition in $Z(kH)$. Moreover $t_F^G(e)$ is fixed under G, hence commutes with G, and therefore $t_F^G(e)$ lies in $Z(kG)$. Thus its image $\phi(t_F^G(e))$ is a central idempotent of A. Since $\phi(e) \neq 0$ and since the decomposition $\phi(t_F^G(e)) = t_F^G(\phi(e)) = \sum_{g\in[G/F]} {}^g(\phi(e))$ is orthogonal, $\phi(t_F^G(e))$ is non-zero. But as A is simple, the centre of A is $k{\cdot}1_A$, and the unique non-zero central idempotent of A is 1_A. Therefore $\phi(t_F^G(e)) = 1_A$.

We now have an orthogonal decomposition $1_A = \sum_{g\in[G/F]} {}^g f$ where $f = \phi(e)$. Therefore M decomposes as

$$M = \bigoplus_{g\in[G/F]} {}^g fM\,,$$

and since f is F-invariant, fM is a kF-submodule of M. By construction of induced modules, it follows that $M \cong \mathrm{Ind}_F^G(fM)$. But by assumption M is not induced from a proper subgroup, so that $F = G$ and $f = 1_A$. This shows that the primitive idempotent e of $Z(kH)$ maps to 1_A under ϕ (and also that e is G-invariant). Therefore $\phi(1-e) = 0$ and $\phi(e') = 0$ for every primitive idempotent of $Z(kH)$ distinct from e.

Since $H = O_{p'}(G)$ has order prime to p, the group algebra kH is semi-simple (Theorem 17.5), hence isomorphic to a direct product of simple algebras $kH \cong \prod_\alpha S_\alpha$. Therefore $Z(kH) \cong \prod_\alpha k$ and the primitive idempotent e is the unity element of one of the simple factors S_α. It follows that this simple factor is mapped by ϕ isomorphically onto the image $S = \phi(kH)$ and that all the other simple factors are mapped to zero (because $\phi(e) = 1$ and $\phi(e') = 0$ for every primitive idempotent of $Z(kH)$ distinct from e). This proves that S is a simple algebra, as required. Now kH is a G-algebra (because H is a normal subgroup) and $kH \to A$ is clearly a homomorphism of G-algebras. Therefore its image S is G-invariant.

Now S is a simple subalgebra of the algebra $A = \mathrm{End}_k(M)$ and Proposition 7.5 applies. Thus, if we let $T = C_A(S)$, there is an isomorphism of algebras $A \cong S \otimes_k T$ and $T \cong iAi$ where i is a primitive idempotent of S. In particular T is also simple (because A is simple) and we write $T \cong \mathrm{End}_k(V)$ for some k-vector space V (namely $V = iM$ since $iAi \cong \mathrm{End}_k(iM)$). Since S is G-invariant, so is its centralizer T. Moreover since the image of H is contained in S, it centralizes T, and therefore the action of H on T is trivial. On the other hand the image of $Z(G)$ in A is central (because the image of G generates A by Lemma 30.2), hence is contained in the group of scalars $k^*{\cdot}1_A$. Therefore $Z(G)$ acts trivially on A and it follows that $Z(G)H$ acts trivially on T. Thus T is a simple $\overline{G}$-algebra, where $\overline{G} = G/Z(G)H$, and so V is a module over some twisted group algebra $k_\sharp\widehat{\overline{G}}$.

We use Lemma 30.3 to prove that V is a simple $k_\sharp\widehat{\overline{G}}$-module. If it were not simple, then jT would be $\overline{G}$-invariant (in other words G-invariant) for some non-trivial idempotent j of T. Then $1\otimes j$ would be a non-trivial idempotent of $S\otimes_k T$ and $(1\otimes j)(S\otimes_k T) = S\otimes_k jT$ would be G-invariant. This is impossible by Lemma 30.3 again, since $S\otimes_k T \cong A \cong \mathrm{End}_k(M)$ and M is a simple kG-module by assumption.

By Proposition 10.5, $k_\sharp\widehat{\overline{G}}$ is isomorphic to a quotient of a group algebra kG', where G' is a finite group which is a central extension of $\overline{G}$ by a central subgroup Z of order prime to p. Thus V is a simple kG'-module, and we now show that V is not induced from a proper subgroup. If V is induced from some subgroup E', then

$$V = \bigoplus_{g'\in[G'/E']} {}^{g'}iV \cong \mathrm{Ind}_{E'}^{G'}(iV)$$

for some idempotent $i\in T^{E'}$, and so $\sum_{g'\in[G'/E']} {}^{g'}i = 1_T$ is an orthogonal decomposition. Since the central subgroup Z acts trivially on T (because it maps into the centre of T by Lemma 30.2), the stabilizer E' of i contains Z. Thus if $\overline{E}$ denotes the image of E' in $\overline{G} = G'/Z$, we have $\sum_{\overline{g}\in[\overline{G}/\overline{E}]} {}^{\overline{g}}i = 1_T$. And if in turn E denotes the inverse image of $\overline{E}$ in G, then we obtain an orthogonal decomposition $\sum_{g\in[G/E]} {}^{g}i = 1_T$. Now in the tensor product $S\otimes_k T$, we have an orthogonal decomposition

$$\sum_{g\in[G/E]} {}^{g}(1_S\otimes i) = 1_S\otimes\big(\sum_{g\in[G/E]} {}^{g}i\big) = 1_S\otimes 1_T\,,$$

which shows that the interior G-algebra $\mathrm{End}_k(M) = A \cong S\otimes_k T$ is induced from E (Proposition 16.6). Equivalently this means that the kG-module M is induced from E. By assumption we must have $E=G$, hence $\overline{E}=\overline{G}$ and $E'=G'$. This completes the proof that V is not induced from a proper subgroup.

The central subgroup Z of G' has index $|\overline{G}| = |G/Z(G)H|$, which is strictly smaller than $|G/Z(G)|$ since H is not central in G. Therefore the induction hypothesis applies and there exists a finite subgroup L' of T, of order prime to p, generating T, and invariant under G'. Then L' is invariant under $\overline{G}$ (because the central subgroup Z acts trivially on T), and so L' is G-invariant. On the other hand S is the image of kH, so that the image H' of H in S generates S. Moreover H' has order prime to p and is G-invariant (because H is a normal subgroup of G). It follows that the set $L = \{h\otimes l \mid h\in H',\, l\in L'\}$ is a finite subgroup of $S\otimes_k T$, of order prime to p, generating $S\otimes_k T$, and invariant under G. This completes the proof since $S\otimes_k T\cong A$. $\square$

Now we come to the main result.

(30.5) THEOREM. *Let G be a p-soluble group, let M be a simple kG-module, let P be a vertex of M, and let the kP-module N be a source of M. Then N is an endo-permutation kP-module.*

Proof. If M is induced from a subgroup H, then $M = \mathrm{Ind}_H^G(M')$ for some kH-module M' which is necessarily simple (because if L is a submodule of M', then $\mathrm{Ind}_H^G(L)$ is a submodule of $\mathrm{Ind}_H^G(M')$). If the kP'-module N' is a source of M', we claim that N' is also a source of M. Then since all sources are conjugate (Theorem 18.3), there exists $g \in G$ such that ${}^gP = P'$ and ${}^gN \cong N'$. Thus N is an endo-permutation kP-module if and only if N' is an endo-permutation kP'-module. It follows that it suffices to prove the theorem for a simple module which is not induced from a proper subgroup.

We first prove the above claim. By Proposition 18.11, N' is not projective relative to a proper subgroup of P' and is isomorphic to a direct summand of $\mathrm{Res}_{P'}^H(M')$, and M' is isomorphic to a direct summand of $\mathrm{Ind}_{P'}^H(N')$. It follows that M is isomorphic to a direct summand of $\mathrm{Ind}_{P'}^G(N')$. Moreover since M' is isomorphic to a direct summand of $\mathrm{Res}_H^G \mathrm{Ind}_H^G(M') = \mathrm{Res}_H^G(M)$, it also follows that N' is isomorphic to a direct summand of $\mathrm{Res}_{P'}^G(M)$. Thus by the reverse implication in Proposition 18.11 (b), we see that N' is a source of M.

Now we assume that M is not induced from a proper subgroup. By Lemma 30.4, there exists a G-invariant finite subgroup L of $A = \mathrm{End}_k(M)$ such that L has order prime to p and generates A. By Lemma 30.2, the latter condition implies that M is a simple kL-module, so that A is isomorphic to a simple quotient of kL. But kL is semi-simple because L has order prime to p (Theorem 17.5), and therefore $kL \cong A \times B$, where B is the direct product of all the other simple quotients of kL. Now L is G-invariant so that G acts on kL by permuting the basis elements. As for any G-algebra, G must permute the simple quotients of kL. But as G stabilizes A by construction, G permutes the other simple quotients of kL. In other words G stabilizes B. This means that if we now view kL as a permutation kG-module, we have $kL \cong A \oplus B$. Thus on restriction to P, the summand A is a direct summand of a permutation kP-module. By Corollary 27.2, A is again a permutation kP-module.

Now the source module N is isomorphic to iM for some idempotent $i \in A^P$, and A decomposes as a kP-module:

$$A = iAi \oplus iA(1-i) \oplus (1-i)Ai \oplus (1-i)A(1-i)\,.$$

Therefore iAi is a permutation kP-module (by Corollary 27.2 again). This completes the proof since $iAi \cong \mathrm{End}_k(iM) \cong \mathrm{End}_k(N)$. □

The main result of this section does not hold for arbitrary groups, as the following example shows.

(30.6) EXAMPLE. Let $\mathbb{F}_4$ be the finite field with 4 elements, generated by the element λ with $\lambda^2+\lambda+1=0$. Consider the group $G=SL_2(\mathbb{F}_4)$ (isomorphic to the alternating group A_5). This is a simple group of order 60 and it is the smallest finite group which is not 2-soluble. The set P of upper-triangular matrices (with ones on the diagonal) is a Sylow 2-subgroup of G, isomorphic to the direct product of two cyclic groups of order 2. The matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$$

generate P. If k is an algebraically closed field of characteristic 2 containing $\mathbb{F}_4$, the inclusion $\mathbb{F}_4 \to k$ defines a 2-dimensional representation $\rho : SL_2(\mathbb{F}_4) \to GL_2(k)$, called the natural representation, which is easily seen to be irreducible. The source of this simple kG-module is its restriction to P (because this restriction is indecomposable and has vertex P as a kP-module, as the reader can check). Finally this two dimensional representation of P (given by the above two matrices) is not an endo-permutation module, because its dimension is not congruent to ± 1 modulo 2 (Corollary 28.11).

Theorem 30.5 is connected with a conjecture of Feit on sources of simple kG-modules. Given a finite p-group P and a kP-module M, one says that M is a *source of a simple module* if there exists a finite group G containing P and a simple kG-module N such that P is a vertex of N and M is a source of N. Of course M has to be indecomposable and have vertex P.

(30.7) CONJECTURE (Feit). *Let P be a finite p-group. There are only finitely many isomorphism classes of kP-modules which are sources of a simple module.*

A positive answer to this conjecture would mean in particular that infinitely many simple modules for non-isomorphic groups G would all have the same source. The conjecture also raises the problem of classifying all possible sources of a simple module, for a given p-group P. We mention without proof that there is such a finiteness result if one bounds the dimension of source modules.

(30.8) THEOREM. *Let P be a finite p-group and let n be a positive integer. There are only finitely many isomorphism classes of kP-modules of dimension at most n which are sources of a simple module.*

A weaker form of Feit's conjecture is obtained by specifying a class of finite groups, and asking for finitely many isomorphism classes of kP-modules which are sources of a simple module for some group G in the class. In the special case of the class of p-soluble groups, there is the following theorem, which we state without proof.

(30.9) THEOREM. *Let P be a p-group. There are finitely many isomorphism classes of kP-modules which are sources of a simple module for some p-soluble group G.*

Since Theorem 30.5 asserts that only an endo-permutation module can be such a source, the proof consists in the analysis of the type of endo-permutation modules M which can occur. In fact $\mathrm{End}_k(M)$ must satisfy the additional properties appearing in Lemma 30.4, namely the existence of a P-invariant subgroup L of order prime to p and generating $\mathrm{End}_k(M)$. Puig has proved that there are only finitely many isomorphism classes of such kP-modules. The proof is beyond the scope of this book. It uses the fact that the automorphism group of a finite simple group of order prime to p has cyclic Sylow p-subgroups, a result which is a consequence of the classification of finite simple groups.

Exercises

(30.1) Let G be a p-soluble group, let M be a simple kG-module, and assume that M is not induced from a proper subgroup of G. Prove that $\mathrm{End}_k(M)$ is a p-permutation kG-module. [Hint: Examine the proof of the main result of this section.]

(30.2) Recall that G is called *p-nilpotent* if $G/O_{p'}(G)$ is a p-group.
(a) Prove that if G is a p-nilpotent group, then the subgroup L appearing in the statement of Lemma 30.4 can be chosen to be the image of $O_{p'}(G)$.
(b) Prove that if G is a p-nilpotent group and $O_{p'}(G)$ is abelian, then a source of a simple kG-module is necessarily the trivial module.

(30.3) Prove all the statements in Example 30.6.

Notes on Section 30

In the special case of p-nilpotent groups, the main result of this section is due to Dade [1978b]. The proof of the general case which we have given appears in Puig [1988d]. Feit's conjecture 30.7 was first stated at the 1979 Santa Cruz Conference on finite groups and appears (in a weaker form) in Feit [1980]. Theorem 30.8 is due to Dade [1982] (another proof was given by Picaronny [1987]) and Theorem 30.9 is due to Puig [1988d].

§ 31 DIAGRAMS

Recall that a *finite oriented graph* is a triple (D, E, μ) where D and E are finite sets and $\mu : E \to D \times D$ is a map. The elements of D are called *vertices* and those of E are called *edges*. For every edge $e \in E$, the first component d_1 of $\mu(e) = (d_1, d_2)$ is called the *origin* of e and d_2 is called the *extremity* of e. As usual we abusively identify a graph with its set D of vertices. Notice that several edges may have same origin and extremity.

Let D be a finite oriented graph. An *$\mathcal{O}G$-diagram of shape D* consists of a family of $\mathcal{O}G$-modules M_d, indexed by the set D of vertices, and a family of $\mathcal{O}G$-linear maps f_e, indexed by the set E of edges, such that if d_1 and d_2 are respectively the origin and extremity of an edge e, then $f_e : M_{d_1} \to M_{d_2}$ is a map from M_{d_1} to M_{d_2}. We view an $\mathcal{O}G$-diagram as a pair (M, f), where M is a function from D to $\mathcal{O}G$-modules taking the value M_d on $d \in D$, and similarly f is a function from E to $\mathcal{O}G$-linear maps. We recall that by an $\mathcal{O}G$-module, we always mean a finitely generated left $\mathcal{O}G$-module. An $\mathcal{O}G$-diagram of shape D is often called a *representation* of the graph D by $\mathcal{O}G$-linear maps.

Given two $\mathcal{O}G$-diagrams (M, f) and (M', f') of shape D, we define an $\mathcal{O}G$-linear homomorphism $\psi : (M, f) \to (M', f')$ to be a family of $\mathcal{O}G$-linear maps $\psi_d : M_d \to M'_d$, indexed by the set D of vertices, such that for every edge e with origin d_1 and extremity d_2, we have $f'_e \, \psi_{d_1} = \psi_{d_2} \, f_e$. We write $\mathrm{Hom}_{\mathcal{O}G}((M, f), (M', f'))$ for the $\mathcal{O}$-module of all $\mathcal{O}G$-linear homomorphisms from (M, f) to (M', f'). In particular, if $(M, f) = (M', f')$, we obtain the algebra $\mathrm{End}_{\mathcal{O}G}(M, f)$ of all $\mathcal{O}G$-linear endomorphisms of (M, f). For a fixed oriented graph D, the $\mathcal{O}G$-diagrams of shape D together with the $\mathcal{O}G$-linear homomorphisms form a category (which is abelian). If H is a subgroup of G, there is an obvious restriction functor, sending an $\mathcal{O}G$-diagram (M, f) to the $\mathcal{O}H$-diagram $\mathrm{Res}^G_H(M, f)$ of the same shape. In particular $\mathrm{End}_{\mathcal{O}}(M, f)$ is the algebra of $\mathcal{O}$-linear endomorphisms of $\mathrm{Res}^G_1(M, f)$.

With every $\mathcal{O}G$-diagram (M, f) is associated an interior G-algebra $A = \mathrm{End}_{\mathcal{O}}(M, f)$. The algebra structure has been defined above and the interior structure is described in the following way. By definition A is a subalgebra of $\prod_{d\in D} \mathrm{End}_{\mathcal{O}}(M_d)$. As every $\mathrm{End}_{\mathcal{O}}(M_d)$ is an interior G-algebra (Example 10.6), there is a map

$$\phi : G \longrightarrow \prod_{d\in D} \mathrm{End}_{\mathcal{O}}(M_d) , \quad g \mapsto (g{\cdot}id_{M_d})$$

and the image of ϕ lies in A. Indeed for each edge e, the map f_e is $\mathcal{O}G$-linear by definition of a diagram, hence commutes with the family of maps $(g{\cdot}id_{M_d})$. Therefore $(g{\cdot}id_{M_d})_{d\in D}$ belongs to A^* and this defines the interior G-algebra structure on A.

Given a subgroup H of G, an element $\psi \in \mathrm{End}_{\mathcal{O}}(M, f)$ is fixed under H if and only if each component ψ_d is fixed under H, which means that $\psi_d \in \mathrm{End}_{\mathcal{O}H}(M_d)$, that is, $\psi \in \mathrm{End}_{\mathcal{O}H}(M, f)$. Therefore $\mathrm{End}_{\mathcal{O}}(M, f)^H = \mathrm{End}_{\mathcal{O}H}(M, f)$, as in the case of $\mathcal{O}G$-modules.

In the definition of an $\mathcal{O}G$-diagram, one can impose conditions on the homomorphisms f_e to obtain the notion of diagram with relations. For instance one can require some composites to be zero, or some linear combination of maps to be zero. We do not give a formal definition, but in the following examples, we simply mention when there are relations. We start with the most elementary case.

(31.1) EXAMPLE. Let D be the graph with a single vertex and no edge. Then an $\mathcal{O}G$-diagram of shape D is just an $\mathcal{O}G$-module M. Thus arbitrary diagrams are generalizations of modules.

(31.2) EXAMPLE. Let D be the graph $d_1 \xrightarrow{e} d_2$. Let (M, f) be an $\mathcal{O}G$-diagram of shape D and assume that M_{d_1} is a projective module and that $f_e : M_{d_1} \to M_{d_2}$ is surjective. In that case the interior G-algebra $\mathrm{End}_{\mathcal{O}}(M, f)$ has already been encountered in Exercise 25.4: there is a strict covering exomorphism $\mathrm{End}_{\mathcal{O}}(M, f) \to \mathrm{End}_{\mathcal{O}}(M_{d_2})$.

(31.3) EXAMPLE. Let D be the graph $d_n \xrightarrow{e_n} d_{n-1} \xrightarrow{e_{n-1}} \ldots \xrightarrow{e_1} d_0$. Then an $\mathcal{O}G$-diagram of shape D is a *complex* of $\mathcal{O}G$-modules provided it satisfies the relations $f_{e_i} f_{e_{i+1}} = 0$ for $1 \le i \le n-1$.

(31.4) EXAMPLE. Let D be the graph $d_1 \xrightarrow{e} d_2 \xrightarrow{e'} d_3$. Any short exact sequence of $\mathcal{O}G$-modules is an $\mathcal{O}G$-diagram of shape D with extra conditions, namely the injectivity of f_e, the surjectivity of $f_{e'}$, and the equality $\mathrm{Ker}(f_{e'}) = \mathrm{Im}(f_e)$.

We want to extend to $\mathcal{O}G$-diagrams some properties already shown in the case of modules. Note first that the analogue of Lemma 10.7 does not hold: with two non-isomorphic $\mathcal{O}G$-diagrams of shape D may be associated two isomorphic interior G-algebras (Exercise 31.1). Thus $\mathrm{End}_{\mathcal{O}}(M, f)$ does not reflect the whole structure of (M, f).

We fix a finite oriented graph D and we consider various constructions and properties for $\mathcal{O}G$-diagrams of shape D. The direct sum of two $\mathcal{O}G$-diagrams (M, f) and (M', f') is the $\mathcal{O}G$-diagram

$$(M, f) \oplus (M', f') = (M \oplus M', f \oplus f'),$$

where $(M \oplus M')_d = M_d \oplus M'_d$ for every vertex d and $(f \oplus f')_e = f_e \oplus f'_e$ for every edge e. The composite of the projection and the inclusion

$$(M \oplus M', f \oplus f') \longrightarrow (M, f) \longrightarrow (M \oplus M', f \oplus f')$$

is an idempotent $i \in \mathrm{End}_{\mathcal{O}G}(M \oplus M', f \oplus f')$, and for every vertex d, the d-th component of i is an idempotent $i_d \in \mathrm{End}_{\mathcal{O}G}(M_d \oplus M'_d)$ whose image is M_d.

Conversely if (M, f) is an $\mathcal{O}G$-diagram and $i \in \mathrm{End}_{\mathcal{O}G}(M, f)$ is an idempotent, then the image of i is a direct summand of (M, f), written (iM, if). Indeed i_d is an idempotent for every vertex d, so that $i_d M_d$ is a direct summand of M_d. Moreover, by definition of $\mathrm{End}_{\mathcal{O}G}(M, f)$, we have $f_e\, i_{d_1} = i_{d_2}\, f_e$ for every edge e with origin d_1 and extremity d_2, and this implies that $f_e(i_{d_1} M_{d_1}) \subseteq i_{d_2} M_{d_2}$. Thus we obtain a diagram consisting of the family $\{i_d M_d\}$ together with the restrictions of the maps f_e (which we write in short as either if or fi in view of the equation above). We clearly have a decomposition $(M, f) = (iM, if) \oplus ((1{-}i)M, (1{-}i)f)$. An $\mathcal{O}G$-diagram is called *indecomposable* if it is non-zero and if it cannot be decomposed as a direct sum of two non-zero $\mathcal{O}G$-diagrams. Thus a direct summand (iM, if) of (M, f) is indecomposable if and only if i is a primitive idempotent of $\mathrm{End}_{\mathcal{O}G}(M, f)$. In particular an $\mathcal{O}G$-diagram (M, f) is indecomposable if and only if $\mathrm{End}_{\mathcal{O}}(M, f)$ is a primitive G-algebra.

The correspondence between direct summands and idempotents immediately implies that the Krull–Schmidt theorem holds for $\mathcal{O}G$-diagrams, thanks to our assumption that $\mathcal{O}$ is complete (see Theorem 4.4). Corollary 4.5 also generalizes to diagrams, as follows.

(31.5) PROPOSITION. *Let D be a finite oriented graph and let (M, f) be an $\mathcal{O}G$-diagram of shape D.*

(a) The Krull–Schmidt theorem holds for the direct summands of (M, f).

(b) Two idempotents i and j of $\mathrm{End}_{\mathcal{O}G}(M, f)$ are conjugate if and only if the direct summands (iM, if) and (jM, jf) are isomorphic.

This shows that a point of $\mathrm{End}_{\mathcal{O}G}(M, f)$ corresponds to an isomorphism class of direct summands of (M, f). Lemma 12.4 also extends to diagrams.

(31.6) LEMMA. *Let* D *be a finite oriented graph, let* (M,f) *be an* $\mathcal{O}G$*-diagram of shape* D *, and let* $i \in \mathrm{End}_{\mathcal{O}G}(M,f)$ *be an idempotent. Then the interior* G*-algebras* $\mathrm{End}_{\mathcal{O}}(iM,if)$ *and* $i\,\mathrm{End}_{\mathcal{O}}(M,f)i$ *are isomorphic.*

Proof. For each vertex $d \in D$, let $\psi_d \in i_d\,\mathrm{End}_{\mathcal{O}}(M_d)i_d$ and let $\phi_d \in \mathrm{End}_{\mathcal{O}}(i_dM_d)$ be its image under the isomorphism of Lemma 12.4. It is an easy exercise to check that the family $\psi = (\psi_d)$ is an endomorphism of the diagram (M,f) (that is, $\psi \in i\,\mathrm{End}_{\mathcal{O}}(M,f)i$) if and only if the family $\phi = (\phi_d)$ is an endomorphism of the diagram (iM,if) . □

We now define induction for diagrams. Induction of modules has been defined in Example 16.4: if H is a subgroup of G and M is an $\mathcal{O}H$-module, then $\mathrm{Ind}_H^G(M) = \mathcal{O}G \otimes_{\mathcal{O}H} M$. Since the tensor product is a functor, any homomorphism $f : M \to N$ of $\mathcal{O}H$-modules gives rise to an induced homomorphism

$$\mathrm{Ind}_H^G(f) : \mathrm{Ind}_H^G(M) \longrightarrow \mathrm{Ind}_H^G(N)\,, \qquad g \otimes v \mapsto g \otimes f(v)$$

(where $g \in G$, $v \in M$). Therefore if (M,f) is an $\mathcal{O}H$-diagram of shape D , we can define the induced diagram to be

$$\mathrm{Ind}_H^G(M,f) = (\mathrm{Ind}_H^G(M), \mathrm{Ind}_H^G(f))\,,$$

where $\mathrm{Ind}_H^G(M)_d = \mathrm{Ind}_H^G(M_d)$ and $\mathrm{Ind}_H^G(f)_e = \mathrm{Ind}_H^G(f_e)$ for every vertex d and for every edge e . Thus $\mathrm{Ind}_H^G(M,f)$ is an $\mathcal{O}G$-diagram of the same shape D . As in the case of modules (Example 16.4), there is the expected connection between the induction of a diagram and the induction of the corresponding interior algebra.

(31.7) LEMMA. *Let* H *be a subgroup of* G *, let* D *be a finite oriented graph, and let* (M,f) *be an* $\mathcal{O}H$*-diagram of shape* D *. Then there is an isomorphism of interior* G*-algebras*

$$\mathrm{End}_{\mathcal{O}}(\mathrm{Ind}_H^G(M,f)) \cong \mathrm{Ind}_H^G(\mathrm{End}_{\mathcal{O}}(M,f))\,.$$

Proof. Since $\mathrm{End}_{\mathcal{O}}(M,f)$ is a subalgebra of $\prod_{d\in D} \mathrm{End}_{\mathcal{O}}(M_d)$, there is an injective algebra homomorphism

$$\mathrm{Ind}_H^G(\mathrm{End}_{\mathcal{O}}(M,f)) \longrightarrow \prod_{d\in D} \mathrm{Ind}_H^G(\mathrm{End}_{\mathcal{O}}(M_d))\,,$$

mapping $x \otimes \phi \otimes y$ to $(x \otimes \phi_d \otimes y)_{d \in D}$, where $\phi = (\phi_d)_{d \in D}$ and $x, y \in G$. Consider the isomorphism of Example 16.4

$$\omega : \prod_{d \in D} \mathrm{Ind}_H^G(\mathrm{End}_{\mathcal{O}}(M_d)) \xrightarrow{\sim} \prod_{d \in D} \mathrm{End}_{\mathcal{O}}(\mathrm{Ind}_H^G(M_d)) .$$

Recall that if $(x \otimes \phi_d \otimes y)_{d \in D}$ is mapped to $(\psi_d)_{d \in D}$ under ω , then ψ_d is given by

$$\psi_d(z \otimes v_d) = \begin{cases} x \otimes \phi_d(yz \cdot v_d) & \text{if } yz \in H, \\ 0 & \text{otherwise,} \end{cases}$$

where $z \in G$ and $v_d \in M_d$. Fix $x, y \in G$. Given a family $(x \otimes \phi_d \otimes y)_{d \in D}$, its image $(\psi_d)_{d \in D}$ lies in the subalgebra $\mathrm{End}_{\mathcal{O}}(\mathrm{Ind}_H^G(M, f))$ if and only if

$$\mathrm{Ind}_H^G(f_e)\, \psi_d = \psi_{d'}\, \mathrm{Ind}_H^G(f_e)$$

for every edge e with origin d and extremity d' . From the description of ψ_d , we see that this equation holds if and only if $f_e\, \phi_d = \phi_{d'}\, f_e$. This means that the family $(x \otimes \phi_d \otimes y)_{d \in D}$ lies in (the image of) the algebra $\mathrm{Ind}_H^G(\mathrm{End}_{\mathcal{O}}(M, f))$. Therefore we have proved that the isomorphism ω maps $\mathrm{Ind}_H^G(\mathrm{End}_{\mathcal{O}}(M, f))$ onto $\mathrm{End}_{\mathcal{O}}(\mathrm{Ind}_H^G(M, f))$. The fact that this is an isomorphism of interior G-algebras is an immediate consequence of the corresponding result for modules. □

We mention that Higman's criterion (Corollary 17.3) also holds for $\mathcal{O}G$-diagrams.

(31.8) PROPOSITION. *Let (M, f) be an $\mathcal{O}G$-diagram and let H be a subgroup of G . The following conditions are equivalent.*
(a) The G-algebra $\mathrm{End}_{\mathcal{O}}(M, f)$ is projective relative to H .
(b) (M, f) is isomorphic to a direct summand of $\mathrm{Ind}_H^G \mathrm{Res}_H^G(M, f)$.
(c) (M, f) is isomorphic to a direct summand of $\mathrm{Ind}_H^G(N, g)$ where (N, g) is some $\mathcal{O}H$-diagram.

The proof of Higman's criterion for $\mathcal{O}G$-lattices (Corollary 17.3) used in an essential way Lemma 10.7 which asserts that an $\mathcal{O}G$-lattice can be recovered from the associated interior G-algebra. Since the corresponding fact does not hold in general for $\mathcal{O}G$-diagrams, another approach is necessary. We leave the proof of Higman's criterion for diagrams as an exercise, using the direct module theoretic approach of Proposition 17.7.

The discussion of Example 13.4 for modules extends without change to diagrams. Let (M, f) be an $\mathcal{O}G$-diagram and let $A = \mathrm{End}_{\mathcal{O}}(M, f)$. If H is a subgroup of G , an idempotent i in A^H is a projection onto a direct summand of $\text{Res}_H^G(M,f)$ and i is primitive in A^H if and only if the corresponding direct summand (iM,if) is indecomposable as an $\mathcal{O}H$-diagram. Since two direct summands (iM,if) and (jM,jf) of $\text{Res}_H^G(M,f)$ are isomorphic if and only if the corresponding idempotents i and j are conjugate in A^H (Proposition 31.5), a point α of A^H corresponds to an isomorphism class of indecomposable direct summands of $\text{Res}_H^G(M,f)$. Note also that the localization A_α is the endomorphism algebra of one such direct summand because for $i \in \alpha$, we have $iAi \cong \text{End}_\mathcal{O}(iM,if)$ by Lemma 31.6. The order relation between pointed groups on $A = \text{End}_\mathcal{O}(M,f)$ is now interpreted in the same way as for modules. Let H_α and K_β be pointed groups on A, let $i \in \alpha$ and suppose that $K \leq H$. Then $K_\beta \leq H_\alpha$ if and only if there exists $j \in \beta$ such that (jM,jf) is a direct summand of $\text{Res}_K^H(iM,if)$.

With an indecomposable $\mathcal{O}G$-diagram (M,f) of shape D are associated several invariants. First a defect group P of $A = \text{End}_\mathcal{O}(M,f)$ is also called a *defect group* of (M,f) (or a *vertex* of (M,f) if there is no possible confusion with the vertices of the graph). If $\gamma \in \mathcal{P}(A^P)$ is a source point of A and if $i \in \gamma$, then the direct summand (iM,if) of $\text{Res}_P^G(M,f)$ is called a *source* of (M,f). This is well-defined up to isomorphism because another choice of $i \in \gamma$ yields an isomorphic diagram by Proposition 31.5. Thus we see that a source of a diagram is again a diagram of the same shape. As in the case of Higman's criterion, one can show that (M,f) is a direct summand of $\text{Ind}_P^G(iM,if)$. The corresponding (weaker) result for the associated interior G-algebras (namely that $\text{End}_\mathcal{O}(M,f)$ embeds in $\text{Ind}_P^G(\text{End}_\mathcal{O}(iM,if))$) is an immediate consequence of Theorem 17.9. The last invariant associated with (M,f) is the defect multiplicity module of A, which is an indecomposable projective module over a twisted group algebra, as usual.

(31.9) EXAMPLE. We have seen in Example 31.4 that short exact sequences are special cases of diagrams. For later use, we mention that the constructions above applied to a short exact sequence yield again short exact sequences. This is obvious for direct sums and clear for induction since the induction functor is exact (because $\mathcal{O}G$ is a free right $\mathcal{O}H$-module and tensoring with a free module preserves exactness). The fact that a direct summand of a short exact sequence is again a short exact sequence is left as an exercise. Consequently a source of an indecomposable short exact sequence is again a short exact sequence.

With any $\mathcal{O}G$-diagram is associated an interior G-algebra and it may seem that this provides only special examples of interior algebras. But our next result shows that in fact any interior G-algebra arises in this way.

(31.10) PROPOSITION. *Let A be an interior G-algebra. Then there exists an $\mathcal{O}G$-diagram (M,f) such that $A \cong \mathrm{End}_{\mathcal{O}}(M,f)$ as interior G-algebras.*

Proof. Let $\{a_e \mid e \in E\}$ be a finite set of generators of A as an $\mathcal{O}$-algebra (which exists by our finiteness assumption on $\mathcal{O}$-algebras). Let D be the graph with a single vertex d and the above set E as its set of edges (that is, loops). Let (M,f) be the $\mathcal{O}G$-diagram of shape D with $M_d = A$ and $f_e = r(a_e)$ for every $e \in E$, where $r(a_e)$ denotes the right multiplication by a_e. Since A is interior, A is endowed with an $\mathcal{O}G$-module structure via left multiplication. Since left and right multiplications commute, each $r(a_e)$ is an $\mathcal{O}G$-linear endomorphism of A. Thus (M,f) is indeed an $\mathcal{O}G$-diagram.

Consider the homomorphism of $\mathcal{O}$-algebras

$$\ell : A \longrightarrow \mathrm{End}_{\mathcal{O}}(M,f)\,, \qquad a \mapsto \ell(a)\,,$$

where $\ell(a)$ denotes the left multiplication by a (which is indeed an endomorphism of the diagram since left and right multiplications commute). It is clear that ℓ is injective and is a homomorphism of interior G-algebras. To prove that ℓ is surjective, we let $\phi \in \mathrm{End}_{\mathcal{O}}(M,f)$. Thus $\phi : A \to A$ is $\mathcal{O}$-linear and commutes with $r(a_e)$ for every $e \in E$. Since the elements a_e are generators, ϕ commutes with $r(a)$ for every $a \in A$. This proves the surjectivity since an endomorphism of A commuting with all right multiplications is necessarily a left multiplication $\ell(b)$ for some $b \in A$ (because if $\phi(1_A) = b$, then $\phi(a) = \phi(1_A{\cdot}a) = \phi(1_A)a = ba = \ell(b)(a)$). This completes the proof that ℓ is an isomorphism of interior G-algebras. □

Of course many different $\mathcal{O}G$-diagrams correspond to the same interior G-algebra (Exercise 31.1). The proof above just produces one with a single vertex, but this special procedure itself is not unique.

(31.11) REMARK. If $\mathcal{O}_\sharp\widehat{G}$ is a twisted group algebra, one can define in the same way the notion of $\mathcal{O}_\sharp\widehat{G}$-diagram (M,f). Then, as in the case of modules, $A = \mathrm{End}_{\mathcal{O}}(M,f)$ is a G-algebra, but not necessarily an interior G-algebra. For every subgroup H, there is again a correspondence between $\mathcal{O}_\sharp\widehat{H}$-direct summands of (M,f) and idempotents of $A^H = \mathrm{End}_{\mathcal{O}_\sharp\widehat{H}}(M,f)$. In particular (M,f) is indecomposable if and only if the G-algebra A is primitive, and in that case the notions of defect group and source diagram make sense.

Exercises

(31.1) Construct an example of two non-isomorphic $\mathcal{O}G$-diagrams whose corresponding interior G-algebras are isomorphic. [Hint: Take a graph with a single vertex and a single edge (a loop). Represent the edge first by the zero map, then by the identity map. Alternatively choose a graph with at least two vertices and apply the method of Proposition 31.10.]

(31.2) Provide the details of the proof of Lemma 31.6.

(31.3) Prove Proposition 31.8 (namely Higman's criterion for the case of $\mathcal{O}G$-diagrams). [Hint: Use the module theoretic approach of Proposition 17.7.]

(31.4) Let (M, f) be an $\mathcal{O}G$-diagram. Assume that $\mathrm{Res}_1^G(M, f)$ is a direct sum of $\mathcal{O}$-diagrams $(M, f) = (N_1, f_1) \oplus \ldots \oplus (N_n, f_n)$ and that G permutes the diagrams (N_i, f_i) transitively. Prove that (N_1, f_1) is an $\mathcal{O}H$-diagram and that $(M, f) \cong \mathrm{Ind}_H^G(N_1, f_1)$, where H is the stabilizer of (N_1, f_1).

(31.5) Let (M, f) be an $\mathcal{O}G$-diagram of shape D and let $d \in D$. Prove that if (M, f) is projective relative to a subgroup H, then the $\mathcal{O}G$-module M_d is projective relative to H. Deduce in particular that if (M, f) is an indecomposable $\mathcal{O}G$-diagram and if M_d is an indecomposable $\mathcal{O}G$-module, then a vertex of (M, f) contains a vertex of M_d.

(31.6) Prove that a direct summand of a short exact sequence is again a short exact sequence.

Notes on Section 31

The idea of representing a graph by linear maps is widely used in representation theory. There is however no clear reference for the specific case of $\mathcal{O}G$-diagrams. The interior G-algebra associated with a diagram is used by Garotta [1994] and Puig [1988c] (when the diagram is an almost split sequence), and by Linckelmann [1989, 1992] (when the diagram consists of all projective modules of a block, with suitable maps). Linckelmann was also the first to observe that any interior G-algebra arises from some $\mathcal{O}G$-diagram.

§ 32 AUSLANDER–REITEN DUALITY OVER A FIELD

In this section and the next, we discuss the Auslander–Reiten duality for modules in the special case of modules over group algebras. Given an $\mathcal{O}G$-lattice M, and for every subgroup H of G, we prove the existence of a non-degenerate bilinear form involving stable quotients of some suitable modules of H-homomorphisms. We only discuss this in two cases: the case where $\mathcal{O} = k$ is a field is treated in this section, while the case where $\mathcal{O}$ is a complete discrete valuation ring of characteristic zero will be considered in the next section. These two cases have different behaviours and require seperate treatment. The duality will then be used in Section 34 to construct almost split sequences.

We start with some generalities which are needed in both sections. Recall that if M and N are two $\mathcal{O}G$-lattices, then $\mathrm{Hom}_{\mathcal{O}}(M,N)$ is an $\mathcal{O}G$-lattice (Example 10.6). The action of $g \in G$ on a homomorphism $a \in \mathrm{Hom}_{\mathcal{O}}(M,N)$ is written ${}^g a$ and is defined by ${}^g a(m) = g{\cdot}a(g^{-1}{\cdot}m)$ for every $m \in M$. The submodule of H-fixed elements in $\mathrm{Hom}_{\mathcal{O}}(M,N)$ satisfies $\mathrm{Hom}_{\mathcal{O}}(M,N)^H = \mathrm{Hom}_{\mathcal{O}H}(M,N)$ for every subgroup H of G. The relative trace map t_H^G is defined, as in the case of G-algebras, to be the $\mathcal{O}$-linear map

$$t_H^G : \mathrm{Hom}_{\mathcal{O}H}(M,N) \longrightarrow \mathrm{Hom}_{\mathcal{O}G}(M,N)\,, \qquad t_H^G(a) = \sum_{g\in[G/H]} {}^g a\,.$$

The image of t_H^G is written $\mathrm{Hom}_{\mathcal{O}}(M,N)_H^G$. The analogue of Property 11.1 also holds, with the same elementary proof. Explicitly, if X and Y are $\mathcal{O}G$-lattices and if $a \in \mathrm{Hom}_{\mathcal{O}H}(M,N)$, $b \in \mathrm{Hom}_{\mathcal{O}G}(N,Y)$, and $c \in \mathrm{Hom}_{\mathcal{O}G}(X,M)$, then

$$t_H^G(ac) = t_H^G(a)c \quad \text{and} \quad t_H^G(ba) = b\,t_H^G(a)\,. \tag{32.1}$$

Now we take $H = 1$. Any element of $\mathrm{Hom}_{\mathcal{O}}(M,N)_1^G$ is called a *projective homomorphism* from M to N and the quotient $\mathcal{O}$-module

$$\overline{\mathrm{Hom}}_{\mathcal{O}G}(M,N) = \mathrm{Hom}_{\mathcal{O}G}(M,N)\big/\,\mathrm{Hom}_{\mathcal{O}}(M,N)_1^G$$

is called the *stable quotient* of $\mathrm{Hom}_{\mathcal{O}G}(M,N)$. In representation theory, the word “stable” often refers to the concepts obtained by working modulo projective objects. The word “projective” is justified here by the following lemma. The lemma can be generalized to a relative situation (Exercise 32.1).

(32.2) LEMMA. *Let* $f \in \mathrm{Hom}_{\mathcal{O}G}(M,N)$ *where* M *and* N *are two* $\mathcal{O}G$*-lattices. Then* f *is a projective homomorphism if and only if* f *factorizes through a projective* $\mathcal{O}G$*-lattice* P *. Moreover, in that case,* P *can be chosen to be any projective cap of* N *(for instance the projective cover of* N *).*

Proof. If f factorizes through a projective $\mathcal{O}G$-lattice P, we have $f = ab$ with $a \in \mathrm{Hom}_{\mathcal{O}G}(P,N)$ and $b \in \mathrm{Hom}_{\mathcal{O}G}(M,P)$. Since P is projective, $id_P = t_1^G(c)$ for some $c \in \mathrm{End}_{\mathcal{O}}(P)$ (Corollary 17.4). Therefore by 32.1, we obtain

$$f = a\, id_P\, b = a\, t_1^G(c)\, b = t_1^G(acb)\,,$$

so that f is projective.

Suppose conversely that $f = t_1^G(h)$ for some $h \in \mathrm{Hom}_{\mathcal{O}}(M,N)$. Let $a : P \to N$ be any $\mathcal{O}G$-linear surjection, where P is a projective $\mathcal{O}G$-lattice. Since N is an $\mathcal{O}$-lattice, the surjection splits over $\mathcal{O}$ and we let $s : N \to P$ be an $\mathcal{O}$-linear map such that $as = id_N$. Then $b = t_1^G(sh) : M \to P$ is $\mathcal{O}G$-linear and we have

$$ab = a\, t_1^G(sh) = t_1^G(ash) = t_1^G(h) = f\,.$$

Thus f factorizes through P. This proves both the converse and the additional statement. □

It is an immediate consequence of 32.1 that the composition of homomorphisms induces a well-defined map

$$\overline{\mathrm{Hom}}_{\mathcal{O}G}(M,N) \times \overline{\mathrm{Hom}}_{\mathcal{O}G}(L,M) \longrightarrow \overline{\mathrm{Hom}}_{\mathcal{O}G}(L,N)\,.$$

A surjection $P \to N$ with P projective, as in the above lemma, is a projective cap of N, and its kernel will usually be written TN . If $P \to N$ is a projective cover, then $TN = \Omega N$ (where Ω is the Heller operator), but in general $TN = \Omega N \oplus Q$ for some projective $\mathcal{O}G$-lattice Q (Proposition 5.4). We shall need projective caps which are not necessarily projective covers, and therefore we shall have to add projective modules to modules like ΩN . But we immediately note that stable quotients are not modified by addition of projective modules.

(32.3) LEMMA. *Let M, N, and P be $\mathcal{O}G$-lattices, with P projective.*

(a) *The injection $i : N \to N \oplus P$ and the projection $q : N \oplus P \to N$ induce inverse isomorphisms*

$$i_* : \overline{\mathrm{Hom}}_{\mathcal{O}G}(M, N) \xrightarrow{\sim} \overline{\mathrm{Hom}}_{\mathcal{O}G}(M, N \oplus P) \quad \text{and}$$
$$q_* : \overline{\mathrm{Hom}}_{\mathcal{O}G}(M, N \oplus P) \xrightarrow{\sim} \overline{\mathrm{Hom}}_{\mathcal{O}G}(M, N) .$$

(b) *The injection $j : M \to M \oplus P$ and the projection $r : M \oplus P \to M$ induce inverse isomorphisms*

$$j^* : \overline{\mathrm{Hom}}_{\mathcal{O}G}(M \oplus P, N) \xrightarrow{\sim} \overline{\mathrm{Hom}}_{\mathcal{O}G}(M, N) \quad \text{and}$$
$$r^* : \overline{\mathrm{Hom}}_{\mathcal{O}G}(M, N) \xrightarrow{\sim} \overline{\mathrm{Hom}}_{\mathcal{O}G}(M \oplus P, N) .$$

Proof. (a) Since $qi = id_N$, the map $q_* i_*$ is the identity. Now $id_{N\oplus P} - iq = q'$ is an idempotent endomorphism of $N \oplus P$ with image P, and therefore q' factorizes through P. Thus q' is a projective homomorphism (Lemma 32.2). Therefore $f - iqf = q'f$ is a projective homomorphism for every $f \in \mathrm{Hom}_{\mathcal{O}G}(M, N \oplus P)$. This means that, in the stable quotients, the map $id - i_* q_*$ is zero. This completes the proof that i_* and q_* are inverse isomorphisms.

(b) The proof is similar. □

We now prove that the inclusion map and relative trace map between modules of fixed elements induce maps between corresponding stable quotients. This implies that the family of stable quotients $\overline{\mathrm{Hom}}_{\mathcal{O}H}(M, N)$ has a Mackey functor structure, in the sense of Chapter 8.

(32.4) LEMMA. *Let M and N be two $\mathcal{O}G$-lattices and let $F \leq H \leq G$. The inclusion map $r^H_F : \mathrm{Hom}_{\mathcal{O}H}(M, N) \to \mathrm{Hom}_{\mathcal{O}F}(M, N)$ and the relative trace map $t^H_F : \mathrm{Hom}_{\mathcal{O}F}(M, N) \to \mathrm{Hom}_{\mathcal{O}H}(M, N)$ induce $\mathcal{O}$-linear maps*

$$\bar{r}^H_F : \overline{\mathrm{Hom}}_{\mathcal{O}H}(M, N) \longrightarrow \overline{\mathrm{Hom}}_{\mathcal{O}F}(M, N) \qquad \text{and}$$
$$\bar{t}^H_F : \overline{\mathrm{Hom}}_{\mathcal{O}F}(M, N) \longrightarrow \overline{\mathrm{Hom}}_{\mathcal{O}H}(M, N)$$

satisfying the properties (a), (b), (c), (d), and (g) of Proposition 11.4.

Proof. It is obvious that t^H_F maps $\mathrm{Hom}_{\mathcal{O}}(M, N)^F_1$ to $\mathrm{Hom}_{\mathcal{O}}(M, N)^H_1$, and therefore induces a map $\bar{t}^H_F$ between stable quotients. Similarly r^H_F induces a map $\bar{r}^H_F$ between stable quotients if we show that it maps $\mathrm{Hom}_{\mathcal{O}}(M, N)^H_1$ to $\mathrm{Hom}_{\mathcal{O}}(M, N)^F_1$. But this is a trivial special case of the Mackey decomposition formula 11.3: $r^H_F\, t^H_1(a) = \sum_{h\in[F\backslash H]} t^F_1({}^h a)$. The verification of the properties of Proposition 11.4 is easy and is left to the reader. □

The ordinary trace map is the main tool for the Auslander–Reiten duality and we now recall some of its basic properties. The *trace* $\mathrm{tr}(a)$ of a square matrix a is the sum of all diagonal entries of a. If b is an $(n\times m)$-matrix and if c is an $(m\times n)$-matrix, then bc is an $(n\times n)$-matrix, while cb is an $(m\times m)$-matrix. It is elementary to check that we have $\mathrm{tr}(bc)=\mathrm{tr}(cb)$, and we shall use this fact repeatedly without further notice. In particular if a and b are square matrices and if b is invertible, then we have $\mathrm{tr}(bab^{-1})=\mathrm{tr}(a)$.

Let M be an $\mathcal{O}$-lattice (that is, a finitely generated free $\mathcal{O}$-module). The *trace map* is the $\mathcal{O}$-linear map $\mathrm{tr}:\mathrm{End}_{\mathcal{O}}(M)\to\mathcal{O}$ defined as follows. Given $f\in\mathrm{End}_{\mathcal{O}}(M)$, choose a basis of M, consider the matrix a of f with respect to this basis, and define $\mathrm{tr}(f)=\mathrm{tr}(a)$. Since the matrix of f with respect to some other basis has the form bab^{-1} for some invertible b, the definition of $\mathrm{tr}(f)$ does not depend on the choice of basis. Now if M and N are two $\mathcal{O}$-lattices, the *trace form* is the $\mathcal{O}$-bilinear map

$$\mathrm{tr}:\mathrm{Hom}_{\mathcal{O}}(M,N)\times\mathrm{Hom}_{\mathcal{O}}(N,M)\longrightarrow\mathcal{O}$$

defined by $\mathrm{tr}(a,b)=\mathrm{tr}(ab)=\mathrm{tr}(ba)$. This makes sense since we have $ba\in\mathrm{End}_{\mathcal{O}}(M)$ and $ab\in\mathrm{End}_{\mathcal{O}}(N)$.

Recall that if X and Y are two $\mathcal{O}$-lattices, then a bilinear form $X\times Y\to\mathcal{O}$ is called non-degenerate (respectively unimodular) if both corresponding linear map $X\to Y^*$ and $Y\to X^*$ are injective (respectively bijective). The two notions coincide over a field, but not over a discrete valuation ring.

(32.5) LEMMA. *Let M and N be two $\mathcal{O}$-lattices.*

(a) *The trace form*

$$\mathrm{tr}:\mathrm{Hom}_{\mathcal{O}}(M,N)\times\mathrm{Hom}_{\mathcal{O}}(N,M)\longrightarrow\mathcal{O}$$

is a unimodular symmetric $\mathcal{O}$-bilinear form. Moreover it is associative, in the sense that $\mathrm{tr}(a,bc)=\mathrm{tr}(ab,c)$ for every $a\in\mathrm{Hom}_{\mathcal{O}}(L,M)$, $b\in\mathrm{Hom}_{\mathcal{O}}(N,L)$, and $c\in\mathrm{Hom}_{\mathcal{O}}(M,N)$, where L is an $\mathcal{O}$-lattice.

(b) *If M and N are $\mathcal{O}G$-lattices, then the trace form is G-invariant, that is, $\mathrm{tr}({}^g a, {}^g b)=\mathrm{tr}(a,b)$ for all $g\in G$, $a\in\mathrm{Hom}_{\mathcal{O}}(N,M)$ and $b\in\mathrm{Hom}_{\mathcal{O}}(M,N)$.*

Proof. (a) We have already noticed that tr is symmetric. To check that it is unimodular, we choose bases of M and N and this allows us to identify $\mathrm{Hom}_{\mathcal{O}}(M,N)$ with $(m\times n)$-matrices, and $\mathrm{Hom}_{\mathcal{O}}(N,M)$ with $(n\times m)$-matrices. Then the canonical basis of $\mathrm{Hom}_{\mathcal{O}}(N,M)$ is the dual basis (with respect to tr) of the canonical basis of $\mathrm{Hom}_{\mathcal{O}}(M,N)$. The unimodularity property follows. The associativity of the form is a consequence of the associativity of the composition of maps.

(b) The G-invariance of tr is an easy consequence of the fact that, for $a\in\mathrm{End}_{\mathcal{O}}(M)$, we have $\mathrm{tr}({}^g a)=\mathrm{tr}(g{\cdot}a{\cdot}g^{-1})=\mathrm{tr}(a)$. □

We now start with the case of a field k of characteristic p (which need not be algebraically closed). For every subspace V of $\mathrm{Hom}_k(M,N)$, let $V^\perp$ be the *orthogonal* of V with respect to tr, that is,

$$V^\perp = \{\, a \in \mathrm{Hom}_k(N,M) \mid \mathrm{tr}(ab) = 0 \ \text{for every } b \in V \,\}.$$

Clearly $V^\perp$ is a subspace and we have $(V^\perp)^\perp = V$ by the non-degeneracy of the form (and because all k-spaces are finite dimensional). Moreover if we let $n = \dim_k \mathrm{Hom}_k(N,M) = \dim_k \mathrm{Hom}_k(M,N)$, then it is well known (and easy to check) that $\dim_k(V) + \dim_k(V^\perp) = n$. For example if $M = N$, the kernel of tr viewed as a linear form on $\mathrm{End}_k(M)$ satisfies

$$\text{(32.6)} \qquad \mathrm{Ker}(\mathrm{tr}) = (k{\cdot}id_M)^\perp .$$

Indeed it is obvious that $\mathrm{Ker}(\mathrm{tr})$ is orthogonal to any scalar, and since $\dim_k(\mathrm{Ker}(\mathrm{tr})) = n-1$ and $\dim_k(k{\cdot}id_M) = 1$, the equality follows for reasons of dimension.

Instead of a map $t_1^G : \mathrm{Hom}_k(M,N) \to \mathrm{Hom}_k(M,N)^G$, let us view the relative trace map t_1^G as an endomorphism of $\mathrm{Hom}_k(M,N)$. The next lemma is very simple, but extremely useful.

(32.7) LEMMA. *Let M and N be two kG-modules. The adjoint with respect to tr of the relative trace map $t_1^G : \mathrm{Hom}_k(M,N) \to \mathrm{Hom}_k(M,N)$ is the relative trace map $t_1^G : \mathrm{Hom}_k(N,M) \to \mathrm{Hom}_k(N,M)$.*

Proof. If $a \in \mathrm{Hom}_k(M,N)$ and $b \in \mathrm{Hom}_k(N,M)$, then we have

$$\begin{aligned}\mathrm{tr}(t_1^G(a)b) &= \mathrm{tr}\Big(\sum_{g\in G} {}^g a{\cdot}b\Big) = \sum_{g\in G} \mathrm{tr}(g{\cdot}(a\, {}^{g^{-1}}b){\cdot}g^{-1}) = \sum_{g\in G} \mathrm{tr}(a\, {}^{g^{-1}}b) \\ &= \mathrm{tr}(a\, t_1^G(b)),\end{aligned}$$

as required. □

(32.8) COROLLARY. $\mathrm{Im}(t_1^G) = \mathrm{Ker}(t_1^G)^\perp$.

Proof. This is a general property of adjoints. The proof is easy and is left to the reader. □

For the endomorphism algebra of a projective kG-module, we can use the trace form to define a non-degenerate form on G-fixed elements. For later use, we do this in the more general situation of a twisted group algebra. We first need a lemma.

(32.9) LEMMA. *Let $\widehat{G}$ be a central extension of G with kernel k^* and let $k_\sharp \widehat{G}$ be the corresponding twisted group algebra. Let P be a $k_\sharp \widehat{G}$-module and let $S = \mathrm{End}_k(P)$ be the corresponding G-algebra. Then $\mathrm{Ker}(t_1^G) \subseteq \mathrm{Ker}(\mathrm{tr})$ if and only if P is projective.*

Proof. Before starting the proof, we first note that tr is a G-invariant form on S. This is not directly a consequence of Lemma 32.5 because we are dealing with twisted group algebras. However, the action of $g \in G$ on S is equal to the inner automorphism $\mathrm{Inn}(\widehat{g})$ for some $\widehat{g} \in \widehat{G}$, and therefore $\mathrm{tr}({}^g a) = \mathrm{tr}(\widehat{g} \cdot a \cdot \widehat{g}^{-1}) = \mathrm{tr}(a)$. It follows that Lemma 32.7 and Corollary 32.8 also hold in this context.

Since the trace form on S is non-degenerate, it suffices to show that P is projective if and only if $\mathrm{Ker}(t_1^G)^\perp \supseteq \mathrm{Ker}(\mathrm{tr})^\perp$. But the right hand side is equal to $k \cdot 1_S$ by 32.6 and the left hand side is equal to $\mathrm{Im}(t_1^G) = S_1^G$ by Corollary 32.8. The inclusion $k \cdot 1_S \subseteq S_1^G$ is equivalent to the condition $1_S \in S_1^G$, that is, $S_1^G = S^G$. By Corollary 17.8, $S_1^G = S^G$ if and only if P is projective. □

(32.10) PROPOSITION. *Let $\widehat{G}$ be a central extension of G with kernel k^* and let $k_\sharp \widehat{G}$ be the corresponding twisted group algebra. Let P be a projective $k_\sharp \widehat{G}$-module and let $S = \mathrm{End}_k(P)$ be the corresponding G-algebra.*

(a) For every $a \in S^G = \mathrm{End}_{k_\sharp \widehat{G}}(P)$, let $\lambda(a) = \mathrm{tr}(a')$ where $a' \in S$ is such that $t_1^G(a') = a$. Then $\lambda : S^G \to k$ is a well-defined linear form.

(b) The k-algebra S^G is a symmetric algebra, with symmetrizing form λ.

Proof. (a) This follows immediately from Lemma 32.9.

(b) Let $(a, b) \mapsto \lambda(ab)$ be the corresponding bilinear form on S^G. To prove that it is symmetric, let $a' \in S$ be such that $t_1^G(a') = a$. Then we have $\lambda(ab) = \mathrm{tr}(a'b)$ because $t_1^G(a'b) = t_1^G(a')b = ab$ by 32.1. Similarly $\lambda(ba) = \mathrm{tr}(ba')$ and the symmetry follows from the symmetry of tr. For the non-degeneracy, suppose that $\lambda(ab) = 0$ for every $a \in S^G$. Then $\mathrm{tr}(a'b) = 0$ for every $a' \in S$ and therefore $b = 0$ since tr is non-degenerate. □

Let A be a symmetric k-algebra. Recall that, by Exercise 6.1, the socle $\mathrm{Soc}(A_\ell)$ of the left A-module A coincides with the socle $\mathrm{Soc}(A_r)$ of the right A-module A. It is a two-sided ideal, written $\mathrm{Soc}(A)$, and called simply the *socle* of A. Moreover $\mathrm{Soc}(A) = J(A)^\perp$ by Exercise 6.1. The use of both forms tr and λ above yields the following result.

(32.11) COROLLARY. *Let* $\widehat{G}$ *be a central extension of* G *with kernel* k^* *and let* $k_\sharp\widehat{G}$ *be the corresponding twisted group algebra. Let* P *be a projective* $k_\sharp\widehat{G}$*-module and let* $S = \mathrm{End}_k(P)$ *be the corresponding* G*-algebra, endowed with the trace form. Then* $\mathrm{Soc}(S^G)^\perp = (t_1^G)^{-1}(J(S^G))$.

Proof. Let V be the orthogonal of $(t_1^G)^{-1}(J(S^G))$ (with respect to tr). Since we obviously have $\mathrm{Ker}(t_1^G) \subseteq (t_1^G)^{-1}(J(S^G))$, we deduce that $V \subseteq S_1^G = S^G$ by Corollary 32.8. It follows from this and the definition of the form λ on S^G (Proposition 32.10) that V is also the orthogonal of $J(S^G)$ with respect to the form λ. But since S^G is a symmetric algebra, the orthogonal of $J(S^G)$ is equal to $\mathrm{Soc}(S^G)$ (Exercise 6.1). □

Now we can define the form which will induce the Auslander–Reiten duality. We fix a kG-module M and we choose a projective cap $q : P \to M$ of M. Let $TM = \mathrm{Ker}(q)$ and let $j : TM \to P$ be the inclusion, so that there is a short exact sequence

$$0 \longrightarrow TM \xrightarrow{\ j\ } P \xrightarrow{\ q\ } M \longrightarrow 0\,.$$

If $q : P \to M$ is a projective cover of M, then $TM = \Omega M$, the Heller translate of M. In general, we have $TM = \Omega M \oplus Q$ for some projective kG-module Q (Proposition 5.4). On restriction to any subgroup H of G, this short exact sequence is a projective cap of $\mathrm{Res}_H^G(M)$. Indeed $\mathrm{Res}_H^G(P)$ is a projective kH-module, since the restriction of a free kG-module is a free kH-module. If we had started with a projective cover of M, then, on restriction to H, we would only have obtained a projective cap of $\mathrm{Res}_H^G(M)$, and this is one reason for using arbitrary projective caps.

Since $\mathrm{Res}_H^G(P)$ is projective, there is by Proposition 32.10 a linear form $\lambda^H : \mathrm{End}_{kH}(P) \to k$ defined by $\lambda^H(f) = \mathrm{tr}(f')$ where $f = t_1^H(f')$. For every kG-module L, we define a bilinear form

$$\widetilde{\phi}^H_{M,L} : \mathrm{Hom}_{kH}(L, TM) \times \mathrm{Hom}_{kH}(M, L) \longrightarrow k\,, \qquad \widetilde{\phi}^H_{M,L}(a,b) = \lambda^H(jabq)\,,$$

where j and q are the maps appearing in the above exact sequence.

(32.12) THEOREM (Auslander–Reiten duality). *Let* $q : P \to M$ *be a projective cap of a* kG*-module* M *and let* $TM = \mathrm{Ker}(q)$.

(a) *For every* kG*-module* L *and for every subgroup* H *of* G, *the bilinear form* $\widetilde{\phi}^H_{M,L}$ *defined above induces a non-degenerate bilinear form*

$$\phi^H_{M,L} : \overline{\mathrm{Hom}}_{kH}(L, TM) \times \overline{\mathrm{Hom}}_{kH}(M, L) \longrightarrow k$$

satisfying the following properties.

(b) If $F \leq H \leq G$, the restriction map $\overline{r}_F^H$ is the left and right adjoint of the relative trace map $\overline{t}_F^H$ (with respect to the forms $\phi_{M,L}^H$ and $\phi_{M,L}^F$).

(c) Let $\overline{f} \in \overline{\mathrm{Hom}}_{kH}(L,N)$. Then the forms $\phi_{M,L}^H$ and $\phi_{M,N}^H$ satisfy the relation

$$\phi_{M,L}^H(\overline{a}\overline{f},\overline{b}) = \phi_{M,N}^H(\overline{a},\overline{fb})$$

for all $\overline{a} \in \overline{\mathrm{Hom}}_{kH}(N,TM)$ and $\overline{b} \in \overline{\mathrm{Hom}}_{kH}(M,L)$.

Proof. (a) In order to compute the value of λ^H on some composite $a_1a_2\ldots a_r$, we note that it suffices to be able to write $a_i = t_1^H(a_i')$ for some i. Indeed by 32.1 we have

$$\begin{aligned} a_1\ldots a_r &= t_1^H(a_1\ldots a_{i-1}a_i'a_{i+1}\ldots a_r) \qquad \text{and} \\ \lambda^H(a_1\ldots a_r) &= \mathrm{tr}(a_1\ldots a_{i-1}a_i'a_{i+1}\ldots a_r). \end{aligned}$$

We shall use this observation repeatedly.

Let $\mathrm{Ker}_\ell(\widetilde{\phi}_{M,L}^H)$ and $\mathrm{Ker}_r(\widetilde{\phi}_{M,L}^H)$ be respectively the left and right kernels of the form $\widetilde{\phi}_{M,L}^H$. We claim that $\mathrm{Ker}_\ell(\widetilde{\phi}_{M,L}^H) = \mathrm{Hom}_k(L,TM)_1^H$. If $a \in \mathrm{Hom}_k(L,TM)_1^H$, then $a = t_1^H(a')$ for some a' and therefore, for every $b \in \mathrm{Hom}_{kH}(M,L)$, we have

$$\widetilde{\phi}_{M,L}^H(a,b) = \lambda^H(jabq) = \mathrm{tr}(ja'bq) = \mathrm{tr}(a'bqj) = 0$$

because $qj = 0$. Assuming conversely that $a \in \mathrm{Ker}_\ell(\widetilde{\phi}_{M,L}^H)$, we want to prove that $a \in \mathrm{Hom}_k(L,TM)_1^H$. By Corollary 32.8, this is equivalent to showing that $a \in \mathrm{Ker}(t_1^H)^\perp$, with respect to the trace form tr. Thus if $f : TM \to L$ satisfies $t_1^H(f) = 0$, we have to prove that $\mathrm{tr}(af) = 0$. The reader is advised to draw a diagram with all the maps involved in the following proof. Let $r : P \to TM$ be a k-linear retraction of j, which exists because j is injective. Then we have

$$t_1^H(fr)j = t_1^H(frj) = t_1^H(f) = 0.$$

Since TM is the kernel of q and $j : TM \to P$ is the inclusion map, the map $t_1^H(fr)$ factorizes through q. Thus there exists $b \in \mathrm{Hom}_{kH}(M,L)$ such that $t_1^H(fr) = bq$. Since j maps to the projective module P, there exists $j' : TM \to P$ such that $t_1^H(j') = j$ (Lemma 32.2). Now, using the fact that t_1^H is the adjoint of t_1^H with respect to tr (Lemma 32.7), we have

$$\begin{aligned} \mathrm{tr}(af) &= \mathrm{tr}(afrj) = \mathrm{tr}(jafr) = \mathrm{tr}(t_1^H(j'a)fr) = \mathrm{tr}(j'a\,t_1^H(fr)) \\ &= \mathrm{tr}(j'abq) = \lambda^H(jabq) = \widetilde{\phi}_{M,L}^H(a,b) = 0, \end{aligned}$$

because $a \in \mathrm{Ker}_\ell(\widetilde{\phi}^H_{M,L})$ by assumption. This completes the proof that $\mathrm{Ker}_\ell(\widetilde{\phi}^H_{M,L}) = \mathrm{Hom}_k(L, TM)^H_1$.

The proof that $\mathrm{Ker}_r(\widetilde{\phi}^H_{M,L}) = \mathrm{Hom}_k(M, L)^H_1$ is very similar. If we let $b \in \mathrm{Hom}_k(M, L)^H_1$, then $b = t^H_1(b')$ for some b' and therefore, for every $a \in \mathrm{Hom}_{kH}(L, TM)$, we have

$$\widetilde{\phi}^H_{M,L}(a, b) = \lambda^H(jabq) = \mathrm{tr}(jab'q) = \mathrm{tr}(ab'qj) = 0$$

because $qj = 0$. Assuming conversely that $b \in \mathrm{Ker}_r(\widetilde{\phi}^H_{M,L})$, we want to prove that $b \in \mathrm{Hom}_k(M, L)^H_1 = \mathrm{Ker}(t^H_1)^\perp$. Thus if $g : L \to M$ satisfies $t^H_1(g) = 0$, we have to prove that $\mathrm{tr}(gb) = 0$. Let $s : M \to P$ be a k-linear section of q , which exists because q is surjective. Then we have

$$q\, t^H_1(sg) = t^H_1(qsg) = t^H_1(g) = 0 .$$

Since TM is the kernel of q and $j : TM \to P$ is the inclusion map, the map $t^H_1(sg)$ factorizes through j . Thus there exists $a \in \mathrm{Hom}_{kH}(L, TM)$ such that $t^H_1(sg) = ja$. Since q maps from the projective module P , there exists $q' : P \to M$ such that $t^H_1(q') = q$. Then we have

$$\begin{aligned}\mathrm{tr}(gb) &= \mathrm{tr}(qsgb) = \mathrm{tr}(sgbq) = \mathrm{tr}(sg\, t^H_1(bq')) = \mathrm{tr}(t^H_1(sg)bq') \\ &= \mathrm{tr}(jabq') = \lambda^H(jabq) = \widetilde{\phi}^H_{M,L}(a, b) = 0 ,\end{aligned}$$

because $b \in \mathrm{Ker}_r(\widetilde{\phi}^H_{M,L})$ by assumption. This completes the proof that $\mathrm{Ker}_r(\widetilde{\phi}^H_{M,L}) = \mathrm{Hom}_k(M, L)^H_1$.

Since both the left and right kernels of $\widetilde{\phi}^H_{M,L}$ are the submodules of projective homomorphisms, we can pass to the quotient by projective homomorphisms and obtain a non-degenerate bilinear form

$$\phi^H_{M,L} : \overline{\mathrm{Hom}}_{kH}(L, TM) \times \overline{\mathrm{Hom}}_{kH}(M, L) \longrightarrow k ,$$

as was to be shown.

(b) First note that if $c \in \mathrm{End}_{kF}(P)$, then $\lambda^F(c) = \lambda^H(t^H_F(c))$, because if $c = t^F_1(c')$ then

$$\lambda^H(t^H_F(c)) = \lambda^H(t^H_F\, t^F_1(c')) = \lambda^H(t^H_1(c')) = \mathrm{tr}(c') = \lambda^F(c) .$$

Now let $a \in \mathrm{Hom}_{kH}(L, TM)$ and $b \in \mathrm{Hom}_{kF}(M, L)$. Then we have

$$\begin{aligned}\widetilde{\phi}^H_{M,L}(a, t^H_F(b)) &= \lambda^H(ja\, t^H_F(b)q) = \lambda^H(t^H_F(jabq)) = \lambda^F(jabq) \\ &= \widetilde{\phi}^F_{M,L}(a, b) = \widetilde{\phi}^F_{M,L}(r^H_F(a), b) .\end{aligned}$$

Therefore $\phi^H_{M,L}(\overline{a}, \overline{t}^H_F(\overline{b})) = \phi^F_{M,L}(\overline{r}^H_F(\overline{a}), \overline{b})$. The other adjointness property is proved similarly.

(c) If $f \in \mathrm{Hom}_{kH}(L, N)$, $a \in \mathrm{Hom}_{kH}(N, TM)$, $b \in \mathrm{Hom}_{kH}(M, L)$, we have

$$\widetilde{\phi}^H_{M,L}(af, b) = \lambda^H(j(af)bq) = \lambda^H(ja(fb)q) = \widetilde{\phi}^H_{M,N}(a, fb) ,$$

and the result follows by taking images in stable quotients. □

Exercises

(32.1) Let $f : L \to M$ be a homomorphism of $\mathcal{O}G$-modules and let H be a subgroup of G. Prove that $f \in \mathrm{Hom}_{\mathcal{O}}(L,M)_H^G$ if and only if f factorizes through some $\mathcal{O}G$-module P which is projective relative to H. [Hint: Show that there always exist an $\mathcal{O}G$-module P which is projective relative to H and a surjective homomorphism of $\mathcal{O}G$-modules $P \to M$ which splits on restriction to H. For instance take $P = \mathrm{Ind}_H^G \mathrm{Res}_H^G(M)$.]

(32.2) Prove the properties stated in Lemma 32.4.

(32.3) State and prove a result asserting that the Auslander–Reiten duality for the kG-module M does not depend on the choice of a projective cap of M. [Hint: Use Lemma 32.3.]

(32.4) Let $q : P \to M$ be a projective cap of a kG-module M, let $TM = \mathrm{Ker}(q)$, and let H be a subgroup of G.

(a) Prove that any $f \in \mathrm{End}_{kH}(M)$ lifts to a kH-endomorphism $\widetilde{f}$ of P, which induces in turn a kH-endomorphism f' of TM.

(b) Given $\overline{f} \in \overline{\mathrm{End}}_{kH}(M)$, choose $f \in \mathrm{End}_{kH}(M)$ in the inverse image of $\overline{f}$ and let $f' \in \mathrm{End}_{kH}(TM)$ be constructed as in (a). Prove that $\overline{f}'$ only depends on $\overline{f}$ (not on the choices of f and $\widetilde{f}$).

(c) Prove that the map

$$\overline{\mathrm{End}}_{kH}(M) \longrightarrow \overline{\mathrm{End}}_{kH}(TM), \qquad \overline{f} \mapsto \overline{f}'$$

defined in (b) is an isomorphism of k-algebras. [Hint: Construct an inverse using the fact that P is also an injective kH-module, by Proposition 6.7 and the fact that kH is a symmetric algebra.]

(d) Let L be a kG-module and let $\phi_{M,L}^H$ be the form defined in Theorem 32.12. Prove that if $\overline{f}'$ is the image of $\overline{f}$ under the map defined in (c), then $\phi_{M,L}^H(\overline{a}, \overline{bf}) = \phi_{M,L}^H(\overline{f}'\overline{a}, \overline{b})$ for all $\overline{a} \in \overline{\mathrm{Hom}}_{kH}(L,TM)$ and $\overline{b} \in \overline{\mathrm{Hom}}_{kH}(M,L)$.

Notes on Section 32

The Auslander–Reiten duality was proved in Auslander–Reiten [1975] for modules over any finite dimensional algebra over a field (and more generally over any Artin algebra), but the general statement is not a straightforward extension of Theorem 32.12. The proof given here for group algebras is taken from Knörr [1985].

§ 33 AUSLANDER–REITEN DUALITY OVER A DISCRETE VALUATION RING

We continue the program started in the previous section and turn to the case of a ring $\mathcal{O}$ satisfying the following assumption.

(33.1) ASSUMPTION. As a base ring, we take a complete discrete valuation ring $\mathcal{O}$ with maximal ideal $\mathfrak{p}$ generated by π. We assume that the field of fractions K of $\mathcal{O}$ has characteristic zero, and that the residue field $k = \mathcal{O}/\mathfrak{p}$ has non-zero characteristic p.

We do not need in this section our usual assumption that k is algebraically closed, but if this is the case, then of course Assumption 2.1 holds. A basic tool in the proof of the Auslander–Reiten duality over a field was the use of orthogonal subspaces, but this does not work over $\mathcal{O}$ (Exercise 6.1). It is the concept of dual lattice which plays a crucial role here and we first review this notion.

If M is an $\mathcal{O}$-lattice, consider the K-vector space $KM = K \otimes_{\mathcal{O}} M$. We identify M with the $\mathcal{O}$-submodule $1 \otimes M$ of KM, so that any $\mathcal{O}$-basis of M is a K-basis of KM. Any element x of KM can be written $x = am$ for some $m \in M$ and $a \in K$, by taking $a = 1/d$ where $d \in \mathcal{O}$ is a common denominator for the coefficients of x with respect to some basis of M. Conversely if V is a K-vector space, then there are many $\mathcal{O}$-lattices M such that $KM = V$, because for any basis of V, one can take for M the set of all linear combinations of this basis with coefficients in $\mathcal{O}$. Any $\mathcal{O}$-lattice M such that $KM = V$ is called an *$\mathcal{O}$-lattice* in V. For instance aM is again an $\mathcal{O}$-lattice in V, for every $a \in K$.

For completeness we also mention the following facts. If M and M' are two $\mathcal{O}$-lattices in V such that $M \subseteq M'$, then any $\mathcal{O}$-submodule L such that $M \subseteq L \subseteq M'$ is again an $\mathcal{O}$-lattice in V, because L is torsion free, hence free by Proposition 1.5. If M and L are two lattices in V, then there exists $d \in \mathcal{O}$ such that $dL \subseteq M$. Since $dL \subseteq (L \cap M) \subseteq M$ and $L \subseteq (L + M) \subseteq (1/d)M$, we deduce that the sum and intersection of two $\mathcal{O}$-lattices in V is again an $\mathcal{O}$-lattice in V. The reader can easily provide proofs of these assertions.

Suppose now that $\psi : M \times M \to \mathcal{O}$ is a non-degenerate symmetric bilinear form on an $\mathcal{O}$-lattice M. The non-degeneracy assumption means that whenever $\psi(x, y) = 0$ for every $y \in M$, then $x = 0$. In other words the associated map $M \to M^*$ into the dual module is injective; but it is not necessarily surjective (that is, M is not necessarily unimodular). The form ψ induces a non-degenerate symmetric bilinear form on the K-vector space KM, still written ψ. Explicitly, if $m, m' \in M$ and $a, a' \in K$, then $\psi(am, a'm') = aa'\psi(m, m')$. It is elementary to check that this is well-defined and non-degenerate over K . Since K is a field, the form ψ induces this time an isomorphism $KM \cong (KM)^* = KM^*$ (that is, we have unimodularity over K). This implies in particular that any basis of KM has a dual basis with respect to ψ . If conversely a K-vector space V is endowed with a non-degenerate symmetric bilinear form ψ , then, for any $\mathcal{O}$-lattice M such that $KM = V$, the restriction of ψ to M has values in $(1/d)\mathcal{O}$ for some $d \in \mathcal{O}$. In particular ψ has values in $\mathcal{O}$ on the lattice dM .

Let V be a K-vector space endowed with a non-degenerate symmetric bilinear form ψ , and let M be an $\mathcal{O}$-lattice in V . The *dual lattice* M^* of M is the $\mathcal{O}$-lattice

$$M^* = \{ x \in V \mid \psi(x,m) \in \mathcal{O} \quad \text{for all } m \in M \} .$$

To see that M^* is an $\mathcal{O}$-lattice in V , choose a basis (m_i) of M , let (m_i^*) be the dual basis of V with respect to the form ψ . Then clearly $m_i^* \in M^*$ for all i . We can write an arbitrary element $x \in M^*$ as $x = \sum_i \psi(x,m_i)m_i^*$, and we have $\psi(x,m_i) \in \mathcal{O}$ by definition of M^* . This shows that (m_i^*) is an $\mathcal{O}$-basis of M^* . This terminology is consistent with the previously defined notion of dual lattice $\mathrm{Hom}_{\mathcal{O}}(M,\mathcal{O})$, because there is a canonical isomorphism $M^* \cong \mathrm{Hom}_{\mathcal{O}}(M,\mathcal{O})$ mapping $x \in M^*$ to the linear form $\psi(x,-)$ on M (Exercise 33.1).

Unimodularity is easily interpreted in terms of dual lattices. Let M be an $\mathcal{O}$-lattice endowed with a non-degenerate symmetric bilinear form ψ (which we extend to a form ψ on KM). Then M is unimodular if and only if $M = M^*$ in KM (Exercise 33.1).

(33.2) LEMMA. *Let L and M be two $\mathcal{O}$-lattices in a K-vector space V endowed with a non-degenerate symmetric bilinear form ψ .*
(a) If $L \subseteq M$, then $M^* \subseteq L^*$.
(b) $M^{**} = M$.
(c) $(L \cap M)^* = L^* + M^*$ and $(L + M)^* = L^* \cap M^*$.

Proof. (a) This follows immediately from the definition.

(b) The inclusion $M \subseteq M^{**}$ follows immediately from the definition. We use dual bases to show that equality holds. Let (m_i) be an $\mathcal{O}$-basis of M and let (m_i^*) be the dual basis of V with respect to the form ψ . We have observed above that (m_i^*) is an $\mathcal{O}$-basis of M^* . Similarly the basis (m_i^{**}) of V dual to (m_i^*) is an $\mathcal{O}$-basis of M^{**} . But clearly $m_i^{**} = m_i$ for all i and it follows that $M^{**} = M$.

(c) We have $(L \cap M) \subseteq L \subseteq (L + M)$ and $(L \cap M) \subseteq M \subseteq (L + M)$, and so

$$(L \cap M)^* \supseteq (L^* + M^*) \quad \text{and} \quad (L^* \cap M^*) \supseteq (L + M)^* .$$

Therefore $(L^* \cap M^*)^* \subseteq (L+M)$ by (a) and (b). But since (b) implies that any lattice is the dual of some lattice, we also have $(L \cap M)^* \subseteq (L^* + M^*)$. Thus $(L \cap M)^* = (L^* + M^*)$. The other equality follows similarly (or by duality). □

Now we introduce an action of G. Let V be a KG-module, endowed with a non-degenerate symmetric bilinear form

$$\psi : V \times V \longrightarrow K$$

which is also *G-invariant*, that is, $\psi(g{\cdot}v, g{\cdot}w) = \psi(v, w)$ for all $v, w \in V$ and $g \in G$. For every subgroup H of G, let V^H be the subspace of H-fixed elements in V and consider the symmetric bilinear form

$$\psi^H : V^H \times V^H \longrightarrow K \tag{33.3}$$

defined by $\psi^H(v, w) = |H|^{-1}\psi(v, w)$. Note that $|H|^{-1}$ is well-defined because the characteristic of K is zero. For the trivial subgroup $H = 1$, we have $\psi^1 = \psi$.

(33.4) LEMMA. *With the notation above, let $F \leq H$ be subgroups of G.*

(a) The inclusion map $r^H_F : V^H \to V^F$ is the adjoint of the relative trace map $t^H_F : V^F \to V^H$ (with respect to the forms ψ^H and ψ^F).

(b) The form ψ^H is non-degenerate.

Proof. (a) If $v \in V^H$ and $w \in V^F$, then

$$\begin{aligned} \psi^H(t^H_F(w), v) &= |H|^{-1}\psi(\sum_{h \in [H/F]} h{\cdot}w, v) = |H|^{-1} \sum_{h \in [H/F]} \psi(h{\cdot}w, h{\cdot}v) \\ &= |H|^{-1}|H:F|\,\psi(w, v) = \psi^F(w, r^H_F(v)). \end{aligned}$$

(b) Let $v \in V^H$ be in the kernel of ψ^H. For every $w \in V$, we have $\psi(w, r^H_1(v)) = \psi^H(t^H_1(w), v) = 0$. Since ψ is non-degenerate, it follows that $r^H_1(v) = 0$, that is, $v = 0$. □

Now we consider lattices in the subspace V^H. If M is an $\mathcal{O}$-lattice in V^H, the dual lattice of M with respect to the form ψ^H will be written M^* without any reference to H, for it will always be clear which space and form we are dealing with. The following easy result is the crucial property for the sequel.

(33.5) PROPOSITION. *Let L be an $\mathcal{O}G$-lattice, endowed with a non-degenerate G-invariant symmetric bilinear form ψ, let H be a subgroup of G, and let $L_1^H = t_1^H(L)$.*
(a) L_1^H is a lattice in $(KL)^H$ and $(L_1^H)^* = (L^*)^H$.
(b) If L is unimodular, then $(L_1^H)^* = L^H$.

Proof. (a) We have $|H|{\cdot}L^H \subseteq L_1^H \subseteq L^H$ (because $|H|{\cdot}v = t_1^H(v)$ for any $v \in L^H$). Therefore L_1^H is a lattice in $K(L^H) = (KL)^H$. Now let $v \in (KL)^H$. Then $v \in (L_1^H)^*$ if and only if $\psi^H(v, t_1^H(w)) \in \mathcal{O}$ for every $w \in L$. Since t_1^H is the adjoint of r_1^H (Lemma 33.4), this holds if and only if $\psi(r_1^H(v), w) \in \mathcal{O}$ for every $w \in L$. But this means that $r_1^H(v) \in L^*$ and therefore

$$(L_1^H)^* = (r_1^H)^{-1}(L^*) = L^* \cap (KL)^H = (L^*)^H .$$

(b) This follows immediately from (a) because $L = L^*$ if L is unimodular (Exercise 33.1). □

More generally, if $F \leq H$ and if M is a lattice in $(KL)^F$, then $t_F^H(M)^*$ is a lattice in $(KL)^H$ and we have $t_F^H(M)^* = M^* \cap (KL)^H$ (Exercise 33.2).

We are ready for the main result. Let us say that a G-algebra A is *symmetric* if A is symmetric as an algebra and if some symmetrizing form is G-invariant. Moreover A is called *unimodular symmetric* if some G-invariant symmetrizing form is unimodular. We also assume that A is free as an $\mathcal{O}$-module, so that A is in particular an $\mathcal{O}G$-lattice and the previous discussion applies.

There are two main examples. If L is an $\mathcal{O}G$-lattice, the G-algebra $A = \mathrm{End}_{\mathcal{O}}(L)$ has a trace form which is G-invariant and unimodular symmetric (Lemma 32.5). The other example is the group algebra $A = \mathcal{O}G$. The symmetrizing form λ, defined by $\lambda(1) = 1$ and $\lambda(g) = 0$ for $1 \neq g \in G$, is unimodular and G-invariant.

Before stating the result, we indicate that we shall work with the ring $\overline{\mathcal{O}} = \mathcal{O}/|G|{\cdot}\mathcal{O}$. Since $\mathcal{O}$ is a discrete valuation ring with unique maximal ideal $\mathfrak{p} = \pi\mathcal{O}$, we have $|G|{\cdot}\mathcal{O} = \pi^r\mathcal{O}$ for some $r \geq 0$. In order to avoid trivialities, we can assume that p divides $|G|$, so that $|G|{\cdot}\mathcal{O} \subseteq \pi\mathcal{O}$ and $\overline{\mathcal{O}} \neq \{0\}$ (that is, $r \geq 1$). The ring $\overline{\mathcal{O}}$ is uniserial, in the sense that it has a unique chain of ideals

$$0 = \overline{\pi}^r\overline{\mathcal{O}} \subset \overline{\pi}^{r-1}\overline{\mathcal{O}} \subset \ldots \subset \overline{\pi}\overline{\mathcal{O}} \subset \overline{\mathcal{O}} ,$$

where $\overline{\pi}$ is the image of π in $\overline{\mathcal{O}}$. In case $\mathcal{O}$ is totally unramified (that is, if we can choose $\pi = p$), then $\overline{\mathcal{O}}$ is an unramified extension of $\mathbb{Z}/p^r\mathbb{Z}$ whose residue field extension is the extension k of $\mathbb{Z}/p\mathbb{Z}$.

(33.6) THEOREM. *Assume that* $\mathcal{O}$ *is a discrete valuation ring satisfying Assumption 33.1. Let* A *be a unimodular symmetric* G*-algebra and assume that* A *is free as an* $\mathcal{O}$*-module.*

(a) *For every subgroup* H *of* G, *the stable quotient* $\overline{A^H} = A^H/A_1^H$ *is a symmetric algebra over* $\overline{\mathcal{O}}$, *where* $\overline{\mathcal{O}} = \mathcal{O}/|G|{\cdot}\mathcal{O}$.

(b) *There exist symmetrizing forms* $\mu^H : \overline{A^H} \to \overline{\mathcal{O}}$ *(for* H *running over all subgroups of* G*) with the following adjointness property. If* $F \le H \le G$, *the restriction map* $\overline{r}_F^H$ *is the adjoint of the relative trace map* $\overline{t}_F^H$ *(with respect to the bilinear forms corresponding to* μ^H *and* μ^F*).*

Proof. By assumption there is a G-invariant unimodular symmetrizing form $\lambda : A \to \mathcal{O}$, with corresponding bilinear form $\psi(a,b) = \lambda(ab)$. We also view λ as a symmetrizing form for the K-algebra $K \otimes_{\mathcal{O}} A$. The linear form

$$\lambda^H = |H|^{-1}{\cdot}\lambda : K \otimes_{\mathcal{O}} A^H \longrightarrow K$$

defines a symmetric algebra structure on $K \otimes_{\mathcal{O}} A^H$ with associated bilinear form $\psi^H = |H|^{-1}\psi$ (as defined in 33.3). Indeed ψ^H is non-degenerate by Lemma 33.4. Note that $\lambda^H(A^H) \subseteq |H|^{-1}{\cdot}\mathcal{O}$ because $\lambda(A) \subseteq \mathcal{O}$.

For every subgroup H of G, we let $\overline{a}$ be the image of $a \in A^H$ in the stable quotient $\overline{A^H}$. Note that $|H|{\cdot}\overline{A^H} = 0$ because we have $|H|{\cdot}A^H \subseteq A_1^H \subseteq A^H$ (using the fact that $|H|{\cdot}a = t_1^H(a)$ if $a \in A^H$). Thus $\overline{A^H}$ is in particular an $\overline{\mathcal{O}}$-algebra. It is convenient to work uniformly for all subgroups with the base ring $\overline{\mathcal{O}} = \mathcal{O}/|G|{\cdot}\mathcal{O}$ (rather than $\mathcal{O}/|H|{\cdot}\mathcal{O}$ for each H). Define a linear form

$$\mu^H : \overline{A^H} \longrightarrow \overline{\mathcal{O}}, \qquad \mu^H(\overline{a}) = \overline{|G|{\cdot}\lambda^H(a)}\,.$$

By definition of λ^H, we have $|G|{\cdot}\lambda^H(a) = |G{:}H|{\cdot}\lambda(a) \in \mathcal{O}$, so that its image in $\overline{\mathcal{O}}$ makes sense. In order to show that μ^H is well-defined, suppose that $\overline{a} = 0$, so that $a \in A_1^H$. Since $A_1^H = (A^H)^*$ (by Proposition 33.5 and the unimodularity of A), we deduce that $\lambda^H(a) = \psi^H(a,1) \in \mathcal{O}$ because $1 \in A^H$. Therefore $|G|{\cdot}\lambda^H(a) \in |G|{\cdot}\mathcal{O}$ and $\overline{|G|{\cdot}\lambda^H(a)} = 0$.

As it is clear that μ^H defines a symmetric form on $\overline{A^H}$, we are left with the proof of non-degeneracy and unimodularity. This is a restatement of the fact that A_1^H is the dual lattice of A^H (Proposition 33.5). Indeed if $\mu^H(\overline{a}\,\overline{A^H}) = 0$, then $|G|{\cdot}\lambda^H(aA^H) \subseteq |G|{\cdot}\mathcal{O}$, so that $\lambda^H(aA^H) \subseteq \mathcal{O}$. Therefore $a \in (A^H)^* = A_1^H$ and $\overline{a} = 0$. This proves the non-degeneracy of the form.

For the unimodularity, we let $\overline{f} : \overline{A^H} \to \overline{\mathcal{O}}$ be any $\overline{\mathcal{O}}$-linear form. We need to prove the existence of $\overline{b} \in \overline{A}^H$ such that $\overline{f}(\overline{a}) = \mu^H(\overline{a}\,\overline{b})$ for all $\overline{a} \in \overline{A^H}$. Since A^H is a free $\mathcal{O}$-module (Proposition 1.5), the map

$A^H \to \overline{A^H} \xrightarrow{\overline{f}} \overline{\mathcal{O}}$ lifts to an $\mathcal{O}$-linear map $f : A^H \to \mathcal{O}$. This map extends to a K-linear form $f : K \otimes_{\mathcal{O}} A^H \to K$. Since the bilinear form ψ^H is non-degenerate over the field K (Lemma 33.4), it is unimodular over K and therefore there exists $b' \in K \otimes_{\mathcal{O}} A^H$ such that $f(a) = \psi^H(a, b')$ for all $a \in K \otimes_{\mathcal{O}} A^H$. Let $b = |G|^{-1} \cdot b'$, so that $f(a) = |G| \cdot \psi^H(a, b)$ for all a. We claim that $b \in A^H$. To this end, it suffices to prove that $b \in (A_1^H)^*$. But for every $c \in A_1^H$, we have $\overline{c} = 0$, hence $\overline{f}(\overline{c}) = 0$. Therefore $f(c) \in |G| \cdot \mathcal{O}$ and so $\psi^H(c, b) \in \mathcal{O}$. This means exactly that $b \in (A_1^H)^* = A^H$. Now the equation

$$f(a) = |G| \cdot \psi^H(a, b) = |G| \cdot \lambda^H(ab)$$

holds for every $a \in A^H$ and has values in $\mathcal{O}$. Therefore $\overline{f}(\overline{a}) = \mu^H(\overline{a}\,\overline{b})$, as was to be shown. The proof of (a) is complete.

We use the forms μ^H to prove (b). Let $F \leq H$ and let $a \in A^H$, $b \in A^F$. By Lemma 33.4, we have

$$\lambda^H(a\, t_F^H(b)) = \psi^H(a, t_F^H(b)) = \psi^F(r_F^H(a), b) = \lambda^F(r_F^H(a) b) .$$

Multiplying by $|G|$ and taking images in $\overline{\mathcal{O}}$, we obtain $\mu^H(\overline{a}\, \overline{t}_F^H(\overline{b})) = \mu^F(\overline{r}_F^H(\overline{a})\, \overline{b})$, which is the required adjointness property. □

(33.7) REMARKS. (a) In the above proof, we did not need to prove unimodularity, because, over the artinian ring $\overline{\mathcal{O}}$, the unimodularity property follows automatically from the non-degeneracy. Indeed any finitely generated $\overline{\mathcal{O}}$-module has a composition length (and any composition factor as an $\mathcal{O}$-module is simply isomorphic to k). The dual $\mathrm{Hom}_{\overline{\mathcal{O}}}(M, \overline{\mathcal{O}})$ of an $\overline{\mathcal{O}}$-module M has the same composition length as M and therefore any injective map $M \to \mathrm{Hom}_{\overline{\mathcal{O}}}(M, \overline{\mathcal{O}})$ must be an isomorphism (see Exercise 33.5).

(b) We indicate why the uniform treatment using $\overline{\mathcal{O}} = \mathcal{O}/|G|\mathcal{O}$ for all subgroups (rather than $\mathcal{O}/|H|\mathcal{O}$ for each subgroup H) does not change the non-degenerate form on $\overline{A^H}$. Since $|H| \cdot \overline{A^H} = 0$, any $\overline{\mathcal{O}}$-valued linear form on $\overline{A^H}$ actually has values in the ideal $|G{:}H| \cdot \overline{\mathcal{O}}$, which is isomorphic to $\mathcal{O}/|H|\mathcal{O}$ as an $\mathcal{O}$-module (via multiplication by $|G{:}H|^{-1}$). This induces an isomorphism $\mathrm{Hom}_{\overline{\mathcal{O}}}(\overline{A^H}, \overline{\mathcal{O}}) \cong \mathrm{Hom}_{\mathcal{O}/|H|\mathcal{O}}(\overline{A^H}, \mathcal{O}/|H|\mathcal{O})$. Therefore the isomorphism between $\overline{A^H}$ and its $\overline{\mathcal{O}}$-dual corresponding to the form μ^H can be viewed as an isomorphism

$$\theta : \overline{A^H} \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O}/|H|\mathcal{O}}(\overline{A^H}, \mathcal{O}/|H|\mathcal{O}) .$$

This corresponds to the $(\mathcal{O}/|H|\mathcal{O})$-valued form which we would have obtained by working with $\mathcal{O}/|H|\mathcal{O}$ (namely the one obtained from λ^H by multiplication by $|H|$ instead of $|G|$).

Theorem 33.6 can be applied to the case of the group algebra $\mathcal{O}G$, but we only specialize here to the case of $\mathcal{O}G$-lattices. If M is an $\mathcal{O}G$-lattice, the trace form $\lambda = \mathrm{tr}$ is a unimodular symmetrizing form on the G-algebra $\mathrm{End}_{\mathcal{O}}(M)$. Then the $\overline{\mathcal{O}}$-valued symmetrizing form μ^H on $\overline{\mathrm{End}}_{\mathcal{O}H}(M)$, as defined in the proof of Theorem 33.6, satisfies $\mu^H(\overline{a}) = \overline{|G:H|\cdot \mathrm{tr}(a)}$. In particular it is simply induced by tr when $G = H$.

More generally, we introduce another $\mathcal{O}G$-lattice L and we define a bilinear form

$$\widetilde{\phi}^H_{M,L} : \mathrm{Hom}_{\mathcal{O}H}(L,M) \times \mathrm{Hom}_{\mathcal{O}H}(M,L) \longrightarrow \overline{\mathcal{O}}$$

by $\widetilde{\phi}^H_{M,L}(a,b) = |G:H|\cdot \mathrm{tr}(ab)$. This form induces the Auslander–Reiten duality.

(33.8) THEOREM (Auslander–Reiten duality). *Let $\mathcal{O}$ satisfy Assumption 33.1, let $\overline{\mathcal{O}} = \mathcal{O}/|G|{\cdot}\mathcal{O}$, and let M be an $\mathcal{O}G$-lattice.*

(a) *For every $\mathcal{O}G$-lattice L and for every subgroup H, the form $\widetilde{\phi}^H_{M,L}$ defined above induces a non-degenerate bilinear form*

$$\phi^H_{M,L} : \overline{\mathrm{Hom}}_{\mathcal{O}H}(L,M) \times \overline{\mathrm{Hom}}_{\mathcal{O}H}(M,L) \longrightarrow \overline{\mathcal{O}}$$

satisfying the following properties.

(b) *If $F \leq H \leq G$, the restriction map $\overline{r}^H_F$ is the left and right adjoint of the relative trace map $\overline{t}^H_F$ (with respect to the forms $\phi^H_{M,L}$ and $\phi^F_{M,L}$).*

(c) *Let $\overline{f} \in \overline{\mathrm{Hom}}_{\mathcal{O}H}(L,N)$. Then the forms $\phi^H_{M,L}$ and $\phi^H_{M,N}$ satisfy the relation*

$$\phi^H_{M,L}(\overline{a}\overline{f}, \overline{b}) = \phi^H_{M,N}(\overline{a}, \overline{fb})$$

for all $\overline{a} \in \overline{\mathrm{Hom}}_{\mathcal{O}H}(N,M)$ and $\overline{b} \in \overline{\mathrm{Hom}}_{\mathcal{O}H}(M,L)$.

Proof. Consider first the case $L = M$. As remarked above, the form $\phi^H_{M,M}$ corresponds to the symmetrizing form μ^H on $\overline{\mathrm{End}}_{\mathcal{O}H}(M)$. Therefore in this case, (a) and (b) are restatements of Theorem 33.6.

For the general case, we apply the first case to the $\mathcal{O}G$-lattice $L \oplus M$. Let $A = \mathrm{End}_{\mathcal{O}H}(L \oplus M)$ and let $\overline{A} = \overline{\mathrm{End}}_{\mathcal{O}H}(L \oplus M)$ (for some fixed subgroup H). Let $e \in A$ be the idempotent projection onto M with kernel L, and let $\overline{e}$ be its image in $\overline{A}$. Then $eA(1-e) \cong \mathrm{Hom}_{\mathcal{O}H}(L,M)$ and $(1-e)Ae \cong \mathrm{Hom}_{\mathcal{O}H}(M,L)$. By Proposition 6.4, the symmetrizing form μ^H on $\overline{A}$ induces by restriction a duality between $\overline{e}A(1-\overline{e})$ and $(1-\overline{e})A\overline{e}$, hence a unimodular bilinear form

$$\psi : \overline{\mathrm{Hom}}_{\mathcal{O}H}(L,M) \times \overline{\mathrm{Hom}}_{\mathcal{O}H}(M,L) \longrightarrow \overline{\mathcal{O}}\,.$$

We are going to show that ψ coincides with the form $\phi^H_{M,L}$ of the statement. Let $i_M : M \to M \oplus L$ and $i_L : L \to M \oplus L$ be the injections, and let $p_M : M \oplus L \to M$ and $p_L : M \oplus L \to L$ be the projections (so that we have $e = i_M p_M$ and $1 - e = i_L p_L$ in the previous notation). An element $a \in \mathrm{Hom}_{\mathcal{O}H}(L, M)$ corresponds to the element $i_M a p_L \in eA(1-e)$, and similarly $b \in \mathrm{Hom}_{\mathcal{O}H}(M, L)$ corresponds to $i_L b p_M \in (1-e)Ae$. Thus we have

$$\begin{aligned}\psi(\overline{a}, \overline{b}) &= \mu^H\big(\,\overline{i_M a\, p_L}\ \overline{i_L b\, p_M}\,\big) = \mu^H\big(\,\overline{i_M a (id_L) b\, p_M}\,\big) \\ &= \overline{|G:H|\cdot \mathrm{tr}(i_M ab\, p_M)}\end{aligned}$$

by definition of the form μ^H. But $\mathrm{tr}(i_M ab\, p_M) = \mathrm{tr}(ab\, p_M i_M) = \mathrm{tr}(ab)$, and it follows that $\psi(\overline{a}, \overline{b}) = \overline{|G:H|\cdot \mathrm{tr}(ab)}$, as required.

Statement (b) is an easy consequence of the fact that it holds in the first case of the proof (applied to $L \oplus M$). The proof is left to the reader. Statement (c) is an immediate application of the obvious formula $\mathrm{tr}((af)b) = \mathrm{tr}(a(fb))$. □

Exercises

(33.1) Let $\mathcal{O}$ satisfy Assumption 33.1 and let V be a K-vector space endowed with a non-degenerate symmetric bilinear form ψ. Let M be an $\mathcal{O}$-lattice in V and let M^* be the dual lattice in V (with respect to ψ).

(a) Prove that the map

$$M^* \longrightarrow \mathrm{Hom}_{\mathcal{O}}(M, \mathcal{O}), \qquad v \mapsto \psi(v, -)$$

is an isomorphism of $\mathcal{O}$-lattices. Here $\psi(v, -)$ denotes the linear form mapping $w \in M$ to $\psi(v, w)$.

(b) Suppose that $\psi(v, w) \in \mathcal{O}$ for all $v, w \in M$ (so that M is endowed with an $\mathcal{O}$-valued non-degenerate symmetric bilinear form). Prove that M is unimodular if and only if $M = M^*$.

(33.2) Let $\mathcal{O}$ satisfy Assumption 33.1 and let V be a KG-module, endowed with a non-degenerate G-invariant symmetric bilinear form ψ. Let F and H be subgroups of G with $F \leq H$. Prove that if M is a lattice in V^F, then $t^H_F(M)^*$ is a lattice in V^H and that $t^H_F(M)^* = M^* \cap V^H$. Here the dual lattice in V^F (respectively V^H) is taken with respect to the form ψ^F (respectively ψ^H).

(33.3) Prove statement (b) in Theorem 33.8.

(33.4) Let $\mathcal{O}$ satisfy Assumption 33.1 and let M be an $\mathcal{O}G$-lattice. As in 33.3, let ψ^G be the bilinear form on $K \otimes_{\mathcal{O}} \mathrm{End}_{\mathcal{O}G}(M)$ defined by $\psi^G(a,b) = |G|^{-1}\,\mathrm{tr}(ab)$. Prove that the following conditions are equivalent.

(a) M is a projective $\mathcal{O}G$-lattice.

(b) $\mathrm{End}_{\mathcal{O}G}(M)$ is unimodular with respect to the form ψ^G.

(c) $\mathrm{tr}(\mathrm{End}_{\mathcal{O}G}(M)) = |G|{\cdot}\mathcal{O}$.

(d) $\mathrm{tr}(\mathrm{End}_{\mathcal{O}G}(M)) \subseteq |G|{\cdot}\mathcal{O}$.

Generalize to the case of an arbitrary unimodular symmetric G-algebra (free as an $\mathcal{O}$-module).

(33.5) Let $\mathcal{O}$ satisfy Assumption 33.1, let π be a generator of $\mathfrak{p}$, and let $\overline{\mathcal{O}} = \mathcal{O}/\pi^r\mathcal{O}$ for some $r \geq 1$. Let X and Y be (finitely generated) $\overline{\mathcal{O}}$-modules and let $\phi : X \times Y \to \overline{\mathcal{O}}$ be a non-degenerate bilinear form.

(a) Prove that X has a finite composition series (with every composition factor isomorphic to k). Prove that any two composition series of X have the same length $\ell(X)$ (Jordan–Hölder theorem).

(b) Prove that $\overline{\mathcal{O}}$ is an injective $\overline{\mathcal{O}}$-module. [Hint: Use for instance the criterion asserting that, for any ideal I, any $\overline{\mathcal{O}}$-linear map $I \to \overline{\mathcal{O}}$ extends to an endomorphism of $\overline{\mathcal{O}}$.]

(c) Deduce from (b) that $\ell(X^*) = \ell(X)$, where $X^* = \mathrm{Hom}_{\overline{\mathcal{O}}}(X, \overline{\mathcal{O}})$.

(d) Prove that ϕ induces isomorphisms $X \to Y^*$ and $Y \to X^*$. [Hint: Compare the lengths of X, Y, X^* and Y^*.]

(e) Let A be a submodule of X. Prove that $\ell(A) + \ell(A^\perp) = \ell(X)$ and that $A^{\perp\perp} = A$. [Hint: Let B be a submodule of X with $A \subseteq B$. Show that if every linear form $X \to \overline{\mathcal{O}}$ vanishing on A vanishes also on B, then $A = B$. Apply with $B = A^{\perp\perp}$.]

(f) Let A and B be submodules of X. Prove that $(A \cap B)^\perp = A^\perp + B^\perp$ and $(A+B)^\perp = A^\perp \cap B^\perp$.

(g) Let Z and T be $\overline{\mathcal{O}}$-modules and let $\psi : Z \times T \to \overline{\mathcal{O}}$ be a non-degenerate bilinear form. Let $f : X \to Z$ and $g : T \to Y$ be $\overline{\mathcal{O}}$-linear maps and assume that f and g are adjoint with respect to the forms ϕ and ψ. For any submodule A of Z, prove that $f^{-1}(A) = (g(A^\perp))^\perp$. In particular $\mathrm{Ker}(f) = \mathrm{Im}(g)^\perp$.

(33.6) Let $\mathcal{O}$ satisfy Assumption 33.1, let M be an $\mathcal{O}G$-lattice, and let $\phi^H_{M,L}$ be the form defined in Theorem 33.8 (where H is a subgroup of G and L is an $\mathcal{O}G$-lattice). Prove that $\phi^H_{M,L}(\overline{a}, \overline{b}\,\overline{f}) = \phi^H_{M,L}(\overline{f}\,\overline{a}, \overline{b})$ for all $\overline{f} \in \overline{\mathrm{End}}_{\mathcal{O}H}(M)$, $\overline{a} \in \overline{\mathrm{Hom}}_{\mathcal{O}H}(L,M)$ and $\overline{b} \in \overline{\mathrm{Hom}}_{\mathcal{O}H}(M,L)$.

Notes on Section 33

For orders and integral group rings, the Auslander–Reiten duality appears in Auslander [1977] and Roggenkamp [1977]. The proof given here for arbitrary unimodular symmetric G-algebras appears in Thévenaz [1988a], where some applications to the case of the group algebra $\mathcal{O}G$ are also discussed. Theorem 33.6 is due to Thévenaz [1988a] (see also Knörr [1987] in the case of $\mathcal{O}G$-lattices).

§ 34 ALMOST SPLIT SEQUENCES

Throughout this section, $\mathcal{O}$ denotes either a field k of characteristic p, or a complete discrete valuation ring of characteristic zero (satisfying Assumption 33.1). We use the Auslander–Reiten duality to prove the existence of almost split sequences of $\mathcal{O}G$-lattices. These sequences play an important role in representation theory and in fact exist for any k-algebra and any $\mathcal{O}$-order in a semi-simple K-algebra (where K is the field of fractions of the discrete valuation ring $\mathcal{O}$). We shall only discuss in this text some aspects of the theory. We shall prove in Section 35 a few properties of almost split sequences related to restriction and induction. Then in Section 36 we shall determine the defect groups of almost split sequences (viewed as indecomposable $\mathcal{O}G$-diagrams).

Recall that a short exact sequence

$$0 \longrightarrow L \stackrel{j}{\longrightarrow} E \stackrel{q}{\longrightarrow} M \longrightarrow 0$$

splits if and only if every homomorphism $f : X \to M$ can be lifted to a homomorphism $\widetilde{f} : X \to E$ such that $q\widetilde{f} = f$. Indeed this condition holds trivially if the sequence splits, and conversely it suffices to apply the condition to the homomorphism $id : M \to M$ to deduce a splitting. Almost split sequences are short exact sequences which do not split, but have the above property in almost all cases. Moreover we are going to see that an almost split sequence is attached to every non-projective indecomposable $\mathcal{O}G$-lattice M, and is unique up to isomorphism.

Let M be an indecomposable $\mathcal{O}G$-lattice. An *almost split sequence terminating in* M (also called an *Auslander–Reiten sequence*) is a short exact sequence

$$S_M : \ 0 \longrightarrow L \stackrel{j}{\longrightarrow} E \stackrel{q}{\longrightarrow} M \longrightarrow 0$$

having the following three properties:

(a) The sequence S_M does not split.
(b) L is indecomposable.
(c) For every homomorphism of $\mathcal{O}G$-lattices $f : X \to M$ which is not a split surjection, there exists a homomorphism $\widetilde{f} : X \to E$ such that $q\widetilde{f} = f$.

By a split surjection $f : X \to M$, we mean a surjection such that there exists a homomorphism $s : M \to X$ with $fs = id_M$. We immediately note that if a split surjection $f : X \to M$ could be lifted to a homomorphism $\widetilde{f} : X \to E$, then the sequence S_M would split (via the splitting $\widetilde{f}s$). Thus condition (c) means that every homomorphism $f : X \to M$ can be lifted to E , except in the trivial cases which would force the splitting of the sequence S_M . In particular there is no almost split sequence terminating in a projective $\mathcal{O}G$-lattice.

For non-projective indecomposable $\mathcal{O}G$-lattices, the existence of almost split sequences is a remarkable fact, which is a consequence of the Auslander–Reiten duality. In contrast the uniqueness of almost split sequences is an easy matter. We first prove this, starting with a lemma.

(34.1) LEMMA. *Let* $0 \longrightarrow L \overset{j}{\longrightarrow} E \overset{q}{\longrightarrow} M \longrightarrow 0$ *be a non-split short exact sequence of* $\mathcal{O}G$*-modules.*
(a) Suppose that L *is indecomposable and that* $f' \in \mathrm{End}_{\mathcal{O}G}(L)$ *and* $f \in \mathrm{End}_{\mathcal{O}G}(E)$ *are such that* (f', f, id_M) *is an endomorphism of the sequence. Then* f *and* f' *are isomorphisms.*
(b) Suppose that M *is indecomposable and that* $f' \in \mathrm{End}_{\mathcal{O}G}(M)$ *and* $f \in \mathrm{End}_{\mathcal{O}G}(E)$ *are such that* (id_L, f, f') *is an endomorphism of the sequence. Then* f *and* f' *are isomorphisms.*

Proof. (a) Since $qf = id_M q = q$, we have $q(id_E - f) = 0$. Thus $\mathrm{Im}(id_E - f)$ is contained in $\mathrm{Ker}(q)$, which is equal to $\mathrm{Im}(j)$. Since j is an isomorphism onto its image, it follows that there exists $s : E \to L$ such that $js = id_E - f$. Now $sj \in \mathrm{End}_{\mathcal{O}G}(L)$ cannot be an isomorphism, otherwise $(sj)^{-1}s$ would be a retraction of j and the sequence would split. Since L is indecomposable, id_L is a primitive idempotent of $\mathrm{End}_{\mathcal{O}G}(L)$, which is therefore a local ring (Corollary 4.6). Thus $sj \in J(\mathrm{End}_{\mathcal{O}G}(L))$ and consequently $id_L - sj \notin J(\mathrm{End}_{\mathcal{O}G}(L))$. It follows that $id_L - sj$ is an isomorphism (again because $\mathrm{End}_{\mathcal{O}G}(L)$ is a local ring). But we have $id_L - sj = f'$ because

$$j(id_L - sj) = j - jsj = j - (id_E - f)j = j - j + fj = jf' ,$$

and the injectivity of j implies $id_L - sj = f'$. Since both f' and id_M are isomorphisms, it follows by elementary diagram chasing (a special case of the so-called five lemma) that f is an isomorphism too.

(b) The proof is similar and is left to the reader. □

(34.2) PROPOSITION. *Let M be an indecomposable $\mathcal{O}G$-lattice. Any two almost split sequences terminating in M are isomorphic.*

Proof. Let the two almost split sequences be

$$0 \longrightarrow L \xrightarrow{j} E \xrightarrow{q} M \longrightarrow 0 \qquad \text{and} \qquad 0 \longrightarrow L' \xrightarrow{j'} E' \xrightarrow{q'} M \longrightarrow 0 .$$

Since the first sequence is almost split and since $q' : E' \to M$ is not a split surjection, there exists $f : E' \to E$ such that $qf = q'$. Similarly $q : E \to M$ lifts to $h : E \to E'$ such that $q'h = q$. The composite fh is an endomorphism of E inducing the identity on M (that is, $qfh = id_M q$). Thus fh also induces an endomorphism of L, hence an endomorphism of the first sequence. By Lemma 34.1 (which applies because L is indecomposable), fh is an automorphism of E, and therefore f has the right inverse $h(fh)^{-1}$. Similarly hf is an automorphism of E' and f has the left inverse $(hf)^{-1}h$. Thus f is an isomorphism, inducing the identity on M (that is, $qf = id_M q'$). It follows that f induces an isomorphism $g : L' \to L$ such that $fj' = jg$. The triple (g, f, id_M) is an isomorphism between the two sequences. □

We are going to use pull-backs in many of the subsequent arguments, in particular in the proof of the existence of almost split sequences. To this end we need the following easy lemma.

(34.3) LEMMA. *Assume that the following diagram of $\mathcal{O}G$-modules is a pull-back diagram.*

$$\begin{array}{ccc} Y & \xrightarrow{q'} & X \\ \downarrow{\scriptstyle h'} & & \downarrow{\scriptstyle h} \\ E & \xrightarrow{q} & M \end{array}$$

(a) *If q is surjective, then so is q', and h' induces an isomorphism* $\mathrm{Ker}(q') \cong \mathrm{Ker}(q)$.

(b) *There exists a homomorphism $\widetilde{h} : X \to E$ such that $q\widetilde{h} = h$ if and only if $q' : Y \to X$ is a split surjection.*

Proof. (a) In a pull-back diagram, the triple (Y, q', h') is unique up to a unique isomorphism. We can choose Y to be the set of all pairs $(e, x) \in E \times X$ such that $q(e) = h(x)$, and then h' and q' are the two projections. If q is surjective, then for every $x \in X$, there exists $e \in E$ such that $q(e) = h(x)$. This proves the surjectivity of q'. Moreover $(e, x) \in \mathrm{Ker}(q')$ if and only if $x = 0$ and $e \in \mathrm{Ker}(q)$, so that h' induces an isomorphism $\mathrm{Ker}(q') \cong \mathrm{Ker}(q)$.

(b) If $s : X \to Y$ is such that $q's = id_X$, then $\widetilde{h} = h's$ satisfies $q\widetilde{h} = qh's = hq's = h$. Conversely, if there exists $\widetilde{h}$ such that $q\widetilde{h} = h$, then the maps $id_X : X \to X$ and $\widetilde{h} : X \to E$ satisfy $q\widetilde{h} = h\, id_X$. Thus by definition of a pull-back, there exists a unique homomorphism $f : X \to Y$ such that $q'f = id_X$ and $h'f = \widetilde{h}$. The first of these equations says that q' is a split surjection. □

In the situation of the lemma, recall that $q' : Y \to X$ is said to be the *pull-back of* $q : E \to M$ *along* h.

The definition of almost split sequences is not symmetric since condition (c) is a condition on the right hand side surjection $q : E \to M$. We show that in fact it is equivalent to a condition on the left hand side injection $j : L \to E$.

(34.4) PROPOSITION. *Let* $0 \longrightarrow L \xrightarrow{j} E \xrightarrow{q} M \longrightarrow 0$ *be a non-split exact sequence, where* L *and* M *are indecomposable* $\mathcal{O}G$*-lattices. Then condition (c) in the definition of an almost split sequence is equivalent to the following condition:*

(c′) For every homomorphism of $\mathcal{O}G$*-lattices* $f : L \to Y$ *which is not a split injection, there exists a homomorphism* $\widetilde{f} : E \to Y$ *such that* $\widetilde{f}j = f$.

Proof. Suppose that (c′) holds and let $h : X \to M$ be a homomorphism which does not factorize through E. We have to prove that h is a split surjection. Consider the following pull-back diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \xrightarrow{j'} & Y & \xrightarrow{q'} & X & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle id_L} & & \downarrow{\scriptstyle h'} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & L & \xrightarrow{j} & E & \xrightarrow{q} & M & \longrightarrow & 0 \end{array}$$

By Lemma 34.3, q' is surjective and its kernel is isomorphic to L, so that j' exists making the top sequence exact and the diagram commute. Since h does not lift to a homomorphism $X \to E$ by assumption, the top sequence does not split (Lemma 34.3). Therefore $j' : L \to Y$ is not a split injection. By (c′), there exists a homomorphism $f' : E \to Y$ such that $f'j = j'$. This means that f' induces the identity on L, and therefore f' induces a homomorphism $f : M \to X$ making the following diagram commute.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \xrightarrow{j} & E & \xrightarrow{q} & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle id_L} & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \\ 0 & \longrightarrow & L & \xrightarrow{j'} & Y & \xrightarrow{q'} & X & \longrightarrow & 0 \end{array}$$

Composing the above two homomorphisms of sequences, we obtain an endomorphism $(id_L, h'f', hf)$ of the given sequence. Since this sequence does not split and M is indecomposable, hf is an isomorphism, by Lemma 34.1. Therefore h is a split surjection, since it has the right inverse $f(hf)^{-1}$.

The proof that (c) implies (c′) is analogous and is left to the reader. □

The proof of the existence of almost split sequences is based on the Auslander–Reiten duality. In order to have a uniform treatment for both the case of a field and the case of a dvr (that is, a discrete valuation ring), we introduce the following convenient notation. Let M be an $\mathcal{O}G$-lattice. We set

$$(34.5) \qquad TM = \begin{cases} \Omega M \oplus Q & \text{if } \mathcal{O} = k, \\ M \oplus Q & \text{if } \mathcal{O} \text{ is a dvr satisfying Assumption 33.1,} \end{cases}$$

where Q is an arbitrary projective $\mathcal{O}G$-lattice. Thus TM is not uniquely defined, but since stable quotients are not modified by addition of projective modules (Lemma 32.3), the stable quotient $\overline{\mathrm{Hom}}_{\mathcal{O}G}(M, TM)$ only depends on M. For the construction of almost split sequences, one can always choose $Q = 0$, but as soon as one discusses restriction to a subgroup H, it is very convenient to have the freedom of adding a projective module. Indeed $\mathrm{Res}^G_H(\Omega M)$ is in general not isomorphic to $\Omega(\mathrm{Res}^G_H(M))$, but to $\Omega(\mathrm{Res}^G_H(M)) \oplus Q$ for some projective $\mathcal{O}H$-lattice Q. Moreover the use of additional projective modules will be essential in Section 36.

With this notation, we can restate the Auslander–Reiten duality as follows. For every $\mathcal{O}G$-lattice L and every subgroup H of G, there exists a non-degenerate bilinear form

$$(34.6) \qquad \phi^H_{M,L} : \overline{\mathrm{Hom}}_{\mathcal{O}H}(L, TM) \times \overline{\mathrm{Hom}}_{\mathcal{O}H}(M, L) \longrightarrow \overline{\mathcal{O}},$$

where $\overline{\mathcal{O}} = \mathcal{O}/|G|\mathcal{O}$. Note that if p does not divide $|G|$, then $\overline{\mathcal{O}} = \{0\}$ and $\overline{\mathrm{Hom}}_{\mathcal{O}H}(L, M) = \{0\}$ for all L and M (because t^H_1 is surjective in that case). Thus we can assume that p divides $|G|$ and we obtain $\overline{\mathcal{O}} = k$ if $\mathcal{O} = k$. The bilinear form $\phi^H_{M,L}$ is obtained from Theorem 32.12 in case $\mathcal{O} = k$ and from Theorem 33.8 in case $\mathcal{O}$ is a discrete valuation ring. If M is projective, then all $\mathcal{O}G$-homomorphisms to M are projective and the stable quotients are zero (this includes the case where p does not divide $|G|$). Thus we can assume that M is non-projective.

We are going to apply the duality when $L = M$ and we write simply ϕ^H_M instead of $\phi^H_{M,M}$. In this case, if we let $A = \mathrm{End}_{\mathcal{O}}(M)$, then the stable quotient $\overline{A^H} = \overline{\mathrm{End}}_{\mathcal{O}H}(M)$ is in duality with $\overline{\mathrm{Hom}}_{\mathcal{O}H}(M, TM)$. Any homomorphism $M \to TM$ can be composed with an endomorphism of M and, as a consequence of 32.1, this induces a right $\overline{A^H}$-module structure on $\overline{\mathrm{Hom}}_{\mathcal{O}H}(M,TM)$. Moreover there is also a left $\overline{\mathrm{End}}_{\mathcal{O}H}(TM)$-module structure on $\overline{\mathrm{Hom}}_{\mathcal{O}H}(M,TM)$, which we turn into a left $\overline{A^H}$-module structure, by means of the isomorphism

$$(34.7)\qquad \overline{\mathrm{End}}_{\mathcal{O}H}(TM) \cong \overline{\mathrm{End}}_{\mathcal{O}H}(M) = \overline{A^H},$$

which we now recall. If $\mathcal{O}$ is a discrete valuation ring, then $TM = M \oplus Q$ and the isomorphism 34.7 follows from Lemma 32.3. In case $\mathcal{O} = k$, then $TM = \Omega M \oplus Q$ and the isomorphism 34.7 is described in Exercise 32.4 (using the fact that $0 \to \Omega M \oplus Q \to P \oplus Q \to M \to 0$ is a projective presentation of M if P is a projective cover of M). As a result of this discussion, $\overline{\mathrm{Hom}}_{\mathcal{O}H}(M,TM)$ is an $(\overline{A^H},\overline{A^H})$-bimodule, and we shall always view it endowed with this structure.

The Auslander–Reiten duality ϕ_M^H satisfies both the properties

$$(34.8)\qquad \phi_M^H(\overline{b}\cdot\overline{a},\overline{c}) = \phi_M^H(\overline{b},\overline{a}\cdot\overline{c}) \qquad \text{and} \qquad \phi_M^H(\overline{a}\cdot\overline{b},\overline{c}) = \phi_M^H(\overline{b},\overline{c}\cdot\overline{a}),$$

where $\overline{a},\overline{c} \in \overline{A^H}$ and $\overline{b} \in \overline{\mathrm{Hom}}_{\mathcal{O}H}(M,TM)$. The first equality follows from Theorems 32.12 and 33.8, and the second from Exercises 32.4 and 33.6.

We shall use repeatedly the following fact, which is an easy consequence of 34.8. Let X be an $\overline{\mathcal{O}}$-submodule of $\overline{A^H}$. Then X is a left (respectively right) ideal of $\overline{A^H}$ if and only if $X^\perp$ is a right (respectively left) $\overline{A^H}$-submodule of $\overline{\mathrm{Hom}}_{\mathcal{O}H}(M,TM)$. Similarly X is a two-sided ideal if and only if $X^\perp$ is an $(\overline{A^H},\overline{A^H})$-sub-bimodule.

Recall that the sum of all the simple submodules of a module X is called the socle of X and is written $\mathrm{Soc}(X)$. We know that the socle of a symmetric algebra is the orthogonal of its Jacobson radical (Exercise 6.2). The same idea is used in the following result.

(34.9) LEMMA. *Let M be an $\mathcal{O}G$-lattice and let $A = \mathrm{End}_{\mathcal{O}}(M)$.*

(a) *Let H be a subgroup of G. The orthogonal of $J(\overline{A^H})$ with respect to the form ϕ_M^H is equal to $\mathrm{Soc}(\overline{\mathrm{Hom}}_{\mathcal{O}H}(M,TM))$, the socle of $\overline{\mathrm{Hom}}_{\mathcal{O}H}(M,TM)$ viewed as a right $\overline{A^H}$-module. Moreover $\mathrm{Soc}(\overline{\mathrm{Hom}}_{\mathcal{O}H}(M,TM))$ is also the socle of $\overline{\mathrm{Hom}}_{\mathcal{O}H}(M,TM)$ as a left $\overline{A^H}$-module.*

(b) *If M is indecomposable and non-projective, $\mathrm{Soc}(\overline{\mathrm{Hom}}_{\mathcal{O}G}(M,TM))$ is a simple right $\overline{A^G}$-module (hence the unique simple right submodule of $\overline{\mathrm{Hom}}_{\mathcal{O}G}(M,TM)$).*

(c) *Assume that M is indecomposable and non-projective. If $f : X \to M$ is a homomorphism of $\mathcal{O}G$-lattices which is not a split surjection and if $\overline{f}$ denotes its image in $\overline{\mathrm{Hom}}_{\mathcal{O}G}(X,M)$, then $\overline{u}\,\overline{f} = 0$ for every $\overline{u} \in \mathrm{Soc}(\overline{\mathrm{Hom}}_{\mathcal{O}G}(M,TM))$ (where $\overline{u}\,\overline{f}$ is induced by the composition of maps).*

Proof. (a) Let $\overline{u} \in \overline{\mathrm{Hom}}_{\mathcal{O}H}(M, TM)$. By definition of the socle, we have $\overline{u} \in \mathrm{Soc}(\overline{\mathrm{Hom}}_{\mathcal{O}H}(M, TM))$ if and only if $\overline{u}\overline{j} = 0$ for all $\overline{j} \in J(\overline{A^H})$. By the non-degeneracy of the form ϕ_M^H , this holds if and only if

$$\phi_M^H(\overline{u}\overline{j}, \overline{a}) = 0 \quad \text{for all } \overline{a} \in \overline{A^H} .$$

But we have $\phi_M^H(\overline{u}\overline{j}, \overline{a}) = \phi_M^H(\overline{u}, \overline{j}\overline{a})$ by 34.8, and $\overline{j}\overline{a}$ runs over $J(\overline{A^H})$ for $\overline{j} \in J(\overline{A^H})$ and $\overline{a} \in \overline{A^H}$. Thus the above condition is equivalent to

$$\phi_M^H(\overline{u}, \overline{j}) = 0 \quad \text{for all } \overline{j} \in J(\overline{A^H}) ,$$

which means that $\overline{u} \in J(\overline{A^H})^\perp$. The proof that $\mathrm{Soc}(\overline{\mathrm{Hom}}_{\mathcal{O}H}(M, TM))$ is also the socle of $\overline{\mathrm{Hom}}_{\mathcal{O}H}(M, TM)$ as a left $\overline{A^H}$-module is similar and is left as an exercise.

(b) If M is indecomposable, A^G is a local ring (Corollary 4.6). Since M is not projective, A is not a projective G-algebra (Corollary 17.4), so that the ideal A_1^G is not the whole of A^G . Therefore $A_1^G \subseteq J(A^G)$ and the stable quotient $\overline{A^G}$ is a local ring with unique maximal ideal $J(\overline{A^G})$. We have to prove that the socle $S = \mathrm{Soc}(\overline{\mathrm{Hom}}_{\mathcal{O}G}(M, TM))$ is a simple right $\overline{A^G}$-module. Let R be a non-zero right submodule of S . By 34.8, $R^\perp$ is a proper left ideal of $\overline{A^G}$. Moreover

$$J(\overline{A^G}) = S^\perp \subseteq R^\perp \neq \overline{A^G} .$$

Since $J(\overline{A^G})$ is a maximal left ideal of $\overline{A^G}$, we deduce that $S^\perp = R^\perp$, and therefore $S = S^{\perp\perp} = R^{\perp\perp} = R$. The equality between a submodule and its double orthogonal is a standard fact for a non-degenerate form over a field and follows from Exercise 33.5 for a non-degenerate form over $\overline{\mathcal{O}}$.

(c) We assume that $f \in \mathrm{Hom}_{\mathcal{O}G}(X, M)$ is not a split surjection. We first prove that $\overline{f}\,\overline{g} \in J(\overline{A^G})$ for every $\overline{g} \in \overline{\mathrm{Hom}}_{\mathcal{O}G}(M, X)$. If $\overline{f}\,\overline{g} \notin J(\overline{A^G})$, then $fg \notin J(A^G)$, and therefore fg is an isomorphism since A^G is a local ring. It follows that f has the right inverse $g(fg)^{-1}$, contradicting the assumption that f is not a split surjection. Consider now the Auslander–Reiten duality $\phi_{M,X}^G$ corresponding to the $\mathcal{O}G$-lattice X . If $\overline{u} \in \mathrm{Soc}(\overline{\mathrm{Hom}}_{\mathcal{O}G}(M, TM))$, then by Theorems 32.12 and 33.8, we have

$$\phi_{M,X}^G(\overline{u}\,\overline{f}, \overline{g}) = \phi_{M,M}^G(\overline{u}, \overline{f}\,\overline{g}) = 0 ,$$

since $\overline{f}\,\overline{g} \in J(\overline{A^G})$ and $\overline{u} \in J(\overline{A^G})^\perp$. As this equation holds for every $\overline{g} \in \overline{\mathrm{Hom}}_{\mathcal{O}G}(M, X)$, the non-degeneracy of the form $\phi_{M,X}^G$ implies that $\overline{u}\,\overline{f} = 0$. □

A homomorphism $u : M \to TM$ will be called *almost projective* if $\overline{u} \in \mathrm{Soc}(\mathrm{Hom}_{\mathcal{O}G}(M, TM))$ but $\overline{u} \neq 0$. Note that $\overline{u} = 0$ if and only if u is projective. We need to know that pull-backs along projective homomorphisms give rise to split sequences.

(34.10) LEMMA. *Let N be an $\mathcal{O}G$-lattice, let $q : P \to N$ be a projective cap of N, and let $u \in \mathrm{Hom}_{\mathcal{O}G}(M, N)$. The pull-back of $q : P \to N$ along u is a split surjection if and only if u is projective.*

Proof. Consider the following pull-back diagram.

$$\begin{array}{ccc} E & \xrightarrow{q'} & M \\ {\scriptstyle u'}\downarrow & & \downarrow{\scriptstyle u} \\ P & \xrightarrow{q} & N \end{array}$$

By Lemma 32.2, u is projective if and only if u factorizes through P. This in turn is equivalent to the splitting of $q' : E \to M$, by Lemma 34.3. □

In fact the pull-backs of $P \to N$ along u and $u + u'$ are isomorphic for any $u' \in \mathrm{Hom}_{\mathcal{O}}(M, N)_1^G$ (Exercise 34.3). We have paved the way for the proof of the existence of almost split sequences.

(34.11) THEOREM. *Let $\mathcal{O}$ be either a field of characteristic p or a discrete valuation ring satisfying Assumption 33.1. Let M be a non-projective indecomposable $\mathcal{O}G$-lattice, let TM be defined as in 34.5, let $q : P \to TM$ be a projective cover of TM, and let $u \in \mathrm{Hom}_{\mathcal{O}G}(M, TM)$.*

(a) *The pull-back along u of the sequence $0 \to \Omega TM \to P \to TM \to 0$ is an almost split sequence if and only if u is almost projective. In particular there exists an almost split sequence terminating in M.*

(b) *The kernel of an almost split sequence terminating in M is isomorphic to $\Omega^2 M$ if $\mathcal{O} = k$ and to ΩM if $\mathcal{O}$ is a discrete valuation ring.*

Proof. The pull-back along u of the projective cover of TM gives rise to the following diagram of exact sequences.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Omega TM & \xrightarrow{j'} & E & \xrightarrow{q'} & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle u'} & & \downarrow{\scriptstyle u} & & \\ 0 & \longrightarrow & \Omega TM & \xrightarrow{j} & P & \xrightarrow{q} & TM & \longrightarrow & 0 \end{array}$$

By Lemma 34.10, the top sequence splits if and only if u is projective, and on the other hand an almost split sequence does not split by definition.

Thus we can assume that u is not projective, that is, $\overline{u} \neq 0$ in the stable quotient $\overline{\mathrm{Hom}}_{\mathcal{O}G}(M, TM)$.

By the construction of TM, there is a projective $\mathcal{O}G$-lattice Q such that $TM = \Omega M \oplus Q$ if $\mathcal{O} = k$, and $TM = M \oplus Q$ if $\mathcal{O}$ is a discrete valuation ring. Since $\Omega Q = 0$, we have $\Omega TM = \Omega^2 M$ in the first case and $\Omega TM = \Omega M$ in the second. This proves that the kernel ΩTM of the sequence is indecomposable (because M is indecomposable), so that the second condition of the definition of an almost split sequence is satisfied. Moreover the assertion (b) is established.

We are left with the proof that $\overline{u} \in \mathrm{Soc}(\overline{\mathrm{Hom}}_{\mathcal{O}G}(M, TM))$ if and only if the third condition of the definition of an almost split sequence is satisfied. Let $f : X \to M$ be any homomorphism of $\mathcal{O}G$-lattices. By definition of a pull-back, f lifts to $\widetilde{f} : X \to E$ if and only if there exists $g : X \to P$ such that $qg = uf$ (because such a pair (g, f) defines a map $\widetilde{f} : X \to E$, and conversely the existence of $\widetilde{f}$ defines $g = u'\widetilde{f}$). Now by Lemma 32.2, the existence of g is equivalent to the condition that uf be projective. This shows that the third condition of the definition of an almost split sequence is equivalent to the following statement:

(34.12) For every homomorphism of $\mathcal{O}G$-lattices $f : X \to M$ which is not a split surjection, uf is projective.

By Lemma 34.9, this condition is satisfied if $\overline{u} \in \mathrm{Soc}(\overline{\mathrm{Hom}}_{\mathcal{O}G}(M, TM))$, proving one implication. If conversely 34.12 is satisfied, we can apply it to the case $X = M$ and $f \in J(\mathrm{End}_{\mathcal{O}G}(M))$. Note that f cannot be a split surjection since an endomorphism of an indecomposable module which is a split surjection is necessarily an isomorphism. Then $\overline{f} \in J(\overline{\mathrm{End}}_{\mathcal{O}G}(M))$ and 34.12 says that $\overline{u}\,\overline{f} = 0$. Thus $\overline{u}$ is annihilated by the radical of $\overline{\mathrm{End}}_{\mathcal{O}G}(M)$ and therefore belongs to the socle of $\overline{\mathrm{Hom}}_{\mathcal{O}G}(M, TM)$ as a right $\overline{\mathrm{End}}_{\mathcal{O}G}(M)$-module. This proves the converse statement and establishes the theorem. □

We end this section with an easy observation.

(34.13) LEMMA. *Let S_M be an almost split sequence terminating in a non-projective indecomposable $\mathcal{O}G$-lattice M. Then S_M is an indecomposable $\mathcal{O}G$-diagram.*

Proof. By Exercise 31.6, any direct summand of a short exact sequence is a short exact sequence. Since both M and ΩTM are indecomposable, the only possible non-trivial decomposition of a short exact sequence S starting in ΩTM and terminating in M has the form

$$S \cong (0 \to \Omega TM \to \Omega TM \to 0 \to 0) \oplus (0 \to 0 \to M \to M \to 0).$$

But this means that the exact sequence S splits. Since an almost split sequence does not split, the result follows. □

Exercises

(34.1) Prove part (b) of Lemma 34.1.

(34.2) Complete the proof of Proposition 34.4 by showing that (c) implies (c′).

(34.3) Let $u, u' : M \to N$ be homomorphisms of $\mathcal{O}G$-lattices and let $P \to N$ be a projective cap of N. If u' is projective, prove that the pull-backs of $P \to N$ along u and $u + u'$ are isomorphic.

(34.4) Let M be an indecomposable $\mathcal{O}G$-lattice and consider a short exact sequence $0 \to L \to E \to M \to 0$ satisfying conditions (a) and (c) of the definition of an almost split sequence. Prove that the sequence is isomorphic to the direct sum of the almost split sequence terminating in M and a sequence of the form $0 \to L' \to L' \to 0 \to 0$.

(34.5) Let M be a (not necessarily indecomposable) $\mathcal{O}G$-lattice, let $u \in \mathrm{Hom}_{\mathcal{O}G}(M, TM)$, and let the short exact sequence

$$S:\ 0 \longrightarrow L \xrightarrow{j} E \xrightarrow{q} M \longrightarrow 0$$

be the pull-back along u of a projective cover of TM.

(a) If $\overline{u} \in \mathrm{Soc}(\overline{\mathrm{Hom}}_{\mathcal{O}G}(M, TM))$, prove that S is a direct sum of split and almost split sequences. [Hint: Choose a decomposition $M = \oplus_i M_i$ into indecomposable $\mathcal{O}G$-lattices and consider the sequence

$$T_i:\ 0 \longrightarrow L \xrightarrow{j} q^{-1}(M_i) \xrightarrow{q} M_i \longrightarrow 0 .$$

Use the assumption on u to prove that T_i satisfies condition (c) of the definition of an almost split sequence. Deduce that

$$T_i \;\cong\; (0 \to L' \to L' \to 0 \to 0) \,\oplus\, S_i$$

for some L', where S_i is either the almost split sequence terminating in M_i or the split sequence $0 \to \Omega TM_i \to \Omega TM_i \oplus M_i \to M_i \to 0$ (Exercise 34.4). Show that S_i is a direct summand of S. In case S_i is almost split, this uses condition (c) of the definition, applied to the surjection $E \to M \to M_i$, followed by an application of Lemma 34.1.]

(b) If S is a direct sum of split and almost split sequences, prove that $\overline{u} \in \mathrm{Soc}(\overline{\mathrm{Hom}}_{\mathcal{O}G}(M, TM))$. [Hint: Prove that any $f \in J(\mathrm{End}_{\mathcal{O}G}(M))$ can be lifted to $\widetilde{f} : M \to E$ such that $q\widetilde{f} = f$. Deduce that $\overline{u}\,\overline{f} = 0$ and use 34.8 to show that $\mathrm{Soc}(\overline{\mathrm{Hom}}_{\mathcal{O}G}(M, TM))$ is the annihilator of $J(\mathrm{End}_{\mathcal{O}G}(M))$.]

Notes on Section 34

The definition and the basic properties of almost split sequences are due to Auslander–Reiten [1975], who also proved their existence for modules over any finite dimensional algebra over a field (and more generally over any Artin algebra). The fact that the kernel of an almost split sequence terminating in M is equal to $\Omega^2 M$ is a special feature of group algebras (and more generally symmetric algebras). The construction of almost split sequences as pull-backs is a classical consequence of the isomorphism $\overline{\mathrm{Hom}}_{\mathcal{O}G}(M, TM) \cong \mathrm{Ext}_{\mathcal{O}G}(M, \Omega TM)$.

The proof of the existence of almost split sequences for group algebras over a complete discrete valuation ring appears in Auslander [1977], Roggenkamp–Schmidt [1976], and Roggenkamp [1977].

The use of almost split sequences in the representation theory of finite groups started with the papers by Webb [1982] and by Benson and Parker [1984]. The theory has been particularly used in Erdmann's work on tame blocks, culminating in her book Erdmann [1990]. We also refer the reader to the book by Benson [1991].

§ 35 RESTRICTION AND INDUCTION OF ALMOST SPLIT SEQUENCES

Throughout this section, $\mathcal{O}$ denotes either a field k of characteristic p, or a complete discrete valuation ring of characteristic zero (satisfying Assumption 33.1). We consider the question of the behaviour of almost split sequences under restriction and induction. We only prove a few results in this direction and refer to the exercises for the general method for handling this question (Exercises 35.3 and 35.4).

We first introduce some notation. Let M be an $\mathcal{O}G$-lattice and let $A = \mathrm{End}_{\mathcal{O}}(M)$ be the corresponding G-algebra. For every subgroup H of G, let $\overline{A^H} = A^H/A_1^H$ be the stable quotient. Since the projective points of A^H are those lying in the ideal A_1^H, the surjection $A^H \to \overline{A^H}$ induces a bijection between the set of all non-projective points of A^H and the set $\mathcal{P}(\overline{A^H})$ (Theorem 3.2). Every non-projective point $\alpha \in \mathcal{P}(A^H - A_1^H)$ corresponds to a maximal ideal $\mathfrak{m}_\alpha$ containing A_1^H, so that

$$\overline{\mathfrak{m}}_\alpha = \mathfrak{m}_\alpha/A_1^H \supseteq J(\overline{A^H}) .$$

Taking orthogonals with respect to the Auslander–Reiten duality ϕ_M^H between $\overline{A^H}$ and $\overline{\mathrm{Hom}}_{\mathcal{O}H}(M, TM)$ (see 34.6), we define

$$\begin{aligned} L_M(H_\alpha) &= \overline{\mathfrak{m}}_\alpha^{\perp} , \\ L_M(H) &= J(\overline{A^H})^{\perp} = \mathrm{Soc}(\overline{\mathrm{Hom}}_{\mathcal{O}H}(M, TM)) . \end{aligned} \tag{35.1}$$

Since $J(\overline{A^H}) = \bigcap_{\alpha \in \mathcal{P}(A^H - A_1^H)} \overline{\mathfrak{m}}_\alpha$ and since we have a decomposition of $(\overline{A^H}, \overline{A^H})$-bimodules

$$\overline{A^H}/J(\overline{A^H}) \cong \prod_{\alpha \in \mathcal{P}(A^H - A_1^H)} \overline{A^H}/\overline{\mathfrak{m}}_\alpha \cong \bigoplus_{\alpha \in \mathcal{P}(A^H - A_1^H)} S(\alpha) ,$$

we deduce by duality a decomposition of $(\overline{A^H}, \overline{A^H})$-bimodules

$$L_M(H) = \bigoplus_{\alpha \in \mathcal{P}(A^H - A_1^H)} L_M(H_\alpha) .$$

Since $\overline{\mathfrak{m}}_\alpha$ is a maximal two-sided ideal of $\overline{A^H}$, its orthogonal $L_M(H_\alpha)$ is in fact a minimal sub-bimodule of $\overline{\mathrm{Hom}}_{\mathcal{O}H}(M, TM)$ (Exercise 35.1).

The first result is concerned with restriction.

(35.2) PROPOSITION. *Let* $A = \mathrm{End}_{\mathcal{O}}(M)$ *be the endomorphism algebra of a non-projective indecomposable* $\mathcal{O}G$*-lattice* M *, and let* $L_M(G)$ *be defined as in 35.1. The following conditions on a subgroup* H *of* G *are equivalent.*

(a) M *is projective relative to* H *.*
(b) $\overline{t}_H^G : \overline{A^H} \to \overline{A^G}$ *is surjective.*
(c) $\overline{r}_H^G : \overline{\mathrm{Hom}}_{\mathcal{O}G}(M, TM) \to \overline{\mathrm{Hom}}_{\mathcal{O}H}(M, TM)$ *is injective.*
(d) $\overline{r}_H^G(L_M(G)) \neq 0$ *.*
(e) *The restriction to* H *of the almost split sequence terminating in* M *does not split.*

Proof. (a) is equivalent to the surjectivity of $t_H^G : A^H \to A^G$ (Corollary 17.3), which in turn is clearly equivalent to (b). The equivalence of (b) and (c) is an immediate consequence of the fact that $\overline{t}_H^G$ and $\overline{r}_H^G$ are adjoint with respect to the Auslander–Reiten duality (Theorems 32.12 and 33.8). Indeed we have $\mathrm{Im}(\overline{t}_H^G) = \mathrm{Ker}(\overline{r}_H^G)^{\perp}$ by Exercise 33.5. Since $\mathrm{Ker}(\overline{r}_H^G)$ and $L_M(G)$ are right $\overline{A^G}$-submodules of $\overline{\mathrm{Hom}}_{\mathcal{O}G}(M, TM)$, the equivalence of (c) and (d) follows from the fact that $L_M(G)$ is a simple right $\overline{A^G}$-submodule (Lemma 34.9) and is therefore contained in any non-zero submodule of $\overline{\mathrm{Hom}}_{\mathcal{O}G}(M, TM)$. Finally the equivalence between (d) and (e) is a consequence of the construction of the almost split sequence terminating in M , using a pull-back of a projective cover of TM along an almost projective element $u \in \mathrm{Hom}_{\mathcal{O}G}(M, TM)$ (Theorem 34.11). Indeed the restriction to H of this pull-back diagram is the following pull-back diagram.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Res}_H^G(\Omega TM) & \xrightarrow{r_H^G(j')} & \mathrm{Res}_H^G(E) & \xrightarrow{r_H^G(q')} & \mathrm{Res}_H^G(M) & \longrightarrow & 0 \\
 & & \big\downarrow{\scriptstyle id} & & \big\downarrow{\scriptstyle r_H^G(u')} & & \big\downarrow{\scriptstyle r_H^G(u)} & & \\
0 & \longrightarrow & \mathrm{Res}_H^G(\Omega TM) & \xrightarrow{r_H^G(j)} & \mathrm{Res}_H^G(P) & \xrightarrow{r_H^G(q)} & \mathrm{Res}_H^G(TM) & \longrightarrow & 0
\end{array}$$

By Lemma 34.10, the top sequence does not split if and only if $r_H^G(u)$ is not projective, that is, $\overline{r}_H^G(\overline{u}) \neq 0$. This is equivalent to (d) because the simple module $L_M(G)$ is generated by its non-zero element $\overline{u}$. □

Since the vertices of M are the minimal subgroups such that (a) holds, another way of stating Proposition 35.2 is the following. A subgroup P is a vertex of an indecomposable $\mathcal{O}G$-lattice M if and only if P is a minimal subgroup such that the restriction to P of the almost split sequence terminating in M does not split.

Our next result gives a characterization of the inclusion of non-projective pointed groups.

(35.3) PROPOSITION. *Let* $A = \mathrm{End}_{\mathcal{O}}(M)$ *be the endomorphism algebra of an* $\mathcal{O}G$*-lattice* M *and let* H *and* F *be subgroups of* G *with* $F \leq H$ *. Let* M_α *(respectively* M_β *) be a non-projective indecomposable direct summand of* $\mathrm{Res}^G_H(M)$ *(respectively* $\mathrm{Res}^G_F(M)$ *) corresponding to a non-projective point* α *of* A^H *(respectively a non-projective point* β *of* A^F *). Let* $L_M(H_\alpha)$ *and* $L_M(F_\beta)$ *be defined as in 35.1. The following conditions are equivalent.*

(a) M_β *is isomorphic to a direct summand of* $\mathrm{Res}^G_F(M_\alpha)$ *.*
(b) $F_\beta \leq H_\alpha$ *.*
(c) $L_M(H_\alpha) \subseteq \bar{t}^H_F(L_M(F_\beta))$ *.*
(d) $L_M(H_\alpha) \cap \bar{t}^H_F(L_M(F_\beta)) \neq 0$ *.*

Proof. By Example 13.4, (a) and (b) are equivalent. Now (b) is equivalent to $(r^H_F)^{-1}(\mathfrak{m}_\beta) \subseteq \mathfrak{m}_\alpha$ (Lemma 13.3), that is,

$$(\bar{r}^H_F)^{-1}(\overline{\mathfrak{m}}_\beta) \subseteq \overline{\mathfrak{m}}_\alpha \,, \tag{35.4}$$

because α and β are non-projective. Since $\bar{r}^H_F$ and $\bar{t}^H_F$ are adjoint and by Exercise 33.5, we have

$$(\bar{r}^H_F)^{-1}(\overline{\mathfrak{m}}_\beta) = \bar{t}^H_F((\overline{\mathfrak{m}}_\beta)^\perp)^\perp = \bar{t}^H_F(L_M(F_\beta))^\perp \,.$$

Therefore 35.4 is equivalent to $\bar{t}^H_F(L_M(F_\beta)) \supseteq (\overline{\mathfrak{m}}_\alpha)^\perp$, which is statement (c). In order to prove the equivalence between (c) and (d), we use the $(\overline{A^F}, \overline{A^F})$-bimodule structure of $\overline{\mathrm{Hom}}_{\mathcal{O}F}(M,TM)$ (and similarly with H instead of F). Since $L_M(F_\beta)$ is a sub-bimodule of $\overline{\mathrm{Hom}}_{\mathcal{O}F}(M,TM)$ and since the relative trace map satisfies 32.1, $\bar{t}^H_F(L_M(F_\beta))$ is a sub-bimodule of $\overline{\mathrm{Hom}}_{\mathcal{O}H}(M,TM)$. Since $L_M(H_\alpha)$ is a minimal sub-bimodule of $\overline{\mathrm{Hom}}_{\mathcal{O}H}(M,TM)$ (Exercise 35.1), it follows that (c) and (d) are equivalent. □

In general, almost split sequences are not preserved by induction (nor by restriction), but they are in the following situation.

(35.5) THEOREM. *Let* H *be a subgroup of* G *, let* N *be a non-projective indecomposable* $\mathcal{O}H$*-lattice, and assume that* N *has multiplicity one as a direct summand of* $\mathrm{Res}^G_H\,\mathrm{Ind}^G_H(N)$ *.*

(a) There is, up to isomorphism, a unique $\mathcal{O}G$*-lattice* M *such that* M *is isomorphic to a direct summand of* $\mathrm{Ind}^G_H(N)$ *and* N *is isomorphic to a direct summand of* $\mathrm{Res}^G_H(M)$ *. Moreover* M *has multiplicity one as a direct summand of* $\mathrm{Ind}^G_H(N)$ *.*

(b) *If* S_N *(respectively* S_M *) denotes the almost split sequence terminating in* N *(respectively in* M *), then* $\mathrm{Ind}_H^G(S_N) \cong S_M \oplus Z$ *, where* Z *is a split short exact sequence of* $\mathcal{O}G$*-lattices.*

(c) S_N *is isomorphic to a direct summand of* $\mathrm{Res}_H^G(S_M)$ *.*

(d) M *is, up to isomorphism, the unique* $\mathcal{O}G$*-lattice such that* N *is isomorphic to a direct summand of* $\mathrm{Res}_H^G(M)$ *.*

Proof. The proof of (a) is an easy exercise which is left to the reader (see Exercise 13.6). We first prove (c) and (d), assuming (b).

(c) It follows from the definition of induction that S_N is a direct summand of $\mathrm{Res}_H^G \mathrm{Ind}_H^G(S_N)$. Thus S_N is isomorphic to a direct summand of $\mathrm{Res}_H^G(S_M \oplus Z)$ by (b). Since S_N does not split and is an indecomposable $\mathcal{O}H$-diagram (Lemma 34.13), S_N cannot be isomorphic to a summand of the split sequence $\mathrm{Res}_H^G(Z)$. Therefore S_N is isomorphic to a direct summand of $\mathrm{Res}_H^G(S_M)$, using the Krull–Schmidt theorem, which holds in the category of diagrams by Proposition 31.5.

(d) Let L be an indecomposable $\mathcal{O}G$-lattice and assume that L is not isomorphic to M . We let E_N (respectively E_M) be the middle module of the almost split sequence terminating in N (respectively in M). By definition of an almost split sequence, the map

$$\mathrm{Hom}_{\mathcal{O}G}(L, E_M) \longrightarrow \mathrm{Hom}_{\mathcal{O}G}(L, M)$$

is surjective, because no homomorphism $L \to M$ can be a split surjection (otherwise $L \cong M$). Therefore

$$\mathrm{Hom}_{\mathcal{O}G}(L, \mathrm{Ind}_H^G(E_N)) \longrightarrow \mathrm{Hom}_{\mathcal{O}G}(L, \mathrm{Ind}_H^G(N))$$

is surjective too, because by (b) $\mathrm{Ind}_H^G(E_N) \to \mathrm{Ind}_H^G(N)$ is isomorphic to the direct sum of $E_M \to M$ and a split surjection $Y \to M'$, and $\mathrm{Hom}_{\mathcal{O}G}(L, -)$ is always exact on split surjections. By Frobenius reciprocity (Exercise 16.5), it follows that

$$\mathrm{Hom}_{\mathcal{O}H}(\mathrm{Res}_H^G(L), E_N) \longrightarrow \mathrm{Hom}_{\mathcal{O}G}(\mathrm{Res}_H^G(L), N)$$

is surjective. By definition of an almost split sequence again, N cannot be isomorphic to a direct summand of $\mathrm{Res}_H^G(L)$, otherwise there would be a split surjection $f : \mathrm{Res}_H^G(L) \to N$, and f would lift to E_N because of the above surjection; then this would force $E_N \to N$ to split. This shows that M is, up to isomorphism, the unique $\mathcal{O}G$-lattice such that N is isomorphic to a direct summand of $\mathrm{Res}_H^G(M)$.

(b) Let $X = \mathrm{Ind}_H^G(N)$ and let $A = \mathrm{End}_{\mathcal{O}}(X)$. Let β be the point of A^H corresponding to the direct summand N of $\mathrm{Res}_H^G(X)$, and let α be the point of A^G corresponding to the direct summand M of X

obtained in (a). Since β has multiplicity one, the corresponding simple quotient $S(\beta)$ of A^H is isomorphic to k if k is algebraically closed, and in general $S(\beta)$ is a division ring (a finite extension of k). Since $\mathfrak{p}A^H$ is in the kernel of $\pi_\beta : A^H \to S(\beta)$ and since $J(A^G)$ is nilpotent modulo $\mathfrak{p}$ (Theorem 2.7), $\pi_\beta r_H^G(J(A^G))$ is a nilpotent ideal of $S(\beta)$. Therefore $\pi_\beta r_H^G(J(A^G)) = 0$, that is, $r_H^G(J(A^G)) \subseteq \mathfrak{m}_\beta$. Moreover we have $r_H^G(A_1^G) \subseteq A_1^H \subseteq \mathfrak{m}_\beta$, because H_β is non-projective by assumption. Thus in the stable quotient $\overline{A^H}$, we have $\overline{r}_H^G(J(\overline{A^G})) \subseteq \overline{\mathfrak{m}}_\beta$ (because $J(\overline{A^G}) = (J(A^G) + A_1^G)/A_1^G$).

Now we consider the Auslander–Reiten duality with respect to the module X. For later use, we choose $TX = \mathrm{Ind}_H^G(TN)$. This is possible because the induction of a projective $\mathcal{O}H$-lattice is a projective $\mathcal{O}G$-lattice, from which it follows that the induction of a projective cover of N is a projective cap of $\mathrm{Ind}_H^G(N)$, and therefore $\mathrm{Ind}_H^G(\Omega N) = \Omega(\mathrm{Ind}_H^G(N)) \oplus Q$ for some projective $\mathcal{O}G$-lattice Q. In the above inclusion, we take orthogonals with respect to ϕ_X^H and ϕ_X^G, and we obtain $\overline{t}_H^G(L_X(H_\beta)) \subseteq L_X(G)$, because $\overline{t}_H^G$ is the adjoint of $\overline{r}_H^G$. Since the relative trace map satisfies 32.1, $\overline{t}_H^G(L_X(H_\beta))$ is a sub-bimodule of $L_X(G)$ and therefore, by Exercise 35.1, we have

$$\overline{t}_H^G(L_X(H_\beta)) = \bigoplus_{\alpha'} L_X(G_{\alpha'}),$$

where α' runs over some subset of $\mathcal{P}(A^G - A_1^G)$. By (a), α is the unique point of A^G such that $G_\alpha \geq H_\beta$. Therefore by Proposition 35.3, we have

$$\overline{t}_H^G(L_X(H_\beta)) \supseteq L_X(G_\alpha) \qquad \text{and} \qquad \overline{t}_H^G(L_X(H_\beta)) \cap L_X(G_{\alpha'}) = 0$$

for every $\alpha' \in \mathcal{P}(A^G - A_1^G)$ distinct from α. It follows that we have $\overline{t}_H^G(L_X(H_\beta)) = L_X(G_\alpha)$.

Let e be the projection onto N corresponding to the decomposition

$$\mathrm{Res}_H^G(X) = \mathrm{Res}_H^G \mathrm{Ind}_H^G(N) = N \bigoplus \Big(\bigoplus_{g\in[G/H],\, g\notin H} g \otimes N \Big).$$

Thus $e \in \beta$, and we identify $\overline{\mathrm{End}}_{\mathcal{O}H}(N)$ with $\overline{eA^He}$, and $\overline{\mathrm{Hom}}_{\mathcal{O}}(N, TN)$ with $\overline{e}\,\overline{\mathrm{Hom}}_{\mathcal{O}}(X, TX)\overline{e}$, as in Exercise 35.2. Since N has multiplicity one as a direct summand of $\mathrm{Res}_H^G(X)$, we have $L_N(H) \cong L_X(H_\beta)$ by Exercise 35.2. Explicitly if $\overline{u}_0$ is any non-zero element of $L_N(H)$ (a generator of the simple module $L_N(H)$), then $u_0 : N \to TN$ extends to a homomorphism $u : X \to TX$, obtained by requiring that u is zero on the other summands of the above decomposition, and then the image of u in the stable quotient is a generator of $L_X(H_\beta)$. The map $\overline{u}_0 \mapsto \overline{u}$ is the isomorphism $L_N(H) \cong L_X(H_\beta)$.

There is also the $\mathcal{O}G$-linear extension of u_0 to a homomorphism

$$id_{\mathcal{O}G} \otimes u_0 : \mathcal{O}G \otimes_{\mathcal{O}H} N = X \longrightarrow \mathcal{O}G \otimes_{\mathcal{O}H} TN = TX ,$$

using our choice $TX = \mathrm{Ind}_H^G(TN)$. We claim that $id_{\mathcal{O}G} \otimes u_0 = t_H^G(u)$. Indeed $t_H^G(u)$ coincides with u_0 on the summand $1 \otimes N = N$, because if $x \in N$, we have

$$t_H^G(u)(1 \otimes x) = \sum_{g \in [G/H]} g{\cdot}u(g^{-1} \otimes x) = u_0(1 \otimes x)$$

since u has been extended by zero on the other summands. As $id_{\mathcal{O}G} \otimes u_0$ is the unique $\mathcal{O}G$-linear extension of u_0, it follows that $id_{\mathcal{O}G} \otimes u_0 = t_H^G(u)$.

We have proved above that $\bar{t}_H^G(L_X(H_\beta)) = L_X(G_\alpha)$. Since u is an arbitrary non-zero element of $L_X(H_\beta)$, there is at least one such u for which the element $\bar{t}_H^G(\overline{u}) = \overline{id_{\mathcal{O}G} \otimes u_0}$ is a generator of the simple module $L_X(G_\alpha)$. Since M is a direct summand of X with multiplicity one, it follows again from Exercise 35.2 that $L_X(G_\alpha) \cong L_M(G)$. In other words if $v_0 : M \to TM$ is an $\mathcal{O}G$-linear map such that $\overline{v}_0$ generates $L_M(G)$, then v_0 extends to $v : X \to TX$, defined to be zero on a complementary summand M' of X (that is, $X = M \oplus M'$), and then the image of v in $\overline{\mathrm{Hom}}_{\mathcal{O}G}(X, TX)$ is a generator of $L_X(G_\alpha)$. Thus we can choose v such that $\overline{v} = \overline{id_{\mathcal{O}G} \otimes u_0}$, and therefore $v = (id_{\mathcal{O}G} \otimes u_0) + v'$, where $v' \in \mathrm{Hom}_{\mathcal{O}}(X, TX)_1^G$ is projective.

The almost split sequence $S_N = (0 \to \Omega TN \to E \to N \to 0)$ is obtained by pull-back of a projective cover of TN along u_0 (Theorem 34.11). Therefore, since the induction functor Ind_H^G is exact, $\mathrm{Ind}_H^G(S_N)$ is a short exact sequence obtained by pull-back along $\mathrm{Ind}_H^G(u_0) = id_{\mathcal{O}G} \otimes u_0$. Thus $\mathrm{Ind}_H^G(S_N)$ is the top sequence in the following diagram.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Ind}_H^G(\Omega TN) & \longrightarrow & \mathrm{Ind}_H^G(E) & \longrightarrow & X & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle id} & & \downarrow & & \downarrow{\scriptstyle id_{\mathcal{O}G} \otimes u_0} & & \\
0 & \longrightarrow & \mathrm{Ind}_H^G(\Omega TN) & \longrightarrow & \mathrm{Ind}_H^G(P) & \longrightarrow & TX & \longrightarrow & 0
\end{array}$$

Since $v = (id_{\mathcal{O}G} \otimes u_0) + v'$, where v' is projective, the top sequence is isomorphic to the sequence obtained by pull-back along v (Exercise 34.3). But $v_0 : M \to TM$ has been extended to a map $v : X \to TX$ which is zero on the other summand M'. Therefore the whole diagram decomposes as the direct sum of two diagrams D_1 and D_2: the diagram D_1 is the pull-back along v_0 of a projective cover of TM, and D_2 is the pull-back along the zero map of the complementary sequence terminating in TM', where

$TX = TM \oplus TM'$. Note that all the projective summands of $\mathrm{Ind}_H^G(\Omega TN)$ split off the bottom sequence (because they are also $\mathcal{O}$-injective by Proposition 6.7), so that they can be put in D_2 , and therefore the kernel module on the left of D_1 is the indecomposable $\mathcal{O}G$-lattice ΩTM .

Since the pull-back of any short exact sequence along the zero map yields a split sequence, the top sequence of D_2 is a split sequence Z . Since v_0 is almost projective, the top sequence of D_1 is the almost split sequence S_M terminating in M . Therefore $\mathrm{Ind}_H^G(S_N) \cong S_M \oplus Z$. □

We apply Theorem 35.5 in the situation of the Green correspondence.

(35.6) COROLLARY. *Let M be an indecomposable $\mathcal{O}G$-lattice with vertex P and source X , let $H \geq N_G(P, X)$, and let the $\mathcal{O}H$-lattice N be the Green correspondent of M . If S_N and S_M denote the almost split sequences terminating in N and M respectively, then $\mathrm{Ind}_H^G(S_N) \cong S_M \oplus Z$ where Z is a split short exact sequence of $\mathcal{O}G$-lattices. Moreover S_N is isomorphic to a direct summand of $\mathrm{Res}_H^G(S_M)$.*

Proof. Proposition 20.7 asserts precisely that the assumption of Theorem 35.5 is satisfied. □

Exercises

(35.1) Let M be an $\mathcal{O}G$-lattice, let TM be defined as in 34.5, let H be a subgroup of G, let $L_M(H) = \mathrm{Soc}(\overline{\mathrm{Hom}}_{\mathcal{O}H}(M, TM))$, and let $A = \mathrm{End}_{\mathcal{O}}(M)$.

(a) For every non-projective point $\alpha \in \mathcal{P}(A^H)$, let $L_M(H_\alpha)$ be defined as in 35.1. Prove that $L_M(H_\alpha)$ is a minimal sub-bimodule of $\overline{\mathrm{Hom}}_{\mathcal{O}H}(M, TM)$. [Hint: $\overline{\mathfrak{m}}_\alpha$ is a maximal ideal of $\overline{A^H}$ and the form ϕ_M^H satisfies 34.8.]

(b) Prove that any sub-bimodule of $L_M(H)$ is equal to $\oplus_\alpha L_M(H_\alpha)$, where α runs over some subset of the set $\mathcal{P}(A^H - A_1^H)$ of all non-projective points of A^H . [Hint: Any two-sided ideal of the semi-simple algebra $\overline{A^H}/J(\overline{A^H})$ is isomorphic to a product of some of the simple factors. Thus any two-sided ideal of $\overline{A^H}$ containing $J(\overline{A^H})$ is the intersection of some of the maximal ideals $\overline{\mathfrak{m}}_\alpha$. Use duality and the fact that any submodule is equal to its double orthogonal (Exercise 33.5).]

(35.2) Let M be an $\mathcal{O}G$-lattice, let $A = \mathrm{End}_{\mathcal{O}}(M)$, and let e be an idempotent of A^G, so that $N = eM$ is a direct summand of M with endomorphism algebra $\mathrm{End}_{\mathcal{O}}(N) \cong eAe$.

(a) Let $N' = (1-e)M$. Prove that $TM = TN \oplus TN'$ (for suitable choices of TN and TN'). If e' denotes the idempotent projector onto TN in $\mathrm{End}_{\mathcal{O}G}(TM)$, prove that $\overline{e}' \in \overline{\mathrm{End}}_{\mathcal{O}G}(TM)$ is the image of $\overline{e} \in \overline{A^G}$ under the isomorphism $\overline{A^G} \cong \overline{\mathrm{End}}_{\mathcal{O}G}(TM)$ (see 34.7).

(b) Deduce from (a) and the definition of the bimodule structure that

$$\overline{\mathrm{Hom}}_{\mathcal{O}G}(N, TN) \cong \overline{e}\, \overline{\mathrm{Hom}}_{\mathcal{O}G}(M, TM)\, \overline{e}\,.$$

(c) The Auslander–Reiten duality ϕ_M^G for M restricts, via the isomorphism of (b) and the isomorphism $\overline{\mathrm{End}}_{\mathcal{O}G}(N) \cong \overline{eA^Ge}$, to a bilinear form

$$\psi : \overline{\mathrm{Hom}}_{\mathcal{O}G}(N, TN) \times \overline{\mathrm{End}}_{\mathcal{O}G}(N) \longrightarrow \overline{\mathcal{O}}\,.$$

Prove that ψ is equal to the Auslander–Reiten duality ϕ_N^G for N. [Hint: Go back to the definition of the bilinear forms, and decompose everything according to the direct sum $M = N \oplus N'$.]

(d) Using the previous isomorphisms, prove that $L_N(G)$ can be identified with $\overline{e}L_M(G)\overline{e}$.

(e) Suppose that N is indecomposable (that is, e is primitive in A^G) and that N has multiplicity one as a direct summand of M. Let α be the point of A^G containing e. Using the identification of (d), prove that $L_N(G) = L_M(G_\alpha)$. [Hint: Show that $\mathfrak{m}_\alpha = J(A^G) + (1-e)A^G$, $((1-\overline{e})\overline{A^G})^\perp = \overline{\mathrm{Hom}}_{\mathcal{O}G}(M, TM)\,\overline{e}$, and $L_M(G_\alpha) = L_M(G)\overline{e}$. Show similarly that $L_M(G_\alpha) = \overline{e}\,L_M(G)$, so that $L_M(G_\alpha) = \overline{e}\,L_M(G)\,\overline{e}$.]

(35.3) Let M be a non-projective indecomposable $\mathcal{O}G$-lattice, let S_M be the almost split sequence terminating in M, let H be a subgroup of G, and let $A = \mathrm{End}_{\mathcal{O}}(M)$. Prove that the following conditions are equivalent.

(a) $\mathrm{Res}_H^G(S_M)$ is a direct sum of split and almost split sequences.

(b) $\overline{r}_H^G(L_M(G)) \subseteq L_M(H)$.

(c) $\overline{t}_H^G(J(\overline{A^H})) \subseteq J(\overline{A^G})$.

(d) $t_H^G(J(A^H)) \subseteq J(A^G)$.

[Hint: For the equivalence of (a) and (b), use Exercise 34.4. For the equivalence of (b) and (c), use the fact that $\overline{r}_H^G$ and $\overline{t}_H^G$ are adjoint and apply Exercise 33.5.]

(35.4) Let H be a subgroup of G, let N be a non-projective indecomposable $\mathcal{O}H$-lattice, and let S_N be the almost split sequence terminating in N. Let $M = \mathrm{Ind}_H^G(N)$, let $A = \mathrm{End}_{\mathcal{O}}(M)$, and let $e \in A^H$ be the projection onto the direct summand N of $\mathrm{Res}_H^G(M)$, so that $eAe \cong \mathrm{End}_{\mathcal{O}}(N)$ and $eL_M(H)e \cong L_N(H)$ (Exercise 35.2). Prove that the following conditions are equivalent.

(a) $\mathrm{Ind}_H^G(S_N)$ is a direct sum of split and almost split sequences.
(b) $\bar{t}_H^G(eL_M(H)e) \subseteq L_M(G)$.
(c) $\bar{e}\,\bar{r}_H^G(J(\overline{A^G}))\,\bar{e} \subseteq J(\overline{eA^He})$.
(d) $e\,r_H^G(J(A^G))\,e \subseteq J(eA^He)$.

[Hint: Show that the maps $\overline{A^G} \xrightarrow{\bar{r}_H^G} \overline{A^H} \xrightarrow{q} \overline{eA^He}$ and

$$\bar{e}\,\overline{\mathrm{Hom}}_{\mathcal{O}H}(M,TM)\,\bar{e} \xrightarrow{j} \overline{\mathrm{Hom}}_{\mathcal{O}H}(M,TM) \xrightarrow{\bar{t}_H^G} \overline{\mathrm{Hom}}_{\mathcal{O}G}(M,TM)$$

are adjoint, where j denotes the inclusion and q denotes the projection (that is, multiplication by $\bar{e}$ on both sides). Then proceed as in Exercise 35.3.]

Notes on Section 35

The question of the behaviour of almost split sequences under restriction and induction has been considered by a number of authors. In particular Benson and Parker [1984] proved Corollary 35.6, Green [1985] proved Theorem 35.5 over a field, and Thévenaz [1988a] extended Green's result to the case of a complete discrete valuation ring. The general techniques of Exercises 35.3 and 35.4 appear in Green [1985] over a field and in Thévenaz [1988a] over a complete discrete valuation ring. Finally a result of Thévenaz [1988b] asserts in general that the restriction (respectively induction) of an almost split sequence is a direct sum of split and almost split sequences if and only if some simple criterion involving the restriction (respectively induction) of a defect multiplicity module is satisfied.

§ 36 DEFECT GROUPS OF ALMOST SPLIT SEQUENCES

We continue with our assumption that $\mathcal{O}$ is either a field or a complete discrete valuation ring of characteristic zero (satisfying Assumption 33.1). As we are going to use multiplicity modules, we return to our usual assumption that the residue field k of $\mathcal{O}$ is algebraically closed. The purpose of this section is to determine a defect group of an arbitrary almost split sequence.

Let M be a non-projective indecomposable $\mathcal{O}G$-lattice. Let P_γ be a defect of the primitive G-algebra $A = \mathrm{End}_{\mathcal{O}}(M)$, so that P is a vertex of M and iM is a source of M for any $i \in \gamma$. Recall that the defect multiplicity module $V(\gamma)$ is an indecomposable projective $k_\sharp\widehat{\overline{N}}_G(P_\gamma)$-module (Theorem 19.2). The radical of $V(\gamma)$ is the submodule

$$J(V(\gamma)) = J(k_\sharp\widehat{\overline{N}}_G(P_\gamma))\cdot V(\gamma)\,,$$

and by the bijection between indecomposable projective modules and simple modules (Proposition 5.1), the quotient $T(\gamma) = V(\gamma)/J(V(\gamma))$ is a simple $k_\sharp\widehat{\overline{N}}_G(P_\gamma)$-module.

Let S_M be the almost split sequence terminating in M, viewed as an indecomposable $\mathcal{O}G$-diagram (Lemma 34.13). The purpose of this section is to show that a defect group of S_M is determined by a vertex of the module $T(\gamma)$, that is, a defect group of the primitive $\overline{N}_G(P_\gamma)$-algebra $\mathrm{End}_k(T(\gamma))$.

(36.1) THEOREM. *Let M be a non-projective indecomposable $\mathcal{O}G$-lattice, let P_γ be a defect of the primitive G-algebra $A = \mathrm{End}_{\mathcal{O}}(M)$, let $V(\gamma)$ be the corresponding multiplicity module, let $T(\gamma) = V(\gamma)/J(V(\gamma))$ be the corresponding simple $k_\sharp\widehat{\overline{N}}_G(P_\gamma)$-module, and let $\overline{Q}$ be a vertex of $T(\gamma)$. If Q is the inverse image of $\overline{Q}$ in $N_G(P_\gamma)$, then Q is a defect group of the almost split sequence S_M terminating in M.*

The notation of the statement will be in force throughout this section. We first reduce the proof of the theorem to the subgroup $N_G(P_\gamma)$.

(36.2) LEMMA. *Let $N = N_G(P_\gamma)$, let the $\mathcal{O}N$-lattice L be the Green correspondent of M, and let S_L be the almost split sequence terminating in L. Then a defect group of S_L is a defect group of S_M.*

Proof. Let $B = \mathrm{End}_{\mathcal{O}}(S_M)$ be the primitive G-algebra corresponding to S_M. By Corollary 35.6, S_L is isomorphic to a direct summand of $\mathrm{Res}^G_N(S_M)$ and S_M is isomorphic to a direct summand of $\mathrm{Ind}^G_N(S_L)$. Let $\alpha = \{1_B\}$ be the unique point of B^G and let $\beta \in \mathcal{P}(B^N)$ be the point corresponding to the summand S_L. Then $G_\alpha \geq N_\beta$ and, by Theorem 17.9, we also have $G_\alpha \, pr \, N_\beta$, because the fact that S_M is isomorphic to a direct summand of $\mathrm{Ind}^G_N(S_L)$ is equivalent to the existence of an embedding $B \to \mathrm{Ind}^G_N(B_\beta)$ satisfying the conditions of Theorem 17.9.

Let Q_δ be a defect of N_β, so that Q is a defect group of S_L. Then Q_δ is local, $G_\alpha \geq N_\beta \geq Q_\delta$, and $G_\alpha \, pr \, N_\beta \, pr \, Q_\delta$. This proves that Q_δ is a defect of G_α. In particular Q is a defect group of S_M. □

Recall that the Green correspondence has been constructed as the composite of the Puig correspondence for the group G and the inverse of the Puig correspondence for the group $N = N_G(P_\gamma)$. Since the Puig correspondent of M is the defect multiplicity module $V(\gamma)$ of M, it follows that $V(\gamma)$ is also the defect multiplicity module of L. In particular the simple $k_\sharp \widehat{\overline{N}}_G(P_\gamma)$-module $T(\gamma)$ is the same for both M and L, and therefore it suffices to prove Theorem 36.1 for the group $N = N_G(P_\gamma)$.

We assume from now on that G stabilizes P_γ, so that $G = N_G(P_\gamma)$. In particular we write $\overline{G} = G/P$. We immediately note the following consequence of this assumption.

(36.3) LEMMA. *Assume that $G = N_G(P_\gamma)$. Then γ is the only point of A^P.*

Proof. Since A is primitive and P_γ is a defect of A, we have $t^G_P(A^P\gamma A^P) = A^G$. Since A^P and γ are invariant under conjugation by G by assumption, we have

$$1_A \in t^G_P(A^P\gamma A^P) = \sum_{g\in[G/P]} {}^g(A^P)\, {}^g\gamma\, {}^g(A^P) = A^P\gamma A^P .$$

It follows that $A^P = A^P\gamma A^P$, so that, by Lemma 4.13, γ is the only point of A^P. □

By construction, the almost split sequence S_M terminating in M is the pull-back along u of a projective cover of TM, where $u : M \to TM$ is almost projective. Recall that TM is only defined up to addition of a projective $\mathcal{O}G$-lattice. We make here a choice of TM having the following properties.

(36.4) LEMMA. *For a suitable choice of TM, there exists an almost projective map $u : M \to TM$ with the following two properties.*

(a) u has an $\mathcal{O}$-linear retraction $r : TM \to M$.

(b) u is indecomposable (viewed as an $\mathcal{O}G$-diagram with two vertices and one arrow).

Proof. Let $u : M \to TM$ be an arbitrary almost projective map. Let $i : M \to J$ be an $\mathcal{O}$-injective hull of M (with cokernel $\Omega^{-1}M$). Since $\mathcal{O}G$ is a symmetric algebra, the $\mathcal{O}G$-lattice J is also projective (Proposition 6.7) and so i is a projective map. Therefore the homomorphism $u \oplus i : M \to TM \oplus J$ has the same image as u in the stable quotient

$$\overline{\mathrm{Hom}}_{\mathcal{O}G}(M, TM) \cong \overline{\mathrm{Hom}}_{\mathcal{O}G}(M, TM \oplus J)$$

(see Lemma 32.3). Thus $u \oplus i$ is again almost projective and moreover $u \oplus i$ has an $\mathcal{O}$-linear retraction. Indeed i has an $\mathcal{O}$-linear retraction h (because the sequence of $\mathcal{O}G$-lattices $0 \to M \overset{i}{\to} J \to \Omega^{-1}M \to 0$ splits over $\mathcal{O}$), and the composition $TM \oplus J \overset{q}{\to} J \overset{h}{\to} M$ is a retraction of $u \oplus i$ (where q denotes the second projection).

Changing notation, we assume now that the almost projective map $u : M \to TM$ has an $\mathcal{O}$-linear retraction r, and we assume also that $\dim_{\mathcal{O}}(TM)$ is minimal with this property. We claim that u is then indecomposable as an $\mathcal{O}G$-diagram. Indeed since M is indecomposable, the only possible decomposition of u has the form

$$(M \overset{u}{\longrightarrow} TM) \cong (M \overset{u'}{\longrightarrow} X) \oplus (0 \longrightarrow Y),$$

where $X \oplus Y = TM$, and u is the composite of u' and the inclusion $X \to TM$. Now by definition $TM \cong M' \oplus R$, where R is projective and where M' is an indecomposable module isomorphic to either M or ΩM. Since u is not a projective map (by definition of almost projectivity), X cannot be a projective module. Therefore, by the Krull–Schmidt theorem, $X \cong M' \oplus R'$ for some projective module R', that is, X is again a module of the form TM. Thus $u' : M \to X$ is almost projective and has an $\mathcal{O}$-linear retraction (namely the restriction of r to X). By minimality of $\dim_{\mathcal{O}}(TM)$, we deduce that $Y = 0$, proving the indecomposability of u. □

The existence of a retraction of u amounts to the injectivity of u when $\mathcal{O} = k$, but is stronger than injectivity when $\mathcal{O}$ is a discrete valuation ring. This property will be crucial in the sequel. However, the indecomposability of u is only a convenient property, which allows us to work with primitive G-algebras (otherwise one would have to consider non-primitive G-algebras having additional projective points).

From now on we assume that u has the two properties of Lemma 36.4 and we write U for the $\mathcal{O}G$-diagram $u : M \to TM$. We use covering homomorphisms to establish a connection between U and the indecomposable $\mathcal{O}G$-diagram S_M. We know that S_M is obtained by pull-back along u of a projective cover $q : PTM \to TM$ (Theorem 34.11). Let D denote the whole pull-back diagram, as follows.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \Omega TM & \xrightarrow{j} & E & \xrightarrow{q} & M & \longrightarrow & 0 \\
 & & \big\downarrow{\scriptstyle id} & & \big\downarrow{\scriptstyle v} & & \big\downarrow{\scriptstyle u} & & \\
0 & \longrightarrow & \Omega TM & \xrightarrow{j'} & PTM & \xrightarrow{q'} & TM & \longrightarrow & 0
\end{array}$$

Any $\mathcal{O}$-linear endomorphism of this diagram can be restricted to the top sequence and this defines a map $f_1 : \mathrm{End}_{\mathcal{O}}(D) \to \mathrm{End}_{\mathcal{O}}(S_M)$. Similarly there is a restriction map $f_2 : \mathrm{End}_{\mathcal{O}}(D) \to \mathrm{End}_{\mathcal{O}}(U)$ to the right hand side vertical map.

(36.5) LEMMA. *Let D be the pull-back diagram above.*
(a) D is an indecomposable $\mathcal{O}G$-diagram.
(b) The restriction map $f_1 : \mathrm{End}_{\mathcal{O}}(D) \to \mathrm{End}_{\mathcal{O}}(S_M)$ is a covering homomorphism of G-algebras.
(c) The restriction map $f_2 : \mathrm{End}_{\mathcal{O}}(D) \to \mathrm{End}_{\mathcal{O}}(U)$ is a covering homomorphism of G-algebras.

Proof. (a) By Lemma 34.13 and Lemma 36.4, we know that both S_M and U are indecomposable $\mathcal{O}G$-diagrams. Therefore, in a direct sum decomposition of D, one summand D' must contain the whole of S_M, hence the whole of U, so that both ends of the bottom sequence are entirely contained in D'. Since a direct summand of a short exact sequence is again a short exact sequence (Exercise 31.6), the whole bottom sequence must also be contained in D', proving that $D' = D$.

(b) We shall show that the map $(f_1)^H : \mathrm{End}_{\mathcal{O}H}(D) \to \mathrm{End}_{\mathcal{O}H}(S_M)$ is surjective for any subgroup H of G. Let $(a, b, c) \in \mathrm{End}_{\mathcal{O}H}(S_M)$, where $a \in \mathrm{End}_{\mathcal{O}H}(\Omega TM)$, $b \in \mathrm{End}_{\mathcal{O}H}(E)$, and $c \in \mathrm{End}_{\mathcal{O}H}(M)$. Since u has an $\mathcal{O}$-linear retraction r, so does v. Indeed the top and bottom sequence in D split over $\mathcal{O}$ and the direct sum $id_{\Omega TM} \oplus r$ yields a retraction r'

of v. On restriction to H, the module PTM is $\mathcal{O}$-injective (because $\mathcal{O}$-injectivity is equivalent to projectivity by Proposition 6.7 and projective modules remain projective on restriction to subgroups). The $\mathcal{O}H$-linear map $vb : E \to PTM$ has an $\mathcal{O}$-linear extension $PTM \to PTM$, namely the map vbr'. Therefore, by the definition of $\mathcal{O}$-injective $\mathcal{O}H$-lattices, there exists an endomorphism b' of PTM such that $vb = b'v$.

Some elementary diagram chasing shows that b' restricts to the endomorphism a of ΩTM (that is, $b'j' = j'a$). This implies that b' induces an endomorphism c' of TM such that $q'b' = c'q'$. Finally $c'u = uc$, because

$$c'uq = c'q'v = q'b'v = q'vb = uqb = ucq\,,$$

and q can be cancelled since it is surjective. Therefore (a, b, c, a, b', c') is an $\mathcal{O}H$-linear endomorphism of D, proving the surjectivity of $(f_1)^H$.

(c) We shall show that the map $(f_2)^H : \mathrm{End}_{\mathcal{O}H}(D) \to \mathrm{End}_{\mathcal{O}H}(U)$ is surjective for any subgroup H of G. Let $(c, c') \in \mathrm{End}_{\mathcal{O}H}(U)$, where $c \in \mathrm{End}_{\mathcal{O}H}(M)$ and $c' \in \mathrm{End}_{\mathcal{O}H}(TM)$. Since $\mathrm{Res}^G_H(PTM)$ is projective, c' can be lifted to an $\mathcal{O}H$-linear endomorphism b' of PTM such that $q'b' = c'q'$. Now b' induces by restriction an endomorphism a of ΩTM such that $j'a = b'j'$. Since D is a pull-back diagram, the pair of endomorphisms $(b', c) \in \mathrm{End}_{\mathcal{O}H}(PTM) \times \mathrm{End}_{\mathcal{O}H}(M)$ induces a unique endomorphism $b \in \mathrm{End}_{\mathcal{O}H}(E)$ of the pull-back. Explicitly the two maps $b'v : E \to PTM$ and $cq : E \to M$ satisfy $q'(b'v) = u(cq)$ (because $q'b'v = c'q'v = c'uq = ucq$), and therefore there exists a unique map $b : E \to E$ such that $vb = b'v$ and $qb = cq$. On restriction to ΩTM, it is easy to see that b induces the endomorphism a (that is, $bj = ja$). This completes the proof that (a, b, c, a, b', c') is an $\mathcal{O}H$-linear endomorphism of D, establishing the surjectivity of $(f_2)^H$. □

(36.6) COROLLARY. *Let Q be a p-subgroup of G. Then Q is a defect group of S_M if and only if Q is a defect group of U.*

Proof. By Proposition 25.6, defect groups (and more precisely defect pointed groups) are preserved by covering homomorphisms. Explicitly, by the indecomposability of U, D, and S_M, the algebra $\mathrm{End}_{\mathcal{O}G}(U)$ has a unique point $\alpha = \{id_U\}$, and similarly with $\alpha^* = \{id_D\}$ and $\alpha' = \{id_{S_M}\}$. Then G_α lifts to G_{α^*} by the covering homomorphism f_2, and if Q_γ is a defect of G_α, then Q_γ lifts to a defect Q_{γ^*} of G_{α^*}. Similarly, by the covering homomorphism f_1, $G_{\alpha'}$ lifts to G_{α^*}, and if $R_{\delta'}$ is a defect of $G_{\alpha'}$, then $R_{\delta'}$ lifts to a defect R_{δ^*} of G_{α^*}. Since all defects of G_{α^*} are G-conjugate, $R_{\delta^*} = {}^g(Q_{\gamma^*})$ for some $g \in G$. In particular $R = {}^gQ$. The result follows since a conjugate of a defect group is again a defect group. □

The last three results 36.4, 36.5, and 36.6 did not use our assumption that $G = N_G(P_\gamma)$. We use it now in an essential way. A defect group of U is a defect group of the G-algebra $\mathrm{End}_{\mathcal{O}}(U)$. But since P is normal in G, we can also consider the $\overline{G}$-algebra $\mathrm{End}_{\mathcal{O}P}(U)$, which is still primitive since we have $\mathrm{End}_{\mathcal{O}P}(U)^{\overline{G}} = \mathrm{End}_{\mathcal{O}G}(U)$.

(36.7) LEMMA. *Let the subgroup* $\overline{Q}$ *of* $\overline{G}$ *be a defect group of the primitive* $\overline{G}$*-algebra* $\mathrm{End}_{\mathcal{O}P}(U)$. *Then the inverse image* Q *of* $\overline{Q}$ *in* G *is a defect group of* U.

Proof. Since M is an indecomposable $\mathcal{O}G$-lattice appearing at a vertex of the diagram U, a defect group R of U contains a defect group of M (Exercise 31.5). Thus $R \geq P$ since P is the only defect group of M (because P is a normal subgroup). Now R is a minimal subgroup such that t_R^G is surjective. But for any subgroup $X \geq P$, the relative trace map

$$t_{\overline{X}}^{\overline{G}} : \mathrm{End}_{\mathcal{O}P}(U)^{\overline{X}} = \mathrm{End}_{\mathcal{O}X}(U) \longrightarrow \mathrm{End}_{\mathcal{O}P}(U)^{\overline{G}} = \mathrm{End}_{\mathcal{O}G}(U)$$

coincides with the relative trace map t_X^G. Therefore the surjectivity of $t_{\overline{X}}^{\overline{G}}$ is equivalent to the surjectivity of t_X^G. The result follows. □

From now on we work with the $\overline{G}$-algebra $\mathrm{End}_{\mathcal{O}P}(U)$. Our aim is to establish a connection between this algebra and the defect multiplicity module $V(\gamma)$. To this end, we first need some more information on the almost projective element u and the duality.

Recall that, for every subgroup H of G, we have defined the stable quotient $\overline{A^H} = A^H/A_1^H$ and the socle $L_M(H) = \mathrm{Soc}(\overline{\mathrm{Hom}}_{\mathcal{O}H}(M, TM))$. Note that since A is primitive and non-projective (and since k is algebraically closed), we have

$$\overline{A^G}/J(\overline{A^G}) \cong A^G/J(A^G) \cong k\,,$$

and therefore $L_M(G)$ is isomorphic to k, because by construction it is in duality with $\overline{A^G}/J(\overline{A^G})$. Similarly $L_M(P)$ is in duality with

$$\overline{A^P}/J(\overline{A^P}) \cong A^P/J(A^P) = A^P/\mathfrak{m}_\gamma = S(\gamma)\,,$$

because γ is the only point of A^P (Lemma 36.3). The first isomorphism follows from the fact that $P \neq 1$ (because A is non-projective) and the unique point γ is local (because it is a source point), so that $A_1^P \subseteq \mathfrak{m}_\gamma$. We show that almost projective elements remain almost projective on restriction to P.

(36.8) LEMMA. $\overline{r}_P^G(L_M(G)) \subseteq L_M(P)$.

Proof. Since γ is the only point of A^P , we have $A^P = A^P\gamma A^P$ and $J(A^P) = \mathfrak{m}_\gamma = \mathfrak{m}_\gamma \cap A^P\gamma A^P$. By Proposition 14.7, it follows that

$$\pi_\gamma\, r_P^G\, t_P^G(\mathfrak{m}_\gamma) = t_1^{\overline{G}}\, \pi_\gamma(\mathfrak{m}_\gamma) = \{0\}\,,$$

so that $t_P^G(\mathfrak{m}_\gamma) \subseteq \mathrm{Ker}(\pi_\gamma\, r_P^G)$. But this ideal does not contain 1_A and so is contained in $J(A^G)$, because $J(A^G)$ is the unique maximal ideal of A^G . Therefore $t_P^G(J(A^P)) \subseteq J(A^G)$ and $\overline{t}_P^G(J(\overline{A^P})) \subseteq J(\overline{A^G})$. The result now follows from Exercise 35.3 but we give the explicit argument. The maps $\overline{r}_P^G$ and $\overline{t}_P^G$ are adjoint (with respect to the Auslander–Reiten duality) and by Exercise 33.5 we have

$$L_M(G) = J(\overline{A^G})^\perp \subseteq \overline{t}_P^G(J(\overline{A^P}))^\perp = \overline{t}_P^G(L_M(P)^\perp)^\perp = (\overline{r}_P^G)^{-1}(L_M(P))\,.$$

Therefore $\overline{r}_P^G(L_M(G)) \subseteq L_M(P)$. □

Our next step is to describe an isomorphism of bimodules between $L_M(P)$ and $S(\gamma)$. We have observed above that they are in duality and we first make this explicit. Since we have $\overline{A^P}/J(\overline{A^P}) \cong S(\gamma)$ and $L_M(P) = J(\overline{A^P})^\perp$, the Auslander–Reiten duality induces a non-degenerate bilinear form

$$\phi_M^P : L_M(P) \times S(\gamma) \longrightarrow \overline{\mathcal{O}}\,.$$

We want this form to have values in k instead of $\overline{\mathcal{O}}$. There is no problem if $\mathcal{O} = k$ because in that case $\overline{\mathcal{O}} = k$ too.

Assume that $\mathcal{O}$ is a discrete valuation ring and let π be a generator of the maximal ideal $\mathfrak{p}$ of $\mathcal{O}$. Then $\overline{\mathcal{O}} = \mathcal{O}/|G|\mathcal{O} = \mathcal{O}/\pi^r\mathcal{O}$ for some r . Note that, since M is non-projective, we have implicitly assumed that p divides $|G|$ (otherwise every $\mathcal{O}G$-lattice is projective by Theorem 17.5), so that $\overline{\mathcal{O}} \neq \{0\}$ and $r \geq 1$. Now both $S(\gamma)$ and $L_M(P)$ are annihilated by π (because $\pi{\cdot}1_A \in J(A^P)$) and are therefore $\overline{\mathcal{O}}$-modules annihilated by $\overline{\pi}$. Thus the form ϕ_M^P takes values in the annihilator of $\overline{\pi}$, that is, the ideal $\overline{\pi}^{r-1}\overline{\mathcal{O}}$ (because every ideal of $\overline{\mathcal{O}}$ has the form $\overline{\pi}^j\overline{\mathcal{O}}$ for some j , and $j = r-1$ is the only possibility for the annihilator of $\overline{\pi}$).

Now multiplication by $\overline{\pi}^{r-1}$ induces an isomorphism

$$\theta : \overline{\mathcal{O}}/\overline{\pi}\overline{\mathcal{O}} = k \xrightarrow{\sim} \overline{\pi}^{r-1}\overline{\mathcal{O}}\,,$$

and therefore the composition of the bilinear form ϕ_M^P with the inverse isomorphism θ^{-1} yields a non-degenerate bilinear form between two k-vector spaces

$$\psi_M^P : L_M(P) \times S(\gamma) \longrightarrow k\,, \qquad \psi_M^P(x,y) = \theta^{-1}(\phi_M^P(x,y))\,.$$

We also use this notation in case $\mathcal{O} = k$, using the convention that $\pi^{r-1} = 1_k$, so that $\theta = id$.

Since $S(\gamma)$ is a symmetric algebra and the trace form is a symmetrizing form, $S(\gamma)^*$ is isomorphic to $S(\gamma)$ by means of the trace form. Composing this isomorphism with the isomorphism $L_M(P) \cong S(\gamma)^*$ corresponding to the form ψ_M^P, we obtain an isomorphism of k-vector spaces $\sigma : L_M(P) \xrightarrow{\sim} S(\gamma)$ having the following properties.

(36.9) LEMMA. *There is an isomorphism $\sigma : L_M(P) \xrightarrow{\sim} S(\gamma)$ induced by the Auslander–Reiten duality ϕ_M^P, the isomorphism $\theta^{-1} : \pi^{r-1}\overline{\mathcal{O}} \xrightarrow{\sim} k$, and the isomorphism $S(\gamma) \cong S(\gamma)^*$ given by the trace form. Moreover σ is an isomorphism of $(\overline{A^P}, \overline{A^P})$-bimodules.*

Proof. The existence of σ follows from the above discussion. Explicitly, if $x \in L_M(P)$, then the k-linear form $\psi_M^P(x, -)$ on $S(\gamma)$ must be equal to $y \mapsto \mathrm{tr}(\sigma(x)y)$ for a uniquely determined $\sigma(x) \in S(\gamma)$. Thus σ is characterized by the property

$$\theta^{-1}(\phi_M^P(x,y)) = \psi_M^P(x,y) = \mathrm{tr}(\sigma(x)y)\,, \qquad x \in L_M(P)\,,\ y \in S(\gamma)\,.$$

To show that σ is an isomorphism of bimodules, we let $\overline{a}, \overline{b} \in \overline{A^P}$. By 34.8, we have

$$\begin{aligned}\mathrm{tr}(\sigma(\overline{a}{\cdot}x{\cdot}\overline{b})y) &= \theta^{-1}(\phi_M^P(\overline{a}{\cdot}x{\cdot}\overline{b}, y)) = \theta^{-1}(\phi_M^P(x, \overline{b}{\cdot}y{\cdot}\overline{a})) \\ &= \mathrm{tr}(\sigma(x){\cdot}\overline{b}{\cdot}y{\cdot}\overline{a}) = \mathrm{tr}((\overline{a}{\cdot}\sigma(x){\cdot}\overline{b})y)\end{aligned}$$

for all $x \in L_M(P)$ and $y \in S(\gamma)$. It follows from the non-degeneracy of tr that $\sigma(\overline{a}{\cdot}x{\cdot}\overline{b}) = \overline{a}{\cdot}\sigma(x){\cdot}\overline{b}$, as required. □

By Lemma 36.8, the almost projective element $\overline{u} \in L_M(G)$ restricts to an almost projective element $\overline{r}_P^G(\overline{u}) \in L_M(P)$. Its image in $S(\gamma)$ via the isomorphism σ has a direct characterization, given in the following crucial result. This result is the key which allows us to make the connection between u and the defect multiplicity algebra $S(\gamma)$. Recall that we have assumed that $G = N_G(P_\gamma)$, so that $S(\gamma)$ is a $\overline{G}$-algebra and $V(\gamma)$ is a $k_\sharp\widehat{\overline{G}}$-module (which is indecomposable and projective).

(36.10) PROPOSITION. *Let $w = \sigma(\overline{r}_P^G(\overline{u})) \in S(\gamma)$.*

(a) $w \in \mathrm{Soc}(S(\gamma)^{\overline{G}})$ and $w \neq 0$.

(b) When w is viewed as an endomorphism of the $k_\sharp\widehat{\overline{G}}$-module $V(\gamma)$, we have $\mathrm{Ker}(w) = J(V(\gamma))$ and $\mathrm{Im}(w) = \mathrm{Soc}(V(\gamma))$.

Proof. (a) We are going to compute the orthogonal of $\sigma(\overline{r}_P^G(\overline{u}))$ with respect to the form tr on $S(\gamma)$. For every $a \in A^P$, we let $\overline{a}$ be its image in $\overline{A^P}$, so that $\pi_\gamma(a)$ is the image of $\overline{a}$ in $\overline{A^P}/J(\overline{A^P}) \cong S(\gamma)$ (Lemma 36.3). Since $\overline{r}_P^G$ and $\overline{t}_P^G$ are adjoint with respect to the Auslander–Reiten duality, we have

$$\begin{aligned}\operatorname{tr}(\sigma(\overline{r}_P^G(\overline{u}))\,\pi_\gamma(a)) &= \psi_M^P(\overline{r}_P^G(\overline{u}), \pi_\gamma(a)) = \theta^{-1}(\phi_M^P(\overline{r}_P^G(\overline{u}), \overline{a})) \\ &= \theta^{-1}(\phi_M^G(\overline{u}, \overline{t}_P^G(\overline{a})))\end{aligned}$$

for every $a \in A^P$. Therefore $\pi_\gamma(a) \in (\sigma(\overline{r}_P^G(\overline{u})))^\perp$ (with respect to tr) if and only if $\overline{t}_P^G(\overline{a}) \in (\overline{u})^\perp$ (with respect to ϕ_M^G). Since $\overline{u}$ is a generator of $L_M(G) = J(\overline{A^G})^\perp$, this condition is equivalent to $\overline{t}_P^G(\overline{a}) \in J(\overline{A^G})$, that is, $t_P^G(a) \in J(A^G)$ (because $A_1^G \subseteq J(A^G)$ as A is non-projective). By Theorem 19.2, the homomorphism

$$\pi_\gamma\, r_P^G : A^G \longrightarrow S(\gamma)^{\overline{G}}$$

is surjective and $J(A^G)$ is the inverse image of $J(S(\gamma)^{\overline{G}})$ (because the ideal $\operatorname{Ker}(\pi_\gamma r_P^G)$ is contained in $J(A^G)$ as it does not contain 1_A). Thus $t_P^G(a) \in J(A^G)$ if and only if $\pi_\gamma r_P^G\, t_P^G(a) \in J(S(\gamma)^{\overline{G}})$. But $a \in A^P$ and $A^P = A^P\gamma A^P$ (because γ is the only point of A^P by Lemma 36.3), and therefore $\pi_\gamma r_P^G\, t_P^G(a) = t_1^{\overline{G}}\pi_\gamma(a)$ by Proposition 14.7. It follows from this discussion that $\pi_\gamma(a) \in (\sigma(\overline{r}_P^G(\overline{u})))^\perp$ if and only if $t_1^{\overline{G}}\pi_\gamma(a) \in J(S(\gamma)^{\overline{G}})$, or in other words $\pi_\gamma(a) \in (t_1^{\overline{G}})^{-1}(J(S(\gamma)^{\overline{G}}))$. Since $S(\gamma) = \operatorname{End}_k(V(\gamma))$ is the endomorphism algebra of a projective $k_\sharp\widehat{\overline{G}}$-module, Corollary 32.11 applies and asserts that

$$(t_1^{\overline{G}})^{-1}(J(S(\gamma)^{\overline{G}})) = \operatorname{Soc}(S(\gamma)^{\overline{G}})^\perp .$$

Therefore $(\sigma(\overline{r}_P^G(\overline{u})))^\perp = \operatorname{Soc}(S(\gamma)^{\overline{G}})^\perp$, so that $w = \sigma(\overline{r}_P^G(\overline{u}))$ is a generator of $\operatorname{Soc}(S(\gamma)^{\overline{G}})$.

(b) Since $V(\gamma)$ is an indecomposable projective $k_\sharp\widehat{\overline{G}}$-module, we can apply Proposition 6.9 to the socle of the algebra $\operatorname{End}_{k_\sharp\widehat{\overline{G}}}(V(\gamma)) \cong S(\gamma)^{\overline{G}}$. Therefore the generator w of this socle satisfies $\operatorname{Im}(w) \subseteq \operatorname{Soc}(V(\gamma))$, hence in fact $\operatorname{Im}(w) = \operatorname{Soc}(V(\gamma))$ since $w \neq 0$ and $\operatorname{Soc}(V(\gamma))$ is simple (Proposition 6.8). It follows that $V(\gamma)/\operatorname{Ker}(w)$ is a simple $k_\sharp\widehat{\overline{G}}$-module isomorphic to $\operatorname{Soc}(V(\gamma))$ and this forces the equality $\operatorname{Ker}(w) = J(V(\gamma))$ since $V(\gamma)/J(V(\gamma)) = T(\gamma)$ is the unique simple quotient of $V(\gamma)$. □

We are now ready for the description of the connection between the $\mathcal{O}G$-diagram U and the defect multiplicity module $V(\gamma)$. First recall that π_γ is a surjective homomorphism of $\overline{G}$-algebras which factorizes as follows:

$$A^P \longrightarrow \overline{A^P} \longrightarrow S(\gamma), \qquad a \mapsto \overline{a} \mapsto \pi_\gamma(a).$$

We denote by $\overline{\pi}_\gamma$ the second surjection, so that $\overline{\pi}_\gamma(\overline{a}) = \pi_\gamma(a)$. Similarly there is also a surjective homomorphism of $\overline{G}$-algebras

$$\mathrm{End}_{\mathcal{O}P}(TM) \longrightarrow \overline{\mathrm{End}}_{\mathcal{O}P}(TM) \xrightarrow{\sim} \overline{\mathrm{End}}_{\mathcal{O}P}(M) = \overline{A^P} \xrightarrow{\overline{\pi}_\gamma} S(\gamma),$$

where the middle isomorphism is the isomorphism 34.7. This shows in fact that $S(\gamma)$ is a simple quotient of $\mathrm{End}_{\mathcal{O}P}(TM)$, corresponding to some point γ'. Although we do not need this, the reader can check that $P_{\gamma'}$ is a defect of the unique non-projective summand of TM (namely ΩM when $\mathcal{O} = k$ and M itself when $\mathcal{O}$ is a discrete valuation ring). Combining the above two surjections, we obtain a surjective homomorphism of $\overline{G}$-algebras

$$\pi : \mathrm{End}_{\mathcal{O}P}(M) \times \mathrm{End}_{\mathcal{O}P}(TM) \longrightarrow \overline{A^P} \times \overline{A^P} \longrightarrow S(\gamma) \times S(\gamma).$$

Now $\mathrm{End}_{\mathcal{O}}(U)$ is a subalgebra of $\mathrm{End}_{\mathcal{O}}(M) \times \mathrm{End}_{\mathcal{O}}(TM)$. At the right hand side, we describe a subalgebra of $S(\gamma) \times S(\gamma)$ corresponding to a diagram. Let $w = \sigma(\overline{r}^G_P(\overline{u}))$ be a generator of $\mathrm{Soc}(S(\gamma)^{\overline{G}})$ (Proposition 36.10) and denote by W the diagram

$$W = (V(\gamma) \xrightarrow{w} V(\gamma))$$

of $k_\sharp\widehat{\overline{G}}$-modules (see Remark 31.11).

(36.11) LEMMA. *The homomorphism π above restricts to a homomorphism of $\overline{G}$-algebras*

$$\pi_U : \mathrm{End}_{\mathcal{O}P}(U) \longrightarrow \mathrm{End}_k(W)$$

which is a covering homomorphism.

Proof. We first have to show that the image of $\mathrm{End}_{\mathcal{O}P}(U)$ is contained in $\mathrm{End}_k(W)$. Let

$$(a, b') \in \mathrm{End}_{\mathcal{O}P}(M) \times \mathrm{End}_{\mathcal{O}P}(TM).$$

By definition, $(a, b') \in \mathrm{End}_{\mathcal{O}P}(U)$ if and only if $ua = b'u$, or more precisely $r^G_P(u)a = b'r^G_P(u)$. The image of this equation in the stable quotient $\overline{\mathrm{Hom}}_{\mathcal{O}P}(M, TM)$ is

$$\overline{r}^G_P(\overline{u})\,\overline{a} = \overline{b}'\overline{r}^G_P(\overline{u}). \tag{36.12}$$

But, by definition, the left $\overline{A^P}$-module structure on $\overline{\mathrm{Hom}}_{\mathcal{O}P}(M,TM)$ uses the isomorphism

$$\overline{\mathrm{End}}_{\mathcal{O}P}(TM) \cong \overline{\mathrm{End}}_{\mathcal{O}P}(M) = \overline{A^P}\,, \qquad \overline{b}' \mapsto \overline{b}\,, \tag{36.13}$$

so that $\overline{b}'\overline{r}^G_P(\overline{u}) = \overline{b}{\cdot}\overline{r}^G_P(\overline{u})$ (see 34.7). Therefore 36.12 is equivalent to $\overline{r}^G_P(\overline{u})\,\overline{a} = \overline{b}{\cdot}\overline{r}^G_P(\overline{u})$. Recall that $\overline{r}^G_P(\overline{u}) \in L_M(P)$ (Lemma 36.8) and that, by Lemma 36.9, we have an isomorphism of $(\overline{A^P},\overline{A^P})$-bimodules $\sigma : L_M(P) \longrightarrow S(\gamma)$. Thus the image under σ of the above equation is $\sigma(\overline{r}^G_P(\overline{u})){\cdot}\overline{a} = \overline{b}{\cdot}\sigma(\overline{r}^G_P(\overline{u}))$. By the definition of w, this gives

$$w\,\overline{\pi}_\gamma(\overline{a}) = \overline{\pi}_\gamma(\overline{b})\,w\,, \tag{36.14}$$

using also the fact that the action of $\overline{a}$ on $S(\gamma)$ is just the multiplication by $\overline{\pi}_\gamma(\overline{a})$. This shows that the pair $\pi(a,b') = (\overline{\pi}_\gamma(\overline{a}),\overline{\pi}_\gamma(\overline{b}))$ is an endomorphism of the diagram W.

Now we prove that π_U is a covering homomorphism. Let H be a subgroup of G containing P. We shall show that the map

$$\pi_U^{\overline{H}} : \mathrm{End}_{\mathcal{O}P}(U)^{\overline{H}} = \mathrm{End}_{\mathcal{O}H}(U) \longrightarrow \mathrm{End}_k(W)^{\overline{H}} = \mathrm{End}_{k_\sharp\widehat{\overline{H}}}(W)$$

is surjective. Since the projective module $V(\gamma)$ remains projective on restriction to $\overline{H}$, the $\overline{H}$-algebra $\mathrm{Res}^{\overline{G}}_{\overline{H}}(S(\gamma))$ is projective, or in other words $S(\gamma)^{\overline{H}} = S(\gamma)^{\overline{H}}_1$. Writing any element of $S(\gamma)^{\overline{H}}$ as a relative trace from 1 and using the surjectivity of

$$\pi : \mathrm{End}_{\mathcal{O}P}(M) \times \mathrm{End}_{\mathcal{O}P}(TM) \longrightarrow S(\gamma) \times S(\gamma)\,,$$

we deduce the surjectivity of

$$\pi^{\overline{H}} : \mathrm{End}_{\mathcal{O}H}(M) \times \mathrm{End}_{\mathcal{O}H}(TM) \longrightarrow S(\gamma)^{\overline{H}} \times S(\gamma)^{\overline{H}}\,.$$

Let $(c,d) \in \mathrm{End}_k(W)^{\overline{H}}$. Thus $c,d \in \mathrm{End}_k(V(\gamma))^{\overline{H}} = S(\gamma)^{\overline{H}}$ and we have $wc = dw$. There exists a pair (a,b') such that $\pi^{\overline{H}}(a,b') = (c,d)$, and the whole point is to show that one can choose (a,b') in such a way that $(a,b') \in \mathrm{End}_{\mathcal{O}H}(U)$ (that is, $ua = b'u$).

To this end we show that we can modify b'. By definition of π and since $wc = dw$, we have $w\,\overline{\pi}_\gamma(\overline{a}) = \overline{\pi}_\gamma(\overline{b})\,w$, where $\overline{b}$ corresponds to $\overline{b}'$ under the isomorphism 36.13. This is the equation 36.14 above, which has been seen in the first part of the proof to be equivalent to 36.12, namely

$$\overline{r}^G_P(\overline{u})\,\overline{a} = \overline{b}'\overline{r}^G_P(\overline{u})\,.$$

This is an equation in $\overline{\mathrm{Hom}}_{\mathcal{O}H}(M, TM)$, so by definition of stable quotients, we have

$$r_P^G(u)\, a = b' r_P^G(u) + t_1^H(f)$$

for some $f \in \mathrm{Hom}_{\mathcal{O}}(M, TM)$, and we write simply $ua = b'u + t_1^H(f)$. By Lemma 36.4, u has an $\mathcal{O}$-linear retraction $r : TM \to M$. Define $b'' = b' + t_1^H(fr)$. Then

$$b''u = b'u + t_1^H(fr)u = b'u + t_1^H(fru) = b'u + t_1^H(f) = ua\,,$$

so that $(a, b'') \in \underline{\mathrm{End}}_{\mathcal{O}H}(U)$. Since the map $\mathrm{End}_{\mathcal{O}H}(TM) \to S(\gamma)^{\overline{H}}$ factorizes through $\overline{\mathrm{End}}_{\mathcal{O}H}(TM)$, it is clear that b' and b'' have the same image $d \in S(\gamma)^{\overline{H}}$. Therefore $\pi^{\overline{H}}(a, b'') = (c, d)$, proving the surjectivity of $\pi_U^{\overline{H}}$. □

(36.15) COROLLARY. *Let Q be a p-subgroup of G containing P. Then $\overline{Q}$ is a defect group of the primitive $\overline{G}$-algebra $\mathrm{End}_{\mathcal{O}P}(U)$ if and only if $\overline{Q}$ is a defect group of W.*

Proof. As noticed in the proof of Corollary 36.6, defect groups (and more precisely defect pointed groups) are preserved by covering homomorphisms. □

We now come to the last step of the proof of Theorem 36.1 and establish a connection between the diagram W and the simple module $T(\gamma) = V(\gamma)/J(V(\gamma))$. Recall that w has kernel $J(V(\gamma))$ and image $\mathrm{Soc}(V(\gamma))$ (Proposition 36.10), so that w induces an isomorphism

$$w_0 : T(\gamma) = V(\gamma)/J(V(\gamma)) \xrightarrow{\sim} \mathrm{Soc}(V(\gamma))\,.$$

Let (c, d) be a k-endomorphism of the diagram W, so that we have $c, d \in \mathrm{End}_k(V(\gamma)) = S(\gamma)$ and $wc = dw$. Since $\mathrm{Ker}(w) = J(V(\gamma))$, we obtain

$$wc(J(V(\gamma))) = dw(J(V(\gamma))) = 0\,,$$

so that $c(J(V(\gamma))) \subseteq \mathrm{Ker}(w) = J(V(\gamma))$. It follows that c induces an endomorphism c_0 of the simple quotient $T(\gamma)$, and this defines a map

$$\rho : \mathrm{End}_k(W) \longrightarrow \mathrm{End}_k(T(\gamma))\,, \qquad (c, d) \mapsto c_0\,.$$

Similarly it is easy to check that d induces an endomorphism of $\mathrm{Soc}(V(\gamma))$, which is isomorphic to $T(\gamma)$ via w_0, and this defines an endomorphism of $T(\gamma)$ which coincides in fact with c_0. This will become clear in the proof below.

(36.16) LEMMA. *The map* $\rho : \mathrm{End}_k(W) \longrightarrow \mathrm{End}_k(T(\gamma))$ *is a covering homomorphism of* $\overline{G}$*-algebras.*

Proof. Let $\overline{H}$ be a subgroup of $\overline{G}$. We show that the homomorphism

$$\rho^{\overline{H}} : \mathrm{End}_k(W)^{\overline{H}} \longrightarrow \mathrm{End}_k(T(\gamma))^{\overline{H}}$$

is surjective. Let $c_0 \in \mathrm{End}_k(T(\gamma))^{\overline{H}}$. Since the projective module $V(\gamma)$ remains projective on restriction to $\overline{H}$, the $k_\sharp\widehat{\overline{H}}$-linear endomorphism c_0 of $T(\gamma)$ can be lifted to a $k_\sharp\widehat{\overline{H}}$-linear endomorphism c of $V(\gamma)$ such that $c(J(V(\gamma))) \subseteq J(V(\gamma))$.

On the other hand c_0 can be carried via the isomorphism w_0 to an automorphism d_0 of $\mathrm{Soc}(V(\gamma))$ defined by $d_0 = w_0 c_0 w_0^{-1}$. Since $k_\sharp\widehat{\overline{H}}$ is a symmetric algebra (Example 10.4), the projective module $\mathrm{Res}^{\overline{G}}_{\overline{H}}(V(\gamma))$ is injective (Proposition 6.7), and therefore d_0 extends to a $k_\sharp\widehat{\overline{H}}$-linear endomorphism d of $V(\gamma)$. Since $\mathrm{Ker}(w) = J(V(\gamma))$ and $\mathrm{Im}(w) = \mathrm{Soc}(V(\gamma))$, the equation $d_0 w_0 = w_0 c_0$ is equivalent to $dw = wc$. This shows that $(c, d) \in \mathrm{End}_k(W)^{\overline{H}}$ and proves the surjectivity of $\rho^{\overline{H}}$. □

(36.17) COROLLARY. *Let* Q *be a* p*-subgroup of* G *containing* P. *Then* $\overline{Q}$ *is a defect group of* W *if and only if* $\overline{Q}$ *is a defect group of* $T(\gamma)$.

Proof. A covering homomorphism preserves defect groups. □

We have now completed the description of the series of covering homomorphisms connecting the almost split sequence S_M to the simple module $T(\gamma)$. Therefore, by Corollary 36.6, Lemma 36.7, Corollaries 36.15 and 36.17, the proof of Theorem 36.1 is complete.

(36.18) REMARK. Since a covering homomorphism perserves not only defect groups, but defect pointed groups, an extension of the argument of the proof of Theorem 36.1 yields also a description of a source of the almost split sequence S_M.

Exercises

(36.1) Let M be a non-projective indecomposable $\mathcal{O}G$-lattice and let P_γ be a defect of $\mathrm{End}_{\mathcal{O}}(M)$. Consider the surjection

$$\mathrm{End}_{\mathcal{O}P}(TM) \longrightarrow \overline{\mathrm{End}}_{\mathcal{O}P}(TM) \xrightarrow{\sim} \overline{\mathrm{End}}_{\mathcal{O}P}(M) \xrightarrow{\overline{\pi}_\gamma} S(\gamma)\,.$$

Let γ' be the point of $\mathrm{End}_{\mathcal{O}P}(TM)$ corresponding to this simple quotient of $\mathrm{End}_{\mathcal{O}P}(TM)$. Prove that $P_{\gamma'}$ is a defect of the unique non-projective summand of TM (namely ΩM when $\mathcal{O}=k$ and M itself when $\mathcal{O}$ is a discrete valuation ring).

(36.2) Let M be a non-projective indecomposable $\mathcal{O}G$-lattice, let (P,X) be a vertex and source of M, and let S_M (respectively S_X) be the almost split sequence terminating in M (respectively in X).

(a) Prove that S_X is a direct summand of $\mathrm{Res}^G_P(S_M)$. [Hint: Use Proposition 35.2 and Lemma 36.8.]

(b) Prove that the point δ of $\mathrm{End}_{\mathcal{O}}(S_M)^P$ corresponding to the direct summand S_X is local. [Hint: Use Proposition 35.2.]

(c) Let $A=\mathrm{End}_{\mathcal{O}}(M)$, let γ be the point of A^P corresponding to X (so that P_γ is a defect of A), let $T(\gamma)=V(\gamma)/J(V(\gamma))$ be the unique simple quotient of the defect multiplicity module $V(\gamma)$, and let $m=\dim(T(\gamma))$. Prove that

$$\mathrm{Res}^G_P(S_M) \cong \Big(\bigoplus_{g\in[N_G(P)/N_G(P_\gamma)]} {}^g\big(\oplus^m S_X\big)\Big) \bigoplus Z\,,$$

where $\oplus^m S_X$ denotes the direct sum of m isomorphic copies of S_X and Z is a split sequence. [Hint: Let $n=\dim(V(\gamma))$ be the multiplicity of γ and let e be the sum of all of the n idempotents in γ appearing in some primitive decomposition of 1_A in A^P (so that $\pi_\gamma(e)=1_{S(\gamma)}$). First observe that

$$\mathrm{Res}^G_P(M) \cong \Big(\bigoplus_{g\in[N_G(P)/N_G(P_\gamma)]} {}^g eM\Big) \bigoplus N\,,$$

where N is the direct sum of all summands which are not sources of M. If $u\in\mathrm{Hom}_{\mathcal{O}G}(M,TM)$ is almost projective, then by extending the method of Lemma 36.8, prove that

$$\overline{r}^G_P(\overline{u}) = \sum_{g\in[N_G(P)/N_G(P_\gamma)]} {}^g\overline{e}\,\overline{r}^G_P(\overline{u})\;{}^g\overline{e}$$

and that the element $\overline{u}_e = \overline{e}\,\overline{r}_P^G(\overline{u})\,\overline{e} \in \overline{e}\,\overline{\mathrm{Hom}}_{\mathcal{O}P}(M,TM)\,\overline{e}$ is almost projective (see Exercise 35.2). Then write

$$e\;\mathrm{Hom}_{\mathcal{O}P}(M,TM)\,e \cong \mathrm{Hom}_{\mathcal{O}P}(X,TX)\otimes_{\mathcal{O}} M_n(\mathcal{O})\,,$$
$$L_{eM}(P) \cong L_X(P)\otimes_k S(\gamma)\,,$$

and write $\overline{u}_e \in L_{eM}(P)$ as $\overline{v}\otimes w$ where $\overline{v}$ is a generator of $L_X(P)$ and $w \in S(\gamma)$. Show that $w \in \mathrm{Soc}(S(\gamma)^{\overline{N}_G(P_\gamma)})$ using Proposition 36.10 and deduce that w is an endomorphism of rank m. A choice of basis of $V(\gamma)$ corresponds to a choice of a decomposition of eM as a direct sum of n indecomposable submodules isomorphic to X, and similarly for $e'TM$ (where $\overline{e}'$ corresponds to $\overline{e}$ via the isomorphism 34.7). By choosing independently decompositions of eM and of $e'TM$, one can write w as a diagonal matrix with exactly m non-zero entries, which can be chosen equal to 1. Deduce from this analysis that the pull-back of a projective cover of TM along u decomposes on restriction to P in a way which yields the result.]

(36.3) Let M be a non-projective indecomposable $\mathcal{O}G$-lattice, let P_γ be a defect of $\mathrm{End}_{\mathcal{O}}(M)$, let $V(\gamma)$ be the corresponding defect multiplicity module, and let S_M be the almost split sequence terminating in M.

(a) Prove that P is a defect group of S_M if and only if $V(\gamma)$ is a simple $k_\sharp\widehat{\overline{N}}_G(P_\gamma)$-module. [Hint: The projective module $V(\gamma)$ is the projective cover of $T(\gamma) = V(\gamma)/J(V(\gamma))$. If $V(\gamma)$ is not simple, then $T(\gamma)$ is not projective and has a non-trivial defect group.]

(b) Let the $\mathcal{O}P$-lattice X be a source of M and let S_X be the almost split sequence terminating in X. If the conditions of (a) are satisfied, prove that S_X is a source of S_M. [Hint: Use Exercise 36.2 (a).]

(c) Prove that the conditions of (a) are always satisfied when $N_G(P_\gamma)$ is a p-group.

(d) Prove that the conditions of (a) are always satisfied when P is a Sylow p-subgroup of G.

Notes on Section 36

The relationship between almost split sequences and defect multiplicity modules (Proposition 36.10 and part (c) of Exercise 36.2) was observed by Thévenaz [1988a] in the case of a discrete valuation ring and was then extended to the case of a field by Garotta [1994]. Some special cases of Theorem 36.1 are due to them, extending the work of Green [1985] who proved Theorem 36.1 when G is a p-group (see part (c) of Exercise 36.3).

In its full generality, Theorem 36.1 is due independently to Puig [1988c] and Uno [1988] (but only over a field). We have followed here Puig's paper.

Puig [1988c] also determined a source of an almost split sequence (see Remark 36.18). It was then proved by Okuyama and Uno [1990] that a defect group of the almost split sequence S_M terminating in M is either a vertex of M or a vertex of one of the summands of the middle term of S_M.

CHAPTER 6

Group algebras and blocks

Having treated modules, we now come to the second main example of interior G-algebras: group algebras and block algebras. We develop the main properties of group algebras and the various special features of pointed groups on group algebras. We introduce Brauer pairs, and we show that the partially ordered set of local pointed groups is a refinement of the poset obtained using Brauer pairs. We also prove the classical three main theorems of Brauer. We end the chapter with a result about the number of blocks with a given defect group.

The concept of source algebra of a block plays a central role throughout this chapter. We show that source algebras of block algebras contain the relevant information of block theory, in particular the generalized decomposition numbers. The theory is tightly linked with the theory of characters: Brauer's second theorem relates the values of characters with the p-local structure of the group algebra by making use of the generalized decomposition numbers. We prove various results about the structure of source algebras. In particular, we entirely determine this structure when the defect group is a normal subgroup of G.

We continue with our assumption that G is a finite group and that $\mathcal{O}$ is a commutative complete local noetherian ring with an algebraically closed residue field k of characteristic p. When we make the connection between characteristic zero and characteristic p, we assume further that $\mathcal{O}$ is a discrete valuation ring, with a field of fractions K of characteristic zero.

§ 37 POINTED GROUPS ON GROUP ALGEBRAS

In this section we describe various special features of the group algebra $\mathcal{O}G$. First recall that it is an interior G-algebra and that it has a G-invariant basis, namely G itself, so that $\mathcal{O}G$ is a permutation G-algebra.

(37.1) LEMMA. *We have* $(\mathcal{O}G)^G = Z\mathcal{O}G$, *where* $Z\mathcal{O}G$ *denotes the centre of* $\mathcal{O}G$. *In particular* $(\mathcal{O}G)^G$ *is commutative.*

Proof. By definition, an element belongs to $(\mathcal{O}G)^G$ if and only if it commutes with G, hence with the whole of $\mathcal{O}G$ by $\mathcal{O}$-linearity. □

Since $(\mathcal{O}G)^G = Z\mathcal{O}G$ is commutative, a point of $(\mathcal{O}G)^G$ consists of a single idempotent b. A primitive idempotent b of $(\mathcal{O}G)^G = Z\mathcal{O}G$ is called a *block* of $\mathcal{O}G$, and the algebra $\mathcal{O}Gb = b\mathcal{O}Gb$ is called a *block algebra*. Note that the block algebra $\mathcal{O}Gb$ is just the localization $(\mathcal{O}G)_\alpha$, where $\alpha = \{b\}$ is the corresponding point of $(\mathcal{O}G)^G$. In particular a block algebra is a primitive interior G-algebra. All the invariants attached to the pointed group $G_{\{b\}}$ (or to the point $\{b\}$) will be viewed as invariants of the block b itself. For instance a defect of $G_{\{b\}}$ will be called a defect of the block b.

The fact that $(\mathcal{O}G)^G$ is central also implies the following basic result.

(37.2) PROPOSITION. *Let* $\mathcal{O}G$ *be the group algebra of* G.
- (a) *Let* H_α *be a pointed group on* $\mathcal{O}G$. *There exists a unique block* b *such that* $H_\alpha \leq G_{\{b\}}$. *Moreover this relation is characterized by the property* $bi = i$ *for every* $i \in \alpha$.
- (b) *The poset of pointed groups on* $\mathcal{O}G$ *is isomorphic to the disjoint union of the posets of pointed groups on* $\mathcal{O}Gb$, *for* b *running over the set of blocks of* $\mathcal{O}G$.

Proof. (a) It is easy to see that $H_\alpha \leq G_{\{b\}}$ for some block b (Exercise 13.5), that is, $bi = i$ for some $i \in \alpha$. For any $i' \in \alpha$, we have $i' = {}^a i$ (where $a \in (\mathcal{O}G)^H$) and therefore

$$bi' = b\,{}^a i = {}^a(bi) = {}^a i = i'$$

because ${}^a b = b$ as b is central. Since $b'b = 0$ for any block b' distinct from b, the relation $b\alpha = \alpha$ implies that $b'\alpha = 0$. Thus H_α cannot be contained in $G_{\{b'\}}$.

(b) This follows directly from (a) and the fact that, since $\mathcal{O}Gb$ is a localization, the embedding $\mathcal{O}Gb \to \mathcal{O}G$ induces a bijection between the poset of pointed groups on $\mathcal{O}Gb$ and the poset of pointed groups on $\mathcal{O}G$ contained in $G_{\{b\}}$ (Proposition 15.2). □

A pointed group H_α on $\mathcal{O}G$ is said to be *associated* with a block b if $H_\alpha \leq G_{\{b\}}$. Note that b is unique by the proposition. Equivalently H_α is associated with b if and only if H_α is the image of a pointed group on $\mathcal{O}Gb$ under the embedding $\mathcal{O}Gb \to \mathcal{O}G$. In fact, as in part (b) of the proposition, we identify the pointed groups on $\mathcal{O}Gb$ with the pointed groups on $\mathcal{O}G$ associated with b.

In a primitive G-algebra, there is a unique conjugacy class of maximal local pointed groups (namely the defects of the G-algebra, see Corollary 18.6). This applies to each $\mathcal{O}Gb$, and so Proposition 37.2 implies that the blocks of $\mathcal{O}G$ are in bijection with the set of conjugacy classes of maximal local pointed groups on $\mathcal{O}G$ (via the map sending a block to its defects).

Applying Proposition 37.2 in the special case $H = 1$, we consider the set of points $\mathcal{P}(\mathcal{O}G)$, which is in bijection with both $\mathrm{Irr}(\mathcal{O}G)$ and $\mathrm{Proj}(\mathcal{O}G)$. Thus if i is a primitive idempotent of $\mathcal{O}G$ belonging to a point α, there is a unique block b such that $bi = i$ (or in other words $1_\alpha \leq G_{\{b\}}$). In that case we say that the corresponding simple kG-module $\mathcal{O}Gi/J(\mathcal{O}G)i$ and the corresponding indecomposable projective $\mathcal{O}G$-module $\mathcal{O}Gi$ are *associated* with the block b, or equivalently that they *belong* to the block b. An important special case of this occurs with the trivial kG-module k, which belongs to a unique block b_0 of $\mathcal{O}G$. This block b_0 is called the *principal block* of $\mathcal{O}G$.

More generally any primitive interior G-algebra A is also associated with a unique block b. Indeed if $\phi : \mathcal{O}G \to A$ is the structural map, then there is an orthogonal decomposition in A^G

$$1_A = \phi(1_{\mathcal{O}G}) = \sum_b \phi(b)\,,$$

where b runs over the blocks of $\mathcal{O}G$. Since A is primitive, there is a unique b such that $\phi(b) = 1_A$ (and $\phi(b') = 0$ for $b' \neq b$), and we say that A is *associated* with the block b, or that A *belongs* to b. In particular any indecomposable $\mathcal{O}G$-module (and more generally any indecomposable $\mathcal{O}G$-diagram) is associated with a unique block b. In that case b acts as the identity on the module, and b' annihilates the module for every block b' distinct from b. Moreover we have the following easy result.

(37.3) PROPOSITION. *Let b be a block of $\mathcal{O}G$ with defect group P.*

(a) Any primitive interior G-algebra A associated with b is projective relative to P. In particular P contains a defect group of A.

(b) Any indecomposable $\mathcal{O}G$-module M associated with b is projective relative to P. In particular P contains a vertex of M.

Proof. By the definition of a defect group, there exists $a \in (\mathcal{O}G)^P$ such that $t_P^G(a) = b$. If $\phi : \mathcal{O}G \to A$ is the structural map, then we have $1_A = \phi(b) = t_P^G(\phi(a))$, proving that A is projective relative to P. The statement in (b) follows from (a) by taking $A = \mathrm{End}_{\mathcal{O}}(M)$. □

There is another way of seeing the fact that the blocks partition the whole situation as a disjoint union. Whenever e is a central idempotent of an $\mathcal{O}$-algebra A, we have an isomorphism $A \cong Ae \times A(1-e)$, mapping a to $(ae, a(1-e))$, with inverse $(a,b) \mapsto a+b$. Applying this to the blocks of $\mathcal{O}G$, we obtain by induction an isomorphism

$$\mathcal{O}G \cong \prod_b \mathcal{O}Gb\,,$$

where b runs over the set of blocks of $\mathcal{O}G$. Thus in particular every $\mathcal{O}G$-module M decomposes as a direct sum $M = \bigoplus_b bM$, and each $\mathcal{O}G$-submodule bM can be viewed as an $\mathcal{O}Gb$-module because the other factors $\mathcal{O}Gb'$ annihilate bM (for $b' \neq b$). In particular if M is indecomposable, then $M = bM$ for some block b, and M is associated with b. Note that if M belongs to b, then M is a projective $\mathcal{O}G$-module if and only if M is a projective $\mathcal{O}Gb$-module. Indeed the free $\mathcal{O}Gb$-module $\mathcal{O}Gb$ is a direct summand of $\mathcal{O}G$ and is therefore projective over $\mathcal{O}G$; thus the same holds for any projective $\mathcal{O}Gb$-module.

Since $\mathcal{O}G$ is a permutation G-algebra, we can easily describe the H-fixed elements, for any subgroup H. If C is an orbit for the conjugation action of H on G, then C is called an *H-conjugacy class*, and the sum $\sum_{g\in C} g$ is called an *H-conjugacy class sum.*

(37.4) PROPOSITION. *Let H be a subgroup of G.*

(a) The set of all H-conjugacy class sums is a basis of $(\mathcal{O}G)^H$.

(b) The quotient map $\mathcal{O}G \to kG$ restricts to a surjective ring homomorphism $(\mathcal{O}G)^H \to (kG)^H$.

(c) The quotient map $\mathcal{O}G \to kG$ induces an isomorphism between the poset of pointed groups on $\mathcal{O}G$ and the poset of pointed groups on kG. In particular any block of kG lifts uniquely to a block of $\mathcal{O}G$.

(d) A pointed group on $\mathcal{O}G$ is local (respectively maximal local) if and only if its image in kG is local (respectively maximal local). In particular the image of the defect of a block is the defect of the image of the block.

Proof. (a) Let $a \in (\mathcal{O}G)^H$. If $g \in G$ appears with a coefficient $\lambda \in \mathcal{O}$ in the expression of a, then hgh^{-1} appears with coefficient λ in the expression of hah^{-1} (where $h \in H$). Since $hah^{-1} = a$, the whole H-orbit of g appears with the same coefficient λ, and the result follows immediately.

(b) This follows from (a) since reduction modulo $\mathfrak{p}$ maps a basis of $(\mathcal{O}G)^H$ to a basis of $(kG)^H$.

(c) Since $\mathfrak{p}(\mathcal{O}G)^H \subseteq J((\mathcal{O}G)^H)$ and since $(\mathcal{O}G)^H \to (kG)^H$ is surjective, the theorem on lifting idempotents implies that $\mathcal{P}((\mathcal{O}G)^H)$ is in bijection with $\mathcal{P}((kG)^H)$. It is easy to check that these bijections (for H running over the set of subgroups of G) are compatible with the order relation between pointed groups. Details are left to the reader (Exercise 37.1).

(d) The statement about local pointed groups is an immediate consequence of the definition, because the quotient $\overline{(\mathcal{O}G)}(P)$ of $(\mathcal{O}G)^P$ coincides with the quotient $\overline{(kG)}(P)$ of $(kG)^P$. The statement about maximal local pointed groups follows from (c). □

In fact reduction modulo $\mathfrak{p}$ is also compatible with the other relation *pr* between pointed groups (Exercise 37.1).

Since $\mathcal{O}G$ is a permutation G-algebra, we have an explicit description of the Brauer homomorphism, as follows. Note that a P-conjugacy class is a singleton $\{g\}$ if and only if $g \in C_G(P)$. In other words a P-conjugacy class outside $C_G(P)$ is a non-trivial P-orbit.

(37.5) PROPOSITION. *Let P be a p-subgroup of G.*

(a) *The composition of the inclusion $\mathcal{O}C_G(P) \to (\mathcal{O}G)^P$ and the Brauer homomorphism $br_P : (\mathcal{O}G)^P \to \overline{\mathcal{O}G}(P)$ induces an isomorphism of k-algebras $kC_G(P) \xrightarrow{\sim} \overline{\mathcal{O}G}(P)$.*

(b) *If $\overline{\mathcal{O}G}(P)$ is identified with $kC_G(P)$ via the isomorphism of (a), then the Brauer homomorphism is the surjective map*

$$br_P : (\mathcal{O}G)^P \longrightarrow kC_G(P)$$

mapping an element of $C_G(P)$ to itself (viewed as a basis element of $kC_G(P)$), and mapping to zero any P-conjugacy class sum involving elements of G outside $C_G(P)$.

Proof. Since $\mathcal{O}G$ has a G-invariant basis (namely G), Proposition 27.6 applies. The set of P-fixed elements in G is $C_G(P)$. Thus $\overline{\mathcal{O}G}(P)$ has a k-basis $br_P(C_G(P))$, and the sum of all elements in a non-trivial P-orbit is in the kernel of br_P. The result follows. □

We shall always identify $\overline{\mathcal{O}G}(P)$ with $kC_G(P)$ via the canonical isomorphism of the proposition and consequently we shall always view br_P as the map described in part (b).

Since a block b of $\mathcal{O}G$ is a central element of $(\mathcal{O}G)^P$, it is mapped by br_P to a central idempotent of $kC_G(P)$. Thus $br_P(b)$ is either zero or a sum of blocks of $kC_G(P)$. Any block e of $kC_G(P)$ appearing in a decomposition of $br_P(b)$ (that is, $br_P(b)e = e$) is called a *Brauer correspondent* of b. Moreover, since $br_P(1_{\mathcal{O}G}) = 1_{kC_G(P)}$, any block of $kC_G(P)$ is the Brauer correspondent of some block of $\mathcal{O}G$, which is clearly unique. Thus the blocks of $\mathcal{O}G$ partition the set of blocks of $kC_G(P)$. Later in Section 40, we shall come back to this approach, which associates blocks of $C_G(P)$ with any given block of $\mathcal{O}G$.

Another important consequence of the proposition is that the local points of $(\mathcal{O}G)^P$ correspond to the irreducible representations of $kC_G(P)$. Indeed $\mathcal{LP}((\mathcal{O}G)^P)$ is in bijection with $\mathcal{P}(kC_G(P))$ via the Brauer homomorphism (Lemma 14.5) and $\mathcal{P}(kC_G(P))$ is in bijection with $\mathrm{Irr}(kC_G(P))$. Viewed slightly differently, the multiplicity algebra $S(\gamma)$ of a local point γ is in fact a simple quotient of $\overline{\mathcal{O}G}(P) = kC_G(P)$ (because γ is local), and so $S(\gamma)$ is isomorphic to the k-endomorphism algebra of a simple $kC_G(P)$-module. Explicitly if i is a primitive idempotent of $(\mathcal{O}G)^P$ belonging to a local point γ, then $br_P(i)$ is primitive in $kC_G(P)$ and defines a simple $kC_G(P)$-module, namely $kC_G(P)br_P(i)/J(kC_G(P))br_P(i)$.

Note that $Z(P)$ acts trivially on any simple $kC_G(P)$-module V. Indeed one can either apply Corollary 21.2 (because $Z(P)$ is a normal p-subgroup of $C_G(P)$), or the fact that, since $Z(P)$ is central in $C_G(P)$, it is mapped to the centre k^* of $\mathrm{End}_k(V)$, forcing the image of $Z(P)$ to be $\{1\}$ since k^* does not contain any non-trivial p-th root of unity. Therefore we have $\mathrm{Irr}(kC_G(P)) \cong \mathrm{Irr}(k\overline{C}_G(P))$, where we set as usual $\overline{C}_G(P) = C_G(P)/Z(P) \cong PC_G(P)/P$.

But in fact the multiplicity algebra $S(\gamma)$ of a local pointed group P_γ has an $\overline{N}_G(P_\gamma)$-algebra structure, which is interior on restriction to the subgroup $\overline{C}_G(P)$. In other words (see Example 10.9) the multiplicity module $V(\gamma)$ of P_γ is endowed with a $k_\sharp\widehat{\overline{N}}_G(P_\gamma)$-module structure, and on restriction to $\overline{C}_G(P)$ it is a module over the untwisted group algebra $k\overline{C}_G(P)$. Summarizing the whole discussion, we have the following result.

(37.6) COROLLARY. *Let P be a p-subgroup of G.*

(a) *If γ is a local point of $(\mathcal{O}G)^P$, then the multiplicity module $V(\gamma)$ of P_γ is a simple $k_\sharp\widehat{\overline{N}}_G(P_\gamma)$-module. Moreover its restriction to $k\overline{C}_G(P)$ is also simple.*

(b) *The Brauer homomorphism induces a bijection*

$$\mathcal{LP}((\mathcal{O}G)^P) \longrightarrow \mathcal{P}(kC_G(P)) \cong \mathrm{Irr}(kC_G(P)) \cong \mathrm{Irr}(k\overline{C}_G(P)),$$

mapping a point γ *to the multiplicity module of* γ *(viewed as a* $k\overline{C}_G(P)$*-module by restriction).*

It should be noted that, since the set of local pointed groups on $\mathcal{O}G$ is a poset and is in bijection with the disjoint union $\bigcup_P \mathrm{Irr}(kC_G(P))$ (where P runs over the set of p-subgroups of G), one can put a partial order relation on $\bigcup_P \mathrm{Irr}(kC_G(P))$; moreover this relation implies the containment relation between the corresponding p-subgroups. However, it is not clear whether it is possible to define this partial order relation directly in terms of irreducible representations. Indeed the description of the relation is obtained by first lifting each point of $kC_G(P)$ to a (local) point of $(\mathcal{O}G)^P$, and then using the known containment relation between pointed groups.

The simplicity of the multiplicity module of a local point has an important consequence for the poset of pointed groups on $\mathcal{O}G$. The result is similar to the Green correspondence, but much stronger.

(37.7) PROPOSITION. *Let* P_γ *be a local point on* $\mathcal{O}G$.
(a) *For every subgroup* H *containing* $PC_G(P)$, *there exists a unique point* $\alpha \in \mathcal{P}((\mathcal{O}G)^H)$ *such that* $H_\alpha \geq P_\gamma$. *Moreover* α *has multiplicity one.*
(b) *The poset* $\{H_\alpha \mid H_\alpha \geq P_\gamma\,,\ H \geq PC_G(P)\}$ *is isomorphic to the poset of subgroups of* G *containing* $PC_G(P)$, *via the map* $H_\alpha \mapsto H$.

Proof. (a) Since H contains P, we can consider the composite map $A^H \overset{r_P^H}{\to} A^P \overset{\pi_\gamma}{\to} S(\gamma)$. Since $H \geq C_G(P)$ and since π_γ is a homomorphism of $C_G(P)$-algebras, the image of $\pi_\gamma r_P^H$ is contained in the $C_G(P)$-fixed elements $S(\gamma)^{C_G(P)}$. But $S(\gamma)^{C_G(P)} \cong \mathrm{End}_{kC_G(P)}(V(\gamma)) \cong k$ by Schur's lemma, because $V(\gamma)$ is simple on restriction to $C_G(P)$ (Corollary 37.6). Therefore the image of $\pi_\gamma r_P^H$ is isomorphic to k (note that $\pi_\gamma r_P^H$ is nonzero because it is a unitary homomorphism). Thus k is a simple quotient of A^H, which corresponds to a point α of A^H with multiplicity one. By construction, α is the unique point of A^H such that $\pi_\gamma r_P^H(\alpha) \neq \{0\}$, or equivalently $H_\alpha \geq P_\gamma$.

(b) By (a), it is clear that the map $H_\alpha \mapsto H$ is a bijection between the two posets defined in the statement. It is also clear that this map is order preserving, so we only have to prove that its inverse is order preserving. Let $H \geq K \geq PC_G(P)$. Let $\alpha \in \mathcal{P}((\mathcal{O}G)^H)$ and $\beta \in \mathcal{P}((\mathcal{O}G)^K)$ be such that $H_\alpha \geq P_\gamma$ and $K_\beta \geq P_\gamma$. By Exercise 13.5, there always exists some pointed group $H_{\alpha'}$ such that $H_{\alpha'} \geq K_\beta$. Then $H_{\alpha'} \geq P_\gamma$, and by uniqueness of α we have $\alpha' = \alpha$, hence $H_\alpha \geq K_\beta$. □

The proposition is stronger than the Green correspondence in many respects. First we go down to the subgroup $PC_G(P)$ rather than $N_G(P_\gamma)$. Next the uniqueness means that we have a "Green correspondence" between two *singletons* $\{G_\alpha\}$ and $\{H_\beta\}$, whenever $G_\alpha \geq H_\beta \geq P_\gamma$. Finally the most crucial remark is that P_γ is an arbitrary local pointed group and need not be a defect of the pointed groups under consideration.

A p-subgroup P of G is called *self-centralizing* if any p-subgroup Q of G centralizing P is contained in P. Then Q is in fact contained in $Z(P)$, so that in other words we require $Z(P)$ to be a Sylow p-subgroup of $C_G(P)$. Since $PC_G(P)/P \cong C_G(P)/Z(P)$, this is also equivalent to requiring that P is a Sylow p-subgroup of $PC_G(P)$. Now defect groups and defect pointed groups are generalizations of Sylow p-subgroups, so we can define an analogous notion for pointed groups. Let P_γ be a local pointed group on $\mathcal{O}G$, and let α be the unique point of $(\mathcal{O}G)^{PC_G(P)}$ such that $P_\gamma \leq (PC_G(P))_\alpha$ (Proposition 37.7). Then P_γ is called *self-centralizing* if P_γ is a defect pointed group of $(PC_G(P))_\alpha$. Since P_γ is local and $P_\gamma \leq (PC_G(P))_\alpha$, it is sufficient to require that P is a defect group of $(PC_G(P))_\alpha$ (using part (v) of Theorem 18.3). In fact it is even sufficient to require that $(PC_G(P))_\alpha$ is projective relative to P, because $br_P\, r_P^{PC_G(P)}(\alpha) \neq \{0\}$ holds anyway as P_γ is local and $P_\gamma \leq (PC_G(P))_\alpha$. We now show that the property of being self-centralizing can be characterized using the multiplicity module.

(37.8) LEMMA. *A local pointed group P_γ on $\mathcal{O}G$ is self-centralizing if and only if the multiplicity module $V(\gamma)$ is projective on restriction to $k\overline{C}_G(P)$.*

Proof. The Puig correspondence (Theorem 19.1) is a bijection between the points in $\mathcal{P}((\mathcal{O}G)^{PC_G(P)})$ with defect P_γ and the isomorphism classes of indecomposable projective direct summands of the multiplicity module $\mathrm{Res}^{\overline{N}_G(P_\gamma)}_{\overline{C}_G(P)}(V(\gamma))$. But by Proposition 37.7, there is a unique point $\alpha \in \mathcal{P}((\mathcal{O}G)^{PC_G(P)})$ such that $P_\gamma \leq (PC_G(P))_\alpha$, and on the other hand $\mathrm{Res}^{\overline{N}_G(P_\gamma)}_{\overline{C}_G(P)}(V(\gamma))$ is indecomposable, because it is simple (Corollary 37.6). Therefore $(PC_G(P))_\alpha$ has defect P_γ if and only if $\mathrm{Res}^{\overline{N}_G(P_\gamma)}_{\overline{C}_G(P)}(V(\gamma))$ is projective. □

If P_γ is self-centralizing, the multiplicity module $V(\gamma)$ is both simple and projective on restriction to $k\overline{C}_G(P)$. Turning now to the characterization of the defect P_γ of a block, we need the stronger requirement that $V(\gamma)$ be projective as a module over $k_\sharp\widehat{\overline{N}}_G(P_\gamma)$. This is made explicit in the following result.

(37.9) THEOREM. *Let P_γ be a local pointed group on $\mathcal{O}G$, let $V(\gamma)$ be its multiplicity module, and let b be the unique block of $\mathcal{O}G$ such that $P_\gamma \leq G_{\{b\}}$. The following conditions are equivalent.*
(a) *P_γ is a defect of b.*
(b) *P_γ is a defect of the primitive G-algebra $\mathcal{O}Gb$.*
(c) *$V(\gamma)$ is projective over $k_\sharp\widehat{\overline{N}}_G(P_\gamma)$.*
(d) *$\mathrm{Res}^{\overline{N}_G(P_\gamma)}_{\overline{C}_G(P)}(V(\gamma))$ is projective over $k\overline{C}_G(P)$ and p does not divide $|N_G(P_\gamma)/PC_G(P)|$.*
(e) *P_γ is self-centralizing and p does not divide $|N_G(P_\gamma)/PC_G(P)|$.*

Proof. The equivalence of (a) and (b) is clear in view of the embedding $\mathcal{O}Gb \to \mathcal{O}G$ (and the fact that (a) means that P_γ is a defect of $G_{\{b\}}$).

The equivalence of (a) and (c) follows from the Puig correspondence (as in the proof of Lemma 37.8 above). Alternatively, one can work in the primitive G-algebra $\mathcal{O}Gb$ and notice that $V(\gamma)$ is still the multiplicity module of P_γ in $\mathcal{O}Gb$ (Exercise 37.6). Then the equivalence of (b) and (c) follows from Corollary 19.3.

For the equivalence between (c) and (d), we note that, by Higman's criterion, $V(\gamma)$ is projective if and only if $t_1^{\overline{N}} : S(\gamma) \to S(\gamma)^{\overline{N}}$ is surjective, where $\overline{N} = \overline{N}_G(P_\gamma)$. Since $V(\gamma)$ is simple on restriction to $\overline{C} = \overline{C}_G(P)$, we have $S(\gamma)^{\overline{C}} \cong k$ by Schur's lemma, and a fortiori $S(\gamma)^{\overline{N}} \cong k$. Therefore the relative trace map $t_1^{\overline{N}}$ factorizes as

$$S(\gamma) \xrightarrow{t_1^{\overline{C}}} k \xrightarrow{t_{\overline{C}}^{\overline{N}}} k\,.$$

Since $\overline{N}/\overline{C}$ necessarily acts trivially on k, the second map is multiplication by $|\overline{N}/\overline{C}|$, which is either zero or an isomorphism. Therefore $t_1^{\overline{N}}$ is surjective if and only if $t_1^{\overline{C}}$ is surjective and $|\overline{N}/\overline{C}|\cdot 1_k \neq 0$. The first condition is equivalent to the projectivity of $\mathrm{Res}^{\overline{N}}_{\overline{C}}(V(\gamma))$ (Higman's criterion), and the second means that p does not divide $|\overline{N}/\overline{C}| = |N_G(P_\gamma)/PC_G(P)|$.

Finally (d) and (e) are equivalent by Lemma 37.8 above. □

In the same vein and with the same proof, there is the following slightly more general result.

(37.10) PROPOSITION. *Let P_γ be a local pointed group on $\mathcal{O}G$, let $V(\gamma)$ be its multiplicity module, let H be a subgroup of G such that $PC_G(P) \leq H$, and let α be the unique point of $(\mathcal{O}G)^H$ such that $P_\gamma \leq H_\alpha$ (see Proposition 37.7). Then P_γ is a defect of H_α if and only if $\mathrm{Res}^{\overline{N}_G(P)}_{\overline{C}_G(P)}(V(\gamma))$ is projective and p does not divide $|N_H(P_\gamma)/PC_G(P)|$.*

Proof. This is left as an exercise for the reader. □

Condition (d) in Theorem 37.9 is expressed entirely in terms of the multiplicity module $V(\gamma)$, provided one can also characterize $N_G(P_\gamma)$ in terms of $V(\gamma)$. But this is easy.

(37.11) PROPOSITION. *Let P_γ be a local pointed group on $\mathcal{O}G$, and view by restriction its multiplicity module $V(\gamma)$ as a module over $kC_G(P)$. Then $N_G(P_\gamma)$ is equal to the inertial subgroup of $V(\gamma)$ in $N_G(P)$.*

Proof. Let $g \in N_G(P)$ and let $\mathrm{Conj}(g) : (\mathcal{O}G)^P \to (\mathcal{O}G)^P$ be conjugation by g. Then $\mathrm{Conj}(g)$ induces an isomorphism of k-algebras $\overline{\mathrm{Conj}(g)} : S(\gamma) \to S({}^g\gamma)$ such that the following diagram commutes.

$$\begin{array}{ccc} (\mathcal{O}G)^P & \xrightarrow{\mathrm{Conj}(g)} & (\mathcal{O}G)^P \\ {\scriptstyle \pi_\gamma}\big\downarrow & & \big\downarrow{\scriptstyle \pi_{{}^g\gamma}} \\ S(\gamma) & \xrightarrow{\overline{\mathrm{Conj}(g)}} & S({}^g\gamma) \end{array}$$

Note that the $kC_G(P)$-module structure on $V(\gamma)$ is given by the interior $C_G(P)$-algebra structure on $S(\gamma)$ mapping $c \in C_G(P)$ to $\pi_\gamma(c{\cdot}1_{\mathcal{O}G})$, and similarly for the $kC_G({}^gP)$-module structure on $V({}^g\gamma)$. Now we have

$$\overline{\mathrm{Conj}(g)}(\pi_\gamma(g^{-1}cg{\cdot}1_{\mathcal{O}G})) = \pi_{{}^g\gamma}\ \mathrm{Conj}(g)(g^{-1}cg{\cdot}1_{\mathcal{O}G}) = \pi_{{}^g\gamma}(c{\cdot}1_{\mathcal{O}G}),$$

and this means that $\overline{\mathrm{Conj}(g)}$ is an isomorphism of interior $C_G(P)$-algebras, provided the algebra $S(\gamma)$ is endowed with the conjugate structure mapping $c \in C_G(P)$ to $\pi_\gamma(g^{-1}cg{\cdot}1_{\mathcal{O}G})$. Reinterpreted in terms of modules, this says that ${}^g(V(\gamma)) \cong V({}^g\gamma)$ (where both $V(\gamma)$ and $V({}^g\gamma)$ are viewed as modules over $kC_G(P)$).

If now $g \in N_G(P_\gamma)$, then ${}^g(V(\gamma)) \cong V({}^g\gamma) = V(\gamma)$, and therefore g belongs to the inertial subgroup of $V(\gamma)$. If conversely $g \notin N_G(P_\gamma)$, then $S(\gamma)$ and $S({}^g\gamma)$ are distinct simple quotients of $(\mathcal{O}G)^P$, and since γ is local (so that ${}^g\gamma$ is local too), $S(\gamma)$ and $S({}^g\gamma)$ are in fact distinct simple quotients of $\overline{(\mathcal{O}G)}(P) = kC_G(P)$, so that $V(\gamma)$ and $V({}^g\gamma)$ are non-isomorphic simple $kC_G(P)$-modules. Therefore $V(\gamma)$ and ${}^g(V(\gamma))$ are non-isomorphic and g does not belong to the inertial subgroup of $V(\gamma)$. □

We know that $Z(P)$ acts trivially on $V(\gamma)$, so that $V(\gamma)$ has in fact a $k\overline{C}_G(P)$-module structure. Proposition 37.11 asserts equivalently that $\overline{N}_G(P_\gamma)$ is characterized as the inertial subgroup in $\overline{N}_G(P)$ of the $k\overline{C}_G(P)$-module $V(\gamma)$.

Note that the $k\overline{C}_G(P)$-module structure of $V(\gamma)$ entirely determines its $k_\sharp\widehat{\overline{N}}_G(P_\gamma)$-module structure. Indeed by Example 10.10, the simple

$k\overline{C}_G(P)$-module $V(\gamma)$ extends canonically to a module over $k_\sharp\widehat{\overline{N}_G(P_\gamma)}$, because $\overline{N}_G(P_\gamma)$ is the inertial subgroup of $V(\gamma)$. This is why it does no harm to restrict $V(\gamma)$ to $k\overline{C}_G(P)$, both in Theorem 37.9 and in the theorem below.

We now show that Brauer's first main theorem is an easy consequence of the previous results. We give a version of the theorem which uses multiplicity modules. We shall see later in Section 40 another version of the result in terms of blocks only.

(37.12) THEOREM (Brauer's first main theorem). *Let P be a p-subgroup of G. There is a bijection between the set of all blocks of $\mathcal{O}G$ with defect group P and the set of all $\overline{N}_G(P)$-conjugacy classes of projective simple $k\overline{C}_G(P)$-modules having an inertial subgroup I in $\overline{N}_G(P)$ such that $|I/\overline{C}_G(P)|$ is prime to p. The bijection maps a block b to the $\overline{N}_G(P)$-conjugacy class of the $k\overline{C}_G(P)$-module $V(\gamma)$, where $V(\gamma)$ is a defect multiplicity module of b (restricted to $k\overline{C}_G(P)$).*

Proof. By Theorem 37.9, the map defined in the statement is well-defined; this uses the fact that $I = \overline{N}_G(P_\gamma)$ by Proposition 37.11. In order to define the inverse map, we let V be a projective simple $k\overline{C}_G(P)$-module having an inertial subgroup I in $\overline{N}_G(P)$ such that $|I/\overline{C}_G(P)|$ is prime to p. Then V is a simple $kC_G(P)$-module, so that $V = V(\gamma)$ for some local pointed group P_γ on $\mathcal{O}G$ (Corollary 37.6). Let b be the unique block of $\mathcal{O}G$ such that $P_\gamma \leq G_{\{b\}}$. By Theorem 37.9 and the fact that $I = \overline{N}_G(P_\gamma)$ (Proposition 37.11), P_γ is a defect of b. In particular b is a block with defect group P. This defines the inverse map, for it is clear that an $N_G(P)$-conjugate of V yields an $N_G(P)$-conjugate of P_γ, hence the same block b. □

If P_γ is a defect of a block b of $\mathcal{O}G$, the Puig correspondence (with respect to P_γ) is a bijection between the singleton $\{b\}$ and the projective simple $k_\sharp\widehat{\overline{N}_G(P_\gamma)}$-module $V(\gamma)$. In that case any $N_G(P)$-conjugate of γ is also a defect of b, so that only the $N_G(P)$-conjugacy class of $V(\gamma)$ can be considered as an invariant of b. Theorem 37.12 can be viewed as the disjoint union over blocks of the above Puig correspondences between singletons.

We shall see in Section 39 that any projective simple $k\overline{C}_G(P)$-module belongs in fact to a block of defect zero of $k\overline{C}_G(P)$ (that is, a block with a trivial defect group). It will follow that the bijection of the theorem can also be viewed as a bijection between blocks of $\mathcal{O}G$ with defect group P and some $\overline{N}_G(P)$-conjugacy class of blocks of defect zero of $k\overline{C}_G(P)$ (see Section 39). Moreover we shall also see that any such block of $k\overline{C}_G(P)$

is the image of a block of $kC_G(P)$, and that this block of $kC_G(P)$ is a Brauer correspondent of the original block of $\mathcal{O}G$ (see Section 40).

We derive another classical version of Brauer's result as a corollary.

(37.13) COROLLARY. *Let P be a p-subgroup of G. There is a bijection between the set of all blocks of $\mathcal{O}G$ with defect group P and the set of all blocks of $\mathcal{O}N_G(P)$ with defect group P. The bijection maps a block b of $\mathcal{O}G$ to a block e of $\mathcal{O}N_G(P)$ if and only if b and e have the same $N_G(P)$-conjugacy class of defect multiplicity modules.*

Proof. By Theorem 37.12, both sets of blocks in the statement are in bijection with the set of all $\overline{N}_G(P)$-conjugacy classes of projective simple $k\overline{C}_G(P)$-modules having an inertial subgroup I in $\overline{N}_G(P)$ such that $|I/\overline{C}_G(P)|$ is prime to p. □

Exercises

(37.1) Let H_α and K_β be two pointed groups on $\mathcal{O}G$. Let $\overline{\alpha}$ (respectively $\overline{\beta}$) be the image of α in $(kG)^H$ (respectively of β in $(kG)^K$). Prove that $H_\alpha \geq K_\beta$ if and only if $H_{\overline{\alpha}} \geq K_{\overline{\beta}}$, and that $H_\alpha \, pr \, K_\beta$ if and only if $H_{\overline{\alpha}} \, pr \, K_{\overline{\beta}}$.

(37.2) Let P be a p-subgroup of G.

(a) Prove that $(kG)_P^G$ has a k-basis consisting of all class sums of elements $g \in G$ such that P contains a Sylow p-subgroup of $C_G(g)$. [Hint: Show that a basis element of $(kG)^P$ has the form $t_{C_P(g)}^P(g)$ and that $t_P^G(t_{C_P(g)}^P(g)) = |C_G(g) : C_P(g)| \cdot t_{C_G(g)}^G(g)$.]

(b) Let b be a block of kG. Prove that the following conditions are equivalent.

(i) P is a defect group of b.

(ii) b is a k-linear combination of elements $g \in G$ such that a Sylow p-subgroup of $C_G(g)$ is contained in a conjugate of P, and P is a minimal subgroup with this property.

(37.3) Prove Proposition 37.10. [Hint: Follow the proof of Theorem 37.9.]

(37.4) Let P_γ be a local pointed group on $\mathcal{O}G$. Let H_α and K_β be pointed groups on $\mathcal{O}G$ such that $P_\gamma \leq K_\beta \leq H_\alpha$ and $PC_G(P) \leq K$. Prove that P_γ is a defect of H_α if and only if P_γ is a defect of K_β and $|N_H(P_\gamma) : N_K(P_\gamma)|$ is prime to p.

(37.5) Let P_γ be a local pointed group on $\mathcal{O}G$, let H_α and K_β be two pointed groups containing P_γ, and suppose that $PC_G(P) \leq H$. Prove that $K_\beta \leq H_\alpha$ if and only $K \leq H$.

(37.6) Let b be a block of $\mathcal{O}G$, let H_α be a pointed group on $\mathcal{O}Gb$, and let $H_{\alpha'}$ be its image in $\mathcal{O}G$ via the embedding $\mathcal{F} : \mathcal{O}Gb \to \mathcal{O}G$. By Proposition 15.3, $\mathcal{F}$ induces an embedding $\overline{\mathcal{F}}(\alpha) : S(\alpha) \to S(\alpha')$. Prove that $\overline{\mathcal{F}}(\alpha)$ is an exo-isomorphism.

(37.7) Prove that a defect group of the principal block of $\mathcal{O}G$ is a Sylow p-subgroup of G.

(37.8) Assume that G has a normal p-subgroup P.
(a) Prove that any defect group of a block of $\mathcal{O}G$ contains P. [Hint: Use Exercise 21.5.]
(b) Prove that any block of $\mathcal{O}G$ is an element of $\mathcal{O}C_G(P)$. [Hint: It suffices to work over k. Using the fact that P acts trivially on every simple kG-module (Corollary 21.2), prove that $(kG)_Q^P \subseteq J(kG)$ for every $Q < P$, so that $(kG)^P = kC_G(P) + J((kG)^P)$. Deduce that $ZkG = (kC_G(P))^G + J(ZkG)$.]
(c) Prove that the set of blocks of $\mathcal{O}PC_G(P)$ coincides with the set of blocks of $\mathcal{O}C_G(P)$.
(d) If b is a block of $\mathcal{O}C_G(P)$, prove that Q is a defect group of b as a block of $\mathcal{O}C_G(P)$ if and only if PQ is a defect group of b as a block of $\mathcal{O}PC_G(P)$. [Hint: It suffices to work with the image $\overline{b}$ of b in kG. Use (a), Corollary 11.10, and the fact that $br_P(\overline{b}) = \overline{b}$.]

Notes on Section 37

The characterization of defect groups of blocks given in Exercise 37.2 is the original approach used by Brauer for the definition of defect groups. Of course Brauer's first main theorem is due to Brauer [1956] (but with a different point of view). For the results on pointed groups on $\mathcal{O}G$, we have followed Puig [1981, 1984].

§ 38 THE SOURCE ALGEBRAS OF A BLOCK

We discuss in this section one of the main concepts of this book: source algebras of blocks. We prove several basic properties of source algebras of blocks and we state Puig's finiteness conjecture, which seems to be one of the main challenges in this subject. Further results on source algebras appear later in this chapter and the next.

Let b be a block of $\mathcal{O}G$ and let P be a defect group of b. For every choice of a source point γ (unique up to $N_G(P)$-conjugation for a fixed P by Theorem 18.3), we have a defect P_γ and an associated embedding $\mathcal{F}_\gamma : (\mathcal{O}Gb)_\gamma \to \mathrm{Res}^G_P(\mathcal{O}Gb)$, unique up to a unique exo-isomorphism. Recall that the interior P-algebra $(\mathcal{O}Gb)_\gamma$ is called a source algebra of $\mathcal{O}Gb$, or simply a source algebra of b, and that it is unique up to isomorphism (but the isomorphism need not be unique whenever we consider the P-algebra $(\mathcal{O}Gb)_\gamma$ without the associated embedding $\mathcal{F}_\gamma$). In practice one can always choose $i \in \gamma$ and take $(\mathcal{O}Gb)_\gamma = i(\mathcal{O}Gb)i$. Then $(\mathcal{O}Gb)_\gamma = i\mathcal{O}Gi$ since $bi = i$ (because $P_\gamma \leq G_{\{b\}}$). Recall also that any $N_G(P)$-conjugate of $(\mathcal{O}Gb)_\gamma$ is again a source algebra of b (corresponding to a conjugate of γ), so that, for a fixed defect group P, only the $N_G(P)$-conjugacy class of source algebras is an invariant of the block b. However, the description of one such source algebra suffices to determine its conjugacy class.

We are going to see why the determination of a source algebra of a block can be considered as one of the main problems of block theory. In fact the p-local invariants attached to a block b can be determined from the knowledge of a source algebra of b. Thus instead of classifying block algebras up to isomorphism (which would be too much to ask for), one is aiming for a classification of blocks up to equivalence, where two blocks $\mathcal{O}Gb$ and $\mathcal{O}G'b'$ are considered to be equivalent if they have the same defect group and isomorphic source algebras. The main idea is that many different blocks (for various finite groups G) actually have the same source algebra. All possible source algebras have been described when the defect group P is either cyclic or the Klein group of order 4.

We first note that source algebras behave well with respect to reduction modulo $\mathfrak{p}$.

(38.1) LEMMA. *Let b be a block of $\mathcal{O}G$, let P_γ be a defect of b, and let $(\mathcal{O}Gb)_\gamma$ be a source algebra of b. Let $\overline{b}$ be the image of b in $kG = \mathcal{O}G/\mathfrak{p}\mathcal{O}G$, and let $\overline{\gamma}$ be the image of the point γ in $(kG)^P$. Then $P_{\overline{\gamma}}$ is a defect of the block $\overline{b}$, and $(kG\overline{b})_{\overline{\gamma}} = (\mathcal{O}Gb)_\gamma/\mathfrak{p}(\mathcal{O}Gb)_\gamma$ is a source algebra of $\overline{b}$.*

Proof. The first statement has already been mentioned in the previous section (Proposition 37.4). The second is an immediate consequence of the first. □

We shall see later in this section that a source algebra of $kG\bar{b}$ determines in fact to a very large extent the structure of a source algebra of $\mathcal{O}Gb$.

We already know that several invariants of a block algebra $\mathcal{O}Gb$ can be detected in a source algebra $(\mathcal{O}Gb)_\gamma$ of b. First of all the poset of local pointed groups on $\mathcal{O}Gb$ is determined up to G-conjugation by the poset of local pointed groups on $(\mathcal{O}Gb)_\gamma$. Indeed if R_ε and Q_δ are local pointed groups on $\mathcal{O}Gb$ such that $R_\varepsilon \leq Q_\delta$, there exists $g \in G$ such that ${}^g(Q_\delta) \leq P_\gamma$, because all maximal local pointed groups are conjugate (Theorem 18.3). Now the embedding $\mathcal{F}_\gamma : (\mathcal{O}Gb)_\gamma \to \mathrm{Res}^G_P(\mathcal{O}Gb)$ induces an isomorphism between the poset of local pointed groups on $(\mathcal{O}Gb)_\gamma$ and the poset of local pointed groups on $\mathcal{O}Gb$ contained in P_γ (Proposition 15.1). Thus the relation ${}^g(R_\varepsilon) \leq {}^g(Q_\delta)$ comes from a containment relation between local pointed groups on the source algebra. A much more precise version of these facts will be proved in Section 47.

By Proposition 18.10, $\mathcal{O}Gb$ and $(\mathcal{O}Gb)_\gamma$ are Morita equivalent, and this implies the following result.

(38.2) PROPOSITION. *Let b be a block of $\mathcal{O}G$, let $(\mathcal{O}Gb)_\gamma$ be a source algebra of b, and let $\bar{b}$ and $\bar{\gamma}$ be the images in kG of b and γ respectively.*

(a) $\mathcal{O}Gb$ and $(\mathcal{O}Gb)_\gamma$ are Morita equivalent.

(b) There is a bijection between $\mathrm{Irr}(\mathcal{O}Gb)$ and $\mathrm{Irr}((\mathcal{O}Gb)_\gamma)$ (that is, between $\mathrm{Irr}(kG\bar{b})$ and $\mathrm{Irr}((kG\bar{b})_{\bar{\gamma}})$), and a bijection between $\mathrm{Proj}(\mathcal{O}Gb)$ and $\mathrm{Proj}((\mathcal{O}Gb)_\gamma)$, induced by the Morita equivalence.

(c) If $\mathcal{O}$ is a domain with field of fractions K, the Morita equivalence induces a Morita equivalence between KGb and $K\otimes_{\mathcal{O}}(\mathcal{O}Gb)_\gamma$, hence a bijection between $\mathrm{Irr}(KGb)$ and $\mathrm{Irr}(K\otimes_{\mathcal{O}}(\mathcal{O}Gb)_\gamma)$.

(d) The Cartan matrices of $kG\bar{b}$ and $(kG\bar{b})_{\bar{\gamma}}$ are equal.

(e) The centres $Z\mathcal{O}Gb$ and $Z(\mathcal{O}Gb)_\gamma$ are isomorphic.

Proof. (a) follows from Proposition 18.10, (b) from Corollary 9.5, (c) from Exercise 9.7, (d) from Corollary 9.6, and (e) from Proposition 9.7. □

It is useful to remember how the Morita equivalence is obtained. Choose $(\mathcal{O}Gb)_\gamma = i\mathcal{O}Gi$ where $i \in \gamma$, and γ is a source point. It follows from the proof of Theorem 9.9 that the Morita equivalence is given by the $(\mathcal{O}Gb, i\mathcal{O}Gi)$-bimodule $\mathcal{O}Gbi = \mathcal{O}Gi$ and the $(i\mathcal{O}Gi, \mathcal{O}Gb)$-bimodule $i\mathcal{O}Gb = i\mathcal{O}G$. Thus the Morita correspondent of an $\mathcal{O}Gb$-module M is equal to $i\mathcal{O}G \otimes_{\mathcal{O}Gb} M \cong iM$, where iM is an $i\mathcal{O}Gi$-module under left multiplication. Since i is fixed under P, we see that iM is a direct summand of $\mathrm{Res}^G_P(M)$. But this gives only the $\mathcal{O}P$-module structure of iM (obtained by restriction via the structural map $\mathcal{O}P \to i\mathcal{O}Gi$). There is more information in the $i\mathcal{O}Gi$-module structure than in its restriction to $\mathcal{O}P$.

Vertices and sources of indecomposable modules belonging to a block b can also be detected from a source algebra of b. Indeed the second statement of the following proposition characterizes vertices and sources of an indecomposable module M belonging to b from the knowledge of the corresponding indecomposable $i\mathcal{O}Gi$-module iM. In fact only the restriction of iM to $\mathcal{O}P$ is used (but this may no longer be indecomposable). Note first that there is an embedding of interior P-algebras $\mathrm{End}_\mathcal{O}(iM) \to \mathrm{Res}^G_P(\mathrm{End}_\mathcal{O}(M))$, so that any pointed group on $\mathrm{End}_\mathcal{O}(iM)$ can be viewed as a pointed group on $\mathrm{End}_\mathcal{O}(M)$ (via the identification of Proposition 15.1). Secondly note that, since the module iM is not necessarily indecomposable on restriction to $\mathcal{O}P$, there might be several P-conjugacy classes of maximal local pointed groups on $\mathrm{End}_\mathcal{O}(iM)$ and it might happen that two of them correspond to subgroups of P of different order.

(38.3) PROPOSITION. *Let $i\mathcal{O}Gi$ be a source algebra of a block b of $\mathcal{O}G$ and let M be an indecomposable $\mathcal{O}Gb$-module.*

(a) For any local pointed group R_ε on $\mathrm{End}_\mathcal{O}(M)$, there exists $x \in G$ such that ${}^x(R_\varepsilon)$ is a pointed group on $\mathrm{End}_\mathcal{O}(iM)$.

(b) Any local pointed group Q_δ on $\mathrm{End}_\mathcal{O}(iM)$ with $|Q|$ maximal is a defect of $\mathrm{End}_\mathcal{O}(M)$.

Proof. (a) Let γ be the point containing i, so that P_γ is a defect of $\mathcal{O}Gb$. The structural homomorphism $\phi : (\mathcal{O}Gb)^R \to \mathrm{End}_\mathcal{O}(M)^R$ maps a primitive decomposition of the unity element b to a (not necessarily primitive) decomposition of id_M. Thus an idempotent e in ε appears in the decomposition of $\phi(j)$ for some primitive idempotent $j \in (\mathcal{O}Gb)^R$. We claim that the point α containing j is local. Indeed if $j \in \sum_{S<R}(\mathcal{O}Gb)^R_S$, then $\phi(j) \in \sum_{S<R} \mathrm{End}_\mathcal{O}(M)^R_S$. Multiplying by e, we deduce that we have $e \in \sum_{S<R} \mathrm{End}_\mathcal{O}(M)^R_S$, which is impossible since ε is local.

The defects of $\mathcal{O}Gb$ are the maximal local pointed groups on $\mathcal{O}Gb$ and are all G-conjugate (Corollary 18.6). Thus there exists $x \in G$ such that ${}^{x}(R_\alpha) \leq P_\gamma$. Changing the choice of $j \in \alpha$, we can assume that ${}^{x}j = i\,{}^{x}j\,i$. Thus $\phi({}^{x}j) = \phi(i)\phi({}^{x}j)\phi(i)$, and so ${}^{x}e = \phi(i)\,{}^{x}e\,\phi(i)$ since ${}^{x}e$ appears in a decomposition of ${}^{x}\phi(j) = \phi({}^{x}j)$. But this means that ${}^{x}e$ belongs to $\phi(i)\,\mathrm{End}_{\mathcal{O}}(M)\phi(i) = \mathrm{End}_{\mathcal{O}}(iM)$ (note that iM stands in fact for $\phi(i)M$). Therefore ${}^{x}\varepsilon$ is a point of $\mathrm{End}_{\mathcal{O}}(iM)^{{}^{x}R}$, as required.

(b) Let Q_δ be a local pointed group on $\mathrm{End}_{\mathcal{O}}(iM)$ with $|Q|$ maximal. Viewing Q_δ as a pointed group on $\mathrm{End}_{\mathcal{O}}(M)$, we have $Q_\delta \leq Q'_{\delta'}$ where $Q'_{\delta'}$ is maximal local (that is, $Q'_{\delta'}$ is a defect of $\mathrm{End}_{\mathcal{O}}(M)$). By (a), some G-conjugate of $Q'_{\delta'}$ is a pointed group on $\mathrm{End}_{\mathcal{O}}(iM)$, and is of course still local. Thus by maximality of $|Q|$, we have $|Q'| \leq |Q|$, forcing the equality $Q_\delta = Q'_{\delta'}$. This proves that Q_δ is a defect of $\mathrm{End}_{\mathcal{O}}(M)$. □

(38.4) COROLLARY. *Let the interior P-algebra $(\mathcal{O}Gb)_\gamma$ be a source algebra of a block b, and let N be an $(\mathcal{O}Gb)_\gamma$-lattice. Then N is a projective $(\mathcal{O}Gb)_\gamma$-module if and only if N is projective on restriction to $\mathcal{O}P$.*

Proof. We can assume that $(\mathcal{O}Gb)_\gamma = i\mathcal{O}Gi$, where $i \in \gamma$. By the Morita equivalence, N is isomorphic to iM for some $\mathcal{O}Gb$-lattice M. We write $\mathrm{Res}_P(iM)$ for the restriction of iM to $\mathcal{O}P$ (via the structural map $\mathcal{O}P \to i\mathcal{O}Gi$). By Proposition 38.2, iM is projective over $i\mathcal{O}Gi$ if and only if M is projective over $\mathcal{O}Gb$ (or equivalently over $\mathcal{O}G$). We can assume that M is indecomposable, so that M has a vertex Q. But since M is an $\mathcal{O}G$-lattice, M is projective if and only if $Q = 1$ (Corollary 17.4). By Proposition 38.3, the requirement $Q = 1$ means that there are no local pointed groups on the P-algebra $\mathrm{End}_{\mathcal{O}}(iM)$, except for $Q = 1$ (for which there is a single local point since $\mathrm{End}_{\mathcal{O}}(iM)$ is a matrix algebra). This in turn means that every indecomposable summand of $\mathrm{Res}_P(iM)$ has vertex 1, or in other words is projective over $\mathcal{O}P$ (Corollary 17.4 again). This completes the proof that M is projective over $\mathcal{O}G$ if and only if $\mathrm{Res}_P(iM)$ is projective over $\mathcal{O}P$. □

One can detect in a source algebra many other important invariants of a block, in particular the generalized decomposition numbers (see Section 43) and the inertial quotient $N_G(P_\gamma)/C_G(P)$ (see Section 47). This is why the concept of source algebra is of fundamental importance. In particular the following conjecture seems to be one of the crucial problems in the subject. Given a finite p-group P and an interior P-algebra B, one says that B is a *source algebra of a block* if there exists a finite group G containing P and a block b of $\mathcal{O}G$ such that P is a defect group of b and B is a source algebra of b. Of course B has to be primitive and have defect group P.

(38.5) CONJECTURE (Puig). *Let P be a finite p-group. There are only finitely many isomorphism classes of interior P-algebras which are source algebras of a block.*

The conjecture has been proved when P is cyclic. It has also been proved in some special cases under some additional hypothesis on the structure of the group G. Moreover we mention here without proof that there is such a finiteness result if one bounds the dimension of source algebras.

(38.6) THEOREM. *Let P be a finite p-group and let n be a positive integer. There are only finitely many isomorphism classes of interior P-algebras of dimension at most n which are source algebras of a block.*

It follows from this theorem that Puig's conjecture is equivalent to the statement that, for a fixed p-group P, any interior P-algebra which is a source algebra of a block has a bounded dimension.

There is a clear analogy between Puig's conjecture and Feit's conjecture 30.7 about sources of simple modules, and also between Theorem 38.6 and Theorem 30.8. Despite the fact that sources of simple modules can be detected in source algebras (by Proposition 38.3), it is not clear whether a positive answer to Puig's conjecture implies a positive answer to Feit's conjecture. Indeed, for a given p-group Q, there might be infinitely many p-groups $P \geq Q$ such that P is a defect group of a block containing a simple module with vertex Q; but Puig's conjecture only implies that, for a given P, there are finitely many possible sources of simple modules.

One of the most useful general facts about source algebras of blocks is that they have invariant bases under the left and right action of the defect group P. Recall that any interior P-algebra A is an $\mathcal{O}P$-module under left multiplication, and also an $\mathcal{O}P$-module under right multiplication. Since both actions of P obviously commute, A can be viewed as a left $\mathcal{O}(P \times P)$-module, by defining the action of $(u, v) \in P \times P$ to be

$$(u, v)\cdot a = u\cdot a\cdot v^{-1}\,, \quad \text{for all } a \in A\,.$$

One needs the inverse of v for a left action. For source algebras, there is the following result, which we state more generally for an arbitrary local pointed group.

(38.7) PROPOSITION. *Let* b *be a block of* $\mathcal{O}G$ *, let* P_γ *be a local pointed group on* $\mathcal{O}Gb$ *, and consider the localization* $(\mathcal{O}Gb)_\gamma$ *(for instance a source algebra of* b *if* P_γ *is a defect of* b *).*

(a) There exists an $\mathcal{O}$*-basis* X *of* $(\mathcal{O}Gb)_\gamma$ *which is invariant under the action of* $P\times P$ *.*

(b) $(\mathcal{O}Gb)_\gamma$ *is free as a left* $\mathcal{O}P$*-module, and also as a right* $\mathcal{O}P$*-module. In other words for any* $x\in X$ *, the left* P*-orbit* $P{\cdot}x$ *has cardinality* $|P|$ *, and similarly* $x{\cdot}P$ *has cardinality* $|P|$ *.*

(c) One can choose a $(P\times P)$*-invariant basis* X *of* $(\mathcal{O}Gb)_\gamma$ *such that* $1_{(\mathcal{O}Gb)_\gamma}\in X$ *.*

Proof. (a) The group algebra $\mathcal{O}G$ is an $\mathcal{O}(G\times G)$-module under left and right multiplication. It is clear that $\mathcal{O}G$ has a $(G\times G)$-invariant basis, namely the basis G itself. One can choose $(\mathcal{O}Gb)_\gamma=i\mathcal{O}Gi$ where $i\in\gamma$, and since i is fixed under P, the direct sum decomposition

$$\mathcal{O}G\,=\,i\mathcal{O}Gi\,\oplus\,i\mathcal{O}G(1-i)\,\oplus\,(1-i)\mathcal{O}Gi\,\oplus\,(1-i)\mathcal{O}G(1-i)$$

is invariant under $P\times P$. Therefore $i\mathcal{O}Gi$ is a direct summand of a permutation $\mathcal{O}(P\times P)$-module. Since $P\times P$ is a p-group, $i\mathcal{O}Gi$ is again a permutation $\mathcal{O}(P\times P)$-module by Corollary 27.2.

(b) First note that $\mathcal{O}G$ is a free $\mathcal{O}P$-module under left multiplication, with an arbitrary set of coset representatives $[P\backslash G]$ as a basis. The above direct sum decomposition shows that $i\mathcal{O}Gi$ is a direct summand of a free $\mathcal{O}P$-module, hence is free again since P is a p-group (Proposition 21.1). Therefore for each $x\in X$, the indecomposable $\mathcal{O}P$-direct summand with $\mathcal{O}$-basis $P{\cdot}x$ must be free of rank one over $\mathcal{O}P$, so that the basis $P{\cdot}x$ must have cardinality $|P|$. The proof for the right action of P is exactly the same.

(c) Consider the conjugation action of P on the basis X of $(\mathcal{O}Gb)_\gamma$, that is, the restriction of the action of $P\times P$ to the diagonal subgroup of $P\times P$. Since the unity element $1=1_{(\mathcal{O}Gb)_\gamma}$ is fixed under this action, it is an $\mathcal{O}$-linear combination of orbit sums

$$1=\sum_{x\in[P\backslash X]}\lambda_x\Big(\sum_{u\in[P/P_x]}{}^u x\Big)\,,$$

where $\lambda_x\in\mathcal{O}$ and where P_x denotes the stabilizer of x. Since $(\mathcal{O}Gb)_\gamma$ is a primitive P-algebra, we have $(\mathcal{O}Gb)_\gamma^P/J((\mathcal{O}Gb)_\gamma^P)\cong k$. But since γ is a local point of $(\mathcal{O}Gb)^P$, the point $\{1\}$ of $(\mathcal{O}Gb)_\gamma^P$ is local (Proposition 15.1), and we still denote it by γ. Therefore the canonical surjection π_γ onto k factorizes through the Brauer homomorphism

$$(\mathcal{O}Gb)_\gamma^P\xrightarrow{\;br_P\;}\overline{(\mathcal{O}Gb)_\gamma}(P)\longrightarrow(\mathcal{O}Gb)_\gamma^P/J((\mathcal{O}Gb)_\gamma^P)\cong k\,.$$

The orbit sum $\sum_{u\in[P/P_x]} {}^u x$ is in the kernel of br_P whenever $P_x < P$. Since $\pi_\gamma(1) = 1_k$, there is at least one basis element y which is fixed under P (that is, $P_y = P$), and such that $\pi_\gamma(\lambda_y y) \neq 0$. Thus $\lambda_y y$ is invertible in $(\mathcal{O}Gb)_\gamma^P$. Also $\lambda_y \in \mathcal{O}^*$ (otherwise $\lambda_y \in \mathfrak{p}$ and $\pi_\gamma(\lambda_y y) = 0$), and therefore y is invertible in $(\mathcal{O}Gb)_\gamma^P$. Now the image of X under left multiplication by y^{-1} is again a basis, and $y^{-1}X$ is still $(P\times P)$-invariant, because y is fixed under conjugation by P, so that

$$(u,v)\cdot y^{-1}x = u\cdot y^{-1}x\cdot v^{-1} = y^{-1}(u\cdot x\cdot v^{-1})\,, \qquad (u,v\in P\,, x\in X)\,.$$

Clearly this new basis contains $y^{-1}y = 1$. □

A more detailed analysis of the $\mathcal{O}(P\times P)$-module structure of a source algebra $(\mathcal{O}Gb)_\gamma$ will be given in Section 44. We now apply Proposition 38.7 to show that the reduction modulo $\mathfrak{p}$ of a source algebra of a block determines to a very large extent this algebra. More precisely the only extra information we need is the existence of a $(P\times P)$-invariant basis. This is analogous to the fact that permutation modules (and more generally p-permutation modules) can be lifted uniquely from k to $\mathcal{O}$ (Proposition 27.11).

(38.8) PROPOSITION. *Let b be a block of $\mathcal{O}G$, let P_γ be a defect of b, let $(\mathcal{O}Gb)_\gamma$ be a source algebra of b, and let $\overline{b}$ and $\overline{\gamma}$ be the images in kG of b and γ respectively. Let B be any interior P-algebra having a $(P\times P)$-invariant $\mathcal{O}$-basis. If $B/\mathfrak{p}B \cong (kG\overline{b})_{\overline{\gamma}}$, then $B \cong (\mathcal{O}Gb)_\gamma$ (as interior P-algebras).*

Proof. We first show that $\mathrm{Ind}_P^G(B)^G \to \mathrm{Ind}_P^G(B/\mathfrak{p}B)^G$ is surjective. Let X be a $(P\times P)$-invariant basis of B. It is easy to check that the set $Y = \{\, g\otimes x\otimes h \mid g,h\in[G/P]\,, x\in X\,\}$ is a basis of $\mathrm{Ind}_P^G(B)$ which is $(P\times P)$-invariant, hence in particular invariant under the conjugation action of P. Thus $\mathrm{Ind}_P^G(B)^P$ has as a basis the set of orbit sums under the conjugation action of P on Y. Therefore $\mathrm{Ind}_P^G(B)^P \to \mathrm{Ind}_P^G(B/\mathfrak{p}B)^P$ is surjective, because it maps this $\mathcal{O}$-basis to the corresponding k-basis. Now there is a commutative diagram

$$\begin{array}{ccc} \mathrm{Ind}_P^G(B)^P & \xrightarrow{\;t_P^G\;} & \mathrm{Ind}_P^G(B)^G \\ \big\downarrow & & \big\downarrow \\ \mathrm{Ind}_P^G(B/\mathfrak{p}B)^P & \xrightarrow{\;t_P^G\;} & \mathrm{Ind}_P^G(B/\mathfrak{p}B)^G \end{array}$$

and t_P^G is surjective by the construction of induction (because we have $1_{\mathrm{Ind}_P^G(B)} = t_P^G(1\otimes 1_B\otimes 1)$). It follows that $\mathrm{Ind}_P^G(B)^G \to \mathrm{Ind}_P^G(B/\mathfrak{p}B)^G$ is surjective.

Let $\mathcal{F}_{\overline{\gamma}} : (kG\bar{b})_{\overline{\gamma}} \to \mathrm{Res}^G_P(kG\bar{b})$ be an embedding associated with $\overline{\gamma}$. By Theorem 17.9, there exists an embedding $\overline{\mathcal{H}} : kG\bar{b} \to \mathrm{Ind}^G_P((kG\bar{b})_{\overline{\gamma}})$ such that $\mathrm{Res}^G_P(\overline{\mathcal{H}})\,\mathcal{F}_{\overline{\gamma}} = \mathcal{D}^G_P$, where $\mathcal{D}^G_P$ denotes the canonical embedding $\mathcal{D}^G_P : (kG\bar{b})_{\overline{\gamma}} \to \mathrm{Res}^G_P \mathrm{Ind}^G_P((kG\bar{b})_{\overline{\gamma}})$. We want to prove that $\overline{\mathcal{H}}$ can be lifted to an embedding $\mathcal{H} : \mathcal{O}Gb \to \mathrm{Ind}^G_P(B)$ such that the following diagram commutes.

$$\text{(38.9)}\qquad \begin{array}{ccccc} \mathcal{O}Gb & & \xrightarrow{\quad\mathcal{H}\quad} & & \mathrm{Ind}^G_P(B) \\ \downarrow & & & & \downarrow \\ kG\bar{b} & \xrightarrow{\overline{\mathcal{H}}} & \mathrm{Ind}^G_P((kG\bar{b})_{\overline{\gamma}}) & \cong & \mathrm{Ind}^G_P(B/\mathfrak{p}B) \end{array}$$

Let $\overline{h} \in \overline{\mathcal{H}}$ and let $\overline{e} = \overline{h}(\bar{b})$, so that we have an isomorphism of algebras $\overline{h} : kG\bar{b} \xrightarrow{\sim} \overline{e}\ \mathrm{Ind}^G_P(B/\mathfrak{p}B)\,\overline{e}$. Since $\mathrm{Ind}^G_P(B)^G \to \mathrm{Ind}^G_P(B/\mathfrak{p}B)^G$ is surjective, $\overline{e}$ lifts to a primitive idempotent $e \in \mathrm{Ind}^G_P(B)^G$ (by Theorem 3.1), and there is a commutative diagram

$$\begin{array}{ccc} \mathcal{O}G & \xrightarrow{\ j\ } & e\ \mathrm{Ind}^G_P(B)\,e \\ \downarrow & & \downarrow \\ kG & \xrightarrow{\ \overline{j}\ } & \overline{e}\ \mathrm{Ind}^G_P(B/\mathfrak{p}B)\,\overline{e} \end{array}$$

where both horizontal maps are the structural homomorphisms. Now let $q : kG \to kG\bar{b}$, $a \mapsto a\bar{b}$, be the surjection onto the block algebra $kG\bar{b}$. The composite $\overline{h}q : kG \to \overline{e}\ \mathrm{Ind}^G_P(B/\mathfrak{p}B)\,\overline{e}$ is a unitary homomorphism of interior G-algebras and is therefore equal to the structural homomorphism $\overline{j}$ (by uniqueness of $\overline{j}$, see Exercise 12.2). Since $q(\overline{b}') = 0$ for any block $b' \neq b$, we have $\overline{j}(\overline{b}') = 0$. Therefore $j(b') = 0$ because $j(b')$ is an idempotent of $e\,\mathrm{Ind}^G_P(B)e$ which is mapped to zero modulo $\mathfrak{p}$. Thus the map j induces a homomorphism $h : \mathcal{O}Gb \to e\,\mathrm{Ind}^G_P(B)e$. The reduction of h modulo $\mathfrak{p}$ is the isomorphism $\overline{h} : kG\bar{b} \xrightarrow{\sim} \overline{e}\,\mathrm{Ind}^G_P(B/\mathfrak{p}B)\overline{e}$. Therefore h is an isomorphism too since both algebras are free $\mathcal{O}$-modules (Proposition 1.3). In other words h defines an embedding $\mathcal{H} : \mathcal{O}Gb \to \mathrm{Ind}^G_P(B)$ such that the diagram 38.9 commutes.

Now let $\mathcal{F}_\gamma : (\mathcal{O}Gb)_\gamma \to \mathrm{Res}^G_P(\mathcal{O}Gb)$ be an embedding associated with γ, lifting the embedding $\mathcal{F}_{\overline{\gamma}}$ associated with $\overline{\gamma}$. The diagram 38.9 can be completed into a commutative diagram

$$\begin{array}{ccccccc} & & (\mathcal{O}Gb)_\gamma & \xrightarrow{\mathcal{F}_\gamma} & \mathrm{Res}^G_P(\mathcal{O}Gb) & \xrightarrow{\mathrm{Res}^G_P(\mathcal{H})} & \mathrm{Res}^G_P\,\mathrm{Ind}^G_P(B) \\ & & \downarrow & & \downarrow & & \downarrow \\ B/\mathfrak{p}B & \cong & (kG\bar{b})_{\overline{\gamma}} & \xrightarrow{\mathcal{F}_{\overline{\gamma}}} & \mathrm{Res}^G_P(kG\bar{b}) & \xrightarrow{\mathrm{Res}^G_P(\overline{\mathcal{H}})} & \mathrm{Res}^G_P\,\mathrm{Ind}^G_P(B/\mathfrak{p}B) \end{array}$$

and the composite map in the second row is the canonical embedding $\mathcal{D}_P^G$. Let δ denote the point of $\mathrm{Ind}_P^G(B)^P$ containing $1 \otimes 1_B \otimes 1$ and let $\overline{\delta} \in \mathcal{P}(\mathrm{Ind}_P^G(B/\mathfrak{p}B)^P)$ be its image. By definition of the canonical embedding $\mathcal{D}_P^G$, the image of the point $\overline{\gamma}$ in $\mathrm{Ind}_P^G(B/\mathfrak{p}B)^P$ is the point $\overline{\delta}$, and therefore the image of γ in $\mathrm{Ind}_P^G(B)^P$ is equal to δ. Since $(\mathcal{O}Gb)_\gamma$ is a primitive P-algebra, this proves that the composite embedding in the top row of the above diagram is an embedding associated with δ. But now the canonical embedding $B \to \mathrm{Res}_P^G \mathrm{Ind}_P^G(B)$ is also associated with δ. Therefore, by Lemma 13.1, the two interior P-algebras $(\mathcal{O}Gb)_\gamma$ and B are isomorphic, as was to be shown. □

Another useful piece of information about source algebras is concerned with the Brauer quotient. Recall that if B is an interior P-algebra, then the centre $Z(P)$ maps to $(B^P)^*$ via the structural map $u \mapsto u{\cdot}1_B$.

(38.10) PROPOSITION. *Let P_γ be a defect of a block b of $\mathcal{O}G$ and let the interior P-algebra $(\mathcal{O}Gb)_\gamma$ be a source algebra of b. Then the structural group homomorphism $Z(P) \to ((\mathcal{O}Gb)_\gamma^P)^*$ induces an isomorphism of k-algebras $kZ(P) \xrightarrow{\sim} \overline{(\mathcal{O}Gb)_\gamma}(P)$.*

Proof. By Exercise 12.4, the embedding $\mathcal{F}_\gamma : (\mathcal{O}Gb)_\gamma \to \mathrm{Res}_P^G(\mathcal{O}Gb)$ induces an embedding

$$\overline{\mathcal{F}_\gamma}(P) : \overline{(\mathcal{O}Gb)_\gamma}(P) \longrightarrow \overline{\mathcal{O}Gb}(P) = kC_G(P)\, br_P(b)\,,$$

which can be described explicitly as follows. Choose $(\mathcal{O}Gb)_\gamma = i\mathcal{O}Gi$, where $i \in \gamma$, and let $\mathcal{F}_\gamma$ contain the inclusion $i\mathcal{O}Gi \to \mathcal{O}Gb$. Then $\overline{\mathcal{F}_\gamma}(P)$ contains the inclusion $br_P(i)\, kC_G(P)\, br_P(i) \to kC_G(P)$. In other words $br_P(i)$ is a primitive idempotent of $kC_G(P)$ (note that it is non-zero because γ is local), and $\overline{(\mathcal{O}Gb)_\gamma}(P) \cong br_P(i)\, kC_G(P)\, br_P(i)$.

Let $\overline{C}_G(P) = C_G(P)/Z(P)$. Clearly $kC_G(P)$ is a free $kZ(P)$-module with basis $[C_G(P)/Z(P)]$, and $k\overline{C}_G(P)$ is a trivial $kZ(P)$-module (with k-basis $\overline{C}_G(P)$). Since the free $kZ(P)$-module of rank one is indecomposable (Proposition 21.1), it is the projective cover of the trivial module k. Therefore the surjection of $kZ(P)$-modules $kC_G(P) \to k\overline{C}_G(P)$ is necessarily a projective cover (isomorphic to the direct sum of $|\overline{C}_G(P)|$ copies of $kZ(P) \to k$).

Let $j = br_P(i)$ and let $\overline{j}$ be the image of j in $k\overline{C}_G(P)$. Since i is fixed under $Z(P)$ (because it is fixed under P), its image j commutes with the left action of $Z(P)$. Therefore, if we write $A = kC_G(P)$, there is a $Z(P)$-invariant direct sum decomposition

$$A = jAj \,\oplus\, jA(1-j) \,\oplus\, (1-j)Aj \,\oplus\, (1-j)A(1-j)\,.$$

Thus $jkC_G(P)j$ is a direct summand of $kC_G(P)$ as a $kZ(P)$-module, and the surjection of $kZ(P)$-modules $jkC_G(P)j \to \overline{j}k\overline{C}_G(P)\overline{j}$ is a direct summand of $kC_G(P) \to k\overline{C}_G(P)$, hence a projective cover again. In particular $jkC_G(P)j$ is a free $kZ(P)$-module. Moreover $\overline{j}k\overline{C}_G(P)\overline{j}$ has dimension r over k if $jkC_G(P)j$ is free of rank r over $kZ(P)$.

Since $jkC_G(P)j$ is free as a module over $kZ(P)$, the structural map $kZ(P) \to jkC_G(P)j$ (given by $u \mapsto u{\cdot}j$) is injective. We claim that it is surjective too, so that $kZ(P) \cong jkC_G(P)j$, as required. For reasons of dimension, it suffices to prove that $jkC_G(P)j$ is free of rank one over $kZ(P)$, and this in turn will follow if we prove that $\overline{j}k\overline{C}_G(P)\overline{j}$ is one-dimensional.

Since j is primitive, the $kC_G(P)$-module $kC_G(P)j$ is indecomposable projective, and its unique simple quotient is the multiplicity module $V(\gamma)$. But as $Z(P)$ is a p-group, the kernel of $kC_G(P) \to k\overline{C}_G(P)$ is contained in $J(kC_G(P))$ by Corollary 21.2, and therefore the image $\overline{j}$ is non-zero and primitive in $k\overline{C}_G(P)$. It follows that $k\overline{C}_G(P)\overline{j}$ is an indecomposable projective $k\overline{C}_G(P)$-module, and $k\overline{C}_G(P)\overline{j}/J(k\overline{C}_G(P))\overline{j}$ is its unique simple quotient. The sequence of surjections

$$kC_G(P)j \longrightarrow k\overline{C}_G(P)\overline{j} \longrightarrow k\overline{C}_G(P)\overline{j}/J(k\overline{C}_G(P))\overline{j}$$

shows that $k\overline{C}_G(P)\overline{j}/J(k\overline{C}_G(P))\overline{j}$, viewed as a $kC_G(P)$-module, is a simple quotient of $kC_G(P)j$, hence is isomorphic to $V(\gamma)$. By Theorem 37.9, we know that $V(\gamma)$ is projective as a module over $k\overline{C}_G(P)$ (and this is where we use the fact that P_γ is a defect of the block b). Thus the simple module $V(\gamma) \cong k\overline{C}_G(P)\overline{j}/J(k\overline{C}_G(P))\overline{j}$ coincides with its projective cover $k\overline{C}_G(P)\overline{j}$ (as modules over $k\overline{C}_G(P)$). Therefore by Schur's lemma, $\mathrm{End}_{k\overline{C}_G(P)}(k\overline{C}_G(P)\overline{j}) \cong k$. But $\mathrm{End}_{k\overline{C}_G(P)}(k\overline{C}_G(P)\overline{j}) \cong (\overline{j}k\overline{C}_G(P)\overline{j})^{op}$ by Proposition 5.11, and this completes the proof that $\overline{j}k\overline{C}_G(P)\overline{j}$ is one-dimensional. □

This result will be used in the next section, where we shall determine the structure of a source algebra in the easiest case of block theory, namely when the block has a central defect group.

Exercises

(38.1) Vertices and sources of indecomposable diagrams belonging to a block b can be detected from a source algebra of b. State and prove this in detail, as in Proposition 38.3. Deduce that defect groups and source algebras of arbitrary primitive interior G-algebras associated with b can be computed from a source algebra of b.

(38.2) Let the interior P-algebra $(\mathcal{O}Gb)_\gamma$ be a source algebra of a block b of $\mathcal{O}G$. Prove that the structural map $P \to (\mathcal{O}Gb)_\gamma^*$ is injective. [Hint: Use Proposition 38.7.]

Notes on Section 38

The concept of source algebra is due to Puig [1981], who also proved all their main properties, in Puig [1981, 1982, 1986, 1988a, 1988b]. Puig's finiteness conjecture 38.5 appears in Puig [1982]. The finiteness theorem 38.6 is also due to Puig [1982]. For the case where P is cyclic, all possible source algebras were described by Linckelmann [1993], using earlier deep results of Dade and Green, and in particular Puig's conjecture is proved in that case. If P is the Klein four group, all possible source algebras were described by Linckelmann [1994], using earlier results of Erdmann, but Puig's conjecture is still open in that case because it is not clear whether or not Linckelmann's list is finite. Puig's conjecture has also been proved under additional assumptions on the type of group G (for instance if G is p-soluble or if G is a symmetric group, see Puig [1994b]). For certain blocks of Chevalley groups, the source algebras were described by Puig [1990b].

§ 39 BLOCKS WITH A CENTRAL DEFECT GROUP

In this section we discuss the structure of blocks with a central defect group, and in particular blocks with a trivial defect group. We show that these blocks have a unique simple module and we determine the structure of a source algebra.

We first discuss the case of blocks with a trivial defect group, called blocks of *defect zero*. Indeed a traditional terminology says that the integer d is a defect of a block b if the order of a defect group of b is p^d . The case $d = 0$ corresponds to a trivial defect group.

(39.1) THEOREM. *Let b be a block of $\mathcal{O}G$ and let $\bar{b}$ be the image of b in kG . The following conditions are equivalent.*

(a) b is a block of defect zero.

(b) There is a unique simple $\mathcal{O}Gb$-module V (up to isomorphism), and V is projective as a module over $kG\bar{b}$.

(c) There exists a simple $\mathcal{O}Gb$-module which is projective as a module over $kG\bar{b}$.

(d) The block algebra $kG\bar{b}$ is simple.

(e) The block algebra $\mathcal{O}Gb$ is $\mathcal{O}$-simple.

(f) Viewed as an $\mathcal{O}$-algebra, a source algebra of $\mathcal{O}Gb$ is isomorphic to $\mathcal{O}$.

Proof. We first prove the equivalence of (b), (c), and (d). It is clear that (b) implies (c), and that (d) implies (b).

(c) ⇒ (d). Let V be a simple projective $kG\bar{b}$-module. Since kG is a symmetric algebra (Example 6.2), every projective kG-module is injective (Proposition 6.7). Thus V is also injective and the assumptions of Corollary 5.14 are satisfied. It follows that $kG\bar{b}$ is a simple k-algebra, using also the fact that $kG\bar{b}$ has no non-trivial central idempotent (because $\bar{b}$ is primitive in ZkG).

(a) ⇒ (d). Since the trivial subgroup 1 is a defect group of b, every $\mathcal{O}Gb$-module is projective relative to 1 by Proposition 37.3. By Higman's criterion (Corollary 17.4), this implies that every $\mathcal{O}Gb$-lattice is projective, and similarly every $kG\bar{b}$-module is projective. Therefore every $kG\bar{b}$-module is semi-simple (because the projectivity of simple modules implies semi-simplicity), and so $kG\bar{b}$ is a semi-simple k-algebra. In particular the centre $Z(kG\bar{b})$ is isomorphic to a direct product of copies of k. But since $\bar{b}$ is a primitive idempotent of the centre of kG (Lemma 37.1), there is a single factor in the direct product. Thus $kG\bar{b}$ is a simple k-algebra.

(d) ⇒ (e). This follows from Exercise 7.6.

(e) ⇒ (f). By assumption $\mathcal{O}Gb \cong \mathrm{End}_{\mathcal{O}}(M)$ as an $\mathcal{O}$-algebra, where M is some $\mathcal{O}$-lattice. But then the image of G in $\mathrm{End}_{\mathcal{O}}(M)$ makes M into an $\mathcal{O}G$-lattice belonging to b, and by construction the isomorphism $\mathcal{O}Gb \cong \mathrm{End}_{\mathcal{O}}(M)$ is an isomorphism of interior G-algebras. Since M is an indecomposable projective $\mathrm{End}_{\mathcal{O}}(M)$-module (Lemma 7.1), M is a projective $\mathcal{O}Gb$-module, hence a projective $\mathcal{O}G$-module. By Higman's criterion (Corollary 17.4), the trivial group is a defect group of the primitive G-algebra $\mathrm{End}_{\mathcal{O}}(M)$, that is, a vertex of M. Then the $\mathcal{O}$-lattice $\mathcal{O}$ is a source of M (because it is the only indecomposable $\mathcal{O}$-lattice up to isomorphism), and therefore a source algebra of $\mathrm{End}_{\mathcal{O}}(M)$ is $\mathrm{End}_{\mathcal{O}}(\mathcal{O}) \cong \mathcal{O}$.

(f) ⇒ (a). Let P be a defect group of b. Since a source algebra of b is a free $\mathcal{O}P$-module under left multiplication (Proposition 38.7), its dimension as a free $\mathcal{O}$-module is a multiple of $|P|$. Thus if the one-dimensional algebra $\mathcal{O}$ is a source algebra of b, then P must be trivial. □

Part (f) shows that there is just one possible source algebra for a block of defect zero, namely the trivial $\mathcal{O}$-algebra $\mathcal{O}$. This proves Puig's conjecture 38.5 when the defect group P is the trivial group.

In Section 42, we shall characterize blocks of defect zero from information coming from the ordinary representation theory in characteristic zero.

There is a connection between self-centralizing local pointed groups and blocks of defect zero. By Lemma 37.8, a local pointed group Q_δ on $\mathcal{O}G$ is self-centralizing if and only if the multiplicity module $V(\delta)$ is a projective simple $k\overline{C}_G(Q)$-module. In that case, by part (c) of Theorem 39.1, $V(\delta)$ belongs to a block of defect zero of $k\overline{C}_G(Q)$. Conversely a block of defect zero of $k\overline{C}_G(Q)$ has a unique simple module, which is projective, and the corresponding local pointed group Q_δ on $\mathcal{O}G$ is self-centralizing. Thus self-centralizing local pointed groups Q_δ correspond precisely to blocks of defect zero of $k\overline{C}_G(Q)$. We shall return on this in Section 41.

In particular if P_γ is a defect of a block b of $\mathcal{O}G$, then P_γ is self-centralizing, with the additional condition that $|\overline{N}_G(P_\gamma) : \overline{C}_G(P)|$ is prime to p (Theorem 37.9). Therefore the bijection in Brauer's first main Theorem 37.12 can be reinterpreted as a bijection between the set of all blocks of $\mathcal{O}G$ with defect group P and the set of all $\overline{N}_G(P)$-conjugacy classes of blocks of defect zero of $k\overline{C}_G(P)$ having an inertial subgroup I in $\overline{N}_G(P)$ such that $|I/\overline{C}_G(P)|$ is prime to p . Here the *inertial subgroup* of a block e of defect zero of $k\overline{C}_G(P)$ is the inertial subgroup of the unique simple module in this block, but it can also be defined directly as the stabilizer of e under the conjugation action of $\overline{N}_G(P)$ on $k\overline{C}_G(P)$ (Exercise 39.2).

For any p-subgroup P of G , the blocks of defect zero of $k\overline{C}_G(P)$ can in fact be lifted to blocks of $kC_G(P)$ with defect group $Z(P)$, and also to blocks of $kPC_G(P)$ with defect group P . Instead of proving this for the central p-subgroup $Z(P)$ of $C_G(P)$, we state the result for an arbitrary central p-subgroup. The result gives the first basic information about blocks with a central defect group.

(39.2) PROPOSITION. *Let P be a central p-subgroup of G .*

(a) *The canonical surjection $G \to \overline{G} = G/P$ induces a bijection between the set of all blocks of $\mathcal{O}G$ with defect group P and the set of all blocks of defect zero of $\mathcal{O}\overline{G}$.*

(b) *If b is a block of $\mathcal{O}G$ with defect group P and if $\overline{b}$ is its image in $\mathcal{O}\overline{G}$, then there is a unique simple $\mathcal{O}Gb$-module V up to isomorphism. Viewed as a $k\overline{G}\overline{b}$-module, V is projective, and it is isomorphic to the defect multiplicity module of b .*

Proof. Since there is a defect-preserving bijection between blocks of $\mathcal{O}G$ and blocks of kG , we can work over k . The map $G \to \overline{G}$ induces an algebra homomorphism $ZkG \to Zk\overline{G}$ (because the image of a central element under a surjection is central). We note that this homomorphism need not be surjective (the quaternion group of order 8 is an example in characteristic 2), so we consider the surjection of ZkG onto its image $B \subseteq Zk\overline{G}$. Its kernel is nilpotent by Corollary 21.2.

Since P is central, $(kG)^P = kG$ maps surjectively onto $k\overline{G}$, and therefore

$$(kG)_P^G \longrightarrow (k\overline{G})_1^{\overline{G}}$$

is surjective. Thus the ideal $(k\overline{G})_1^{\overline{G}}$ of $Zk\overline{G}$ is contained in B. By part (f) of Theorem 3.2, and since ZkG is commutative, the surjection $ZkG \to B$ induces a bijection between the primitive idempotents of ZkG lying in $(kG)_P^G$ and those of B lying in $(k\overline{G})_1^{\overline{G}}$. The primitive idempotents in $(k\overline{G})_1^{\overline{G}}$ are exactly the blocks of $k\overline{G}$ with trivial defect group, that is, the blocks of defect zero. This uses the fact that an idempotent $e \in (k\overline{G})_1^{\overline{G}}$ is primitive in B if and only if it is primitive in $Zk\overline{G}$ (because any decomposition of e lies entirely in the ideal $(k\overline{G})_1^{\overline{G}}$).

We prove now that the primitive idempotents of $(kG)_P^G$ are exactly the blocks of kG with defect group P, and this will complete the proof of (a). If b is a block of kG with defect group P, then $b \in (kG)_P^G$. If conversely $b \in (kG)_P^G$, then b is projective relative to P, so that a defect group Q of b is contained in P. But if R is a proper subgroup of P, then t_R^P is the zero map, because it is multiplication by $|P:R|$ since P is central. Therefore $t_R^G = 0$ and $b \notin (kG)_R^G$ for every proper subgroup R of P. Thus $Q = P$ as required.

Finally we prove (b), and again it suffices to work over k. Since $\overline{b}$ is a block of defect zero of $k\overline{G}$, we have $k\overline{G}\overline{b} \cong \mathrm{End}_k(V)$, where V is the unique simple module belonging to $\overline{b}$, and V is a projective $k\overline{G}$-module (Theorem 39.1). Since the surjection $kGb \to k\overline{G}\overline{b}$ has a nilpotent kernel (Corollary 21.2), $\mathrm{End}_k(V)$ is the unique simple quotient of kGb, so that V is the unique simple kGb-module up to isomorphism. Moreover since $(kGb)^P = kGb$, the simple algebra $\mathrm{End}_k(V)$ is also the unique simple quotient of $(kGb)^P$, corresponding to a point γ. Since P is a defect group of b, the unique point γ of $(kGb)^P$ must be a source point of b (or alternatively, γ is local because $t_R^P = 0$ if $R < P$). It follows that P_γ is a defect of b and that $V = V_\gamma$ is a defect multiplicity module of b. □

In fact the bijection of Proposition 39.2 is a special case of the bijection in Brauer's first main Theorem 37.12 (Exercise 39.3).

(39.3) COROLLARY. *Let P be a p-subgroup of G.*

(a) The canonical surjection $C_G(P) \to \overline{C}_G(P) = C_G(P)/Z(P)$ induces a bijection between the set of all blocks of $\mathcal{O}C_G(P)$ with defect group $Z(P)$ and the set of all blocks of defect zero of $\mathcal{O}\overline{C}_G(P)$. Moreover the image of a block b of $\mathcal{O}C_G(P)$ with defect group $Z(P)$ is the unique block of $\mathcal{O}\overline{C}_G(P)$ containing the defect multiplicity module of b.

(b) The canonical surjection $PC_G(P) \to \overline{C}_G(P) = PC_G(P)/P$ induces a bijection between the set of all blocks of $\mathcal{O}PC_G(P)$ with defect group P and the set of all blocks of defect zero of $\mathcal{O}\overline{C}_G(P)$. Moreover the image of a block b of $\mathcal{O}PC_G(P)$ with defect group P is the unique block of $\mathcal{O}\overline{C}_G(P)$ containing the defect multiplicity module of b.

Proof. (a) This is immediate by Proposition 39.2, because $Z(P)$ is central in $C_G(P)$.

(b) This follows from (a) and Exercise 37.8. Details are left as an exercise for the reader. □

In our next result, we determine the structure of a source algebra of a block with a central defect group.

(39.4) THEOREM. *Let b be a block of $\mathcal{O}G$ with defect P_γ and let $(\mathcal{O}Gb)_\gamma$ be a source algebra of b. If P is a central subgroup of G, then $(\mathcal{O}Gb)_\gamma$ is isomorphic to $\mathcal{O}P$ (as interior P-algebras).*

Proof. Since $\mathcal{O}P$ has a $(P \times P)$-invariant basis, it suffices by Proposition 38.8 to show that kP is a source algebra of $\overline{b}$, where $\overline{b}$ is the image of b in kG. Thus we assume that $\mathcal{O} = k$. Since P is central, $(kG)^P = kG$ and $\overline{kG}(P) = kC_G(P) = kG$, so that $br_P = id$ and $\overline{kGb}(P) = kC_G(P)br_P(b) = kGb$. It follows that the embedding $\mathcal{F}_\gamma : (kGb)_\gamma \to \mathrm{Res}_P^G(kGb)$ coincides with the induced embedding

$$\overline{\mathcal{F}_\gamma}(P) : \overline{(kGb)_\gamma}(P) \longrightarrow \overline{kGb}(P) = kGb$$

(see the beginning of the proof of Proposition 38.10). Therefore we have $(kGb)_\gamma = \overline{(kGb)_\gamma}(P)$. This is isomorphic to kP by Proposition 38.10. □

In Section 45, we shall generalize this result and determine the structure of a source algebra of a block with a normal defect group.

Note that the algebra $\mathcal{O}P$ has a unique simple module up to isomorphism, namely the trivial module (Proposition 21.1). Therefore, by the Morita equivalence between a block algebra and its source algebra, the block algebra of a block b with central defect group has a unique simple module up to isomorphism. This was already proved in a different way in Proposition 39.2. The computation of generalized decomposition numbers of such blocks will be given in Section 43.

Theorem 39.4 applies in particular when the defect group is trivial, in which case a source algebra is isomorphic to $\mathcal{O}$. Thus we recover a result proved in part (f) of Theorem 39.1.

Exercises

(39.1) Suppose that G has a non-trivial normal p-subgroup P. Prove that $\mathcal{O}G$ has no block of defect zero. [Hint: Use Exercise 37.8.]

(39.2) Let H be a normal subgroup of G, let b be a block of defect zero of $\mathcal{O}H$, and let V be the unique simple module in b. Prove that the stabilizer of b under the conjugation action of G on H is equal to the inertial subgroup of V.

(39.3) Prove that the bijection of Proposition 39.2 is a special case of the bijection in Brauer's first main Theorem 37.12.

(39.4) Provide the details of the proof of Corollary 39.3.

(39.5) Let b be a block of $\mathcal{O}G$ with defect P_γ and assume that P is a central subgroup of G.

(a) Prove that $\mathcal{O}Gb \cong S \otimes_{\mathcal{O}} \mathcal{O}P$ as $\mathcal{O}$-algebras, for some $\mathcal{O}$-simple $\mathcal{O}$-algebra S. [Hint: Take for S an $\mathcal{O}$-simple lift of the unique simple quotient of $\mathcal{O}Gb$ and apply Proposition 7.5. Prove that a source algebra of b is $C_{\mathcal{O}Gb}(S) \cong i\mathcal{O}Gbi$, where $i \in \gamma$.]

(b) Prove that $\mathcal{O}Gb$ is isomorphic to $(\mathcal{O}Gb)_\gamma$ (hence to $\mathcal{O}P$) if and only if the unique simple $\mathcal{O}Gb$-module has dimension one over k. Show that this can occur only if P is a Sylow p-subgroup of G.

Notes on Section 39

The first theorem and proposition of this section are classical results of Brauer. More generally, there are classical results about blocks and normal subgroups which can be found in many textbooks (see Feit [1982], Landrock [1983], Benson [1991]). The determination of the source algebra of a block with a central defect group is due to Puig [1988a]. In fact Puig treats the more general case of a normal defect group, which we shall analyse in Section 45. Blocks with a central defect group are examples of nilpotent blocks, considered in Chapter 7.

§ 40 BRAUER PAIRS

The poset of local pointed groups on $\mathcal{O}G$ is a refinement of another poset, whose elements are the Brauer pairs. These pairs involve blocks of centralizers of p-subgroups and have remarkable properties, which we now discuss.

A *Brauer pair* of G (also called a *subpair* in analogy with subgroups) is a pair (P,e) where P is a p-subgroup of G and e is a block of $kC_G(P)$. Since the blocks of $\mathcal{O}C_G(P)$ are in bijection with those of $kC_G(P)$ (Proposition 37.4), we can always lift e to a block of $\mathcal{O}C_G(P)$, but it will be technically more convenient to work with blocks defined over k. The group G acts by conjugation on the set of Brauer pairs: if (P,e) is a Brauer pair and $g \in G$, then ${}^g e$ is a block of $C_G({}^gP) = {}^g(C_G(P))$ and we define ${}^g(P,e) = ({}^gP, {}^ge)$. The stabilizer of (P,e) is also called the *inertial subgroup* of the block e of $C_G(P)$. It is the set of all $g \in N_G(P)$ such that ${}^ge = e$. This is a subgroup containing $PC_G(P)$, and written $N_G(P,e)$.

We first explain the connection between the notion of Brauer pair and that of local pointed group on $\mathcal{O}G$. By Corollary 37.6, we know that the Brauer homomorphism br_P induces a bijection between $\mathcal{LP}((\mathcal{O}G)^P)$ and $\mathcal{P}(kC_G(P)) \cong \mathrm{Irr}(kC_G(P))$. Explicitly the irreducible representation of $kC_G(P)$ corresponding to a local pointed group P_γ is the multiplicity module $V(\gamma)$. Now any irreducible representation of $kC_G(P)$ is associated with a block of $kC_G(P)$, so that the blocks of $kC_G(P)$ define a partition of $\mathrm{Irr}(kC_G(P))$, hence also of $\mathcal{LP}((\mathcal{O}G)^P)$. We say that a local pointed group P_γ is *associated* with the block e of $kC_G(P)$ if $V(\gamma)$ belongs to e. We also say that P_γ is associated with the Brauer pair (P,e). Since $V(\gamma)$ is the simple $kC_G(P)$-module corresponding to the point $br_P(\gamma)$, this is equivalent to requiring that $br_P(i)e = br_P(i)$ for some $i \in \gamma$ (or equivalently for every $i \in \gamma$). In this situation we also say that the primitive idempotent i is associated with e. This discussion shows that the idempotent e, which is primitive in $Z(kC_G(P))$, decomposes in $kC_G(P)$ as a sum of primitive idempotents belonging to the points $br_P(\gamma)$, where P_γ runs over the set of local pointed groups associated with e. Thus the set of Brauer pairs partition the set of local pointed groups: to each Brauer pair (P,e) corresponds the set of all local pointed groups P_γ associated with (P,e). It is clear that if P_γ is associated with (P,e) and $g \in G$, then ${}^g(P_\gamma)$ is associated with ${}^g(P,e)$.

We say that a Brauer pair (Q,f) is *contained in* a Brauer pair (P,e), and we write $(Q,f) \leq (P,e)$, if there exists a local pointed group P_γ associated with e and a local pointed group Q_δ associated with f such that $Q_\delta \leq P_\gamma$. It is clear that the relation is reflexive (that is, we have $(P,e) \leq (P,e)$). It is antisymmetric because if $Q_\delta \leq P_\gamma$ and $P_{\gamma'} \leq Q_{\delta'}$, with P_γ, $P_{\gamma'}$ associated with e and Q_δ, $Q_{\delta'}$ associated with f, then

$P = Q$, and so $\gamma = \delta$, forcing the equality $e = f$. It is not obvious that the relation is also transitive. This will follow from the main theorem below, which asserts that for *every* local pointed group P_γ associated with e, *all* the local pointed groups Q_δ with $Q_\delta \leq P_\gamma$ are associated with the same Brauer pair (Q, f). We first note that this much stronger property can be expressed by the following equations. For simplicity of notation, we write $br_Q(\gamma)$ instead of $br_Q\, r_Q^P(\gamma)$.

(40.1) LEMMA. *Let (P, e) and (Q, f) be two Brauer pairs of G and let P_γ be a local pointed group on $\mathcal{O}G$ associated with e. The following conditions are equivalent.*

(a) Every local pointed group Q_δ with $Q_\delta \leq P_\gamma$ is associated with f.

(b) $br_Q(\gamma)f = br_Q(\gamma)$.

(c) $br_Q(i)f = br_Q(i)$ for some $i \in \gamma$.

Proof. The equivalence between (b) and (c) follows from the fact that f is central in $kC_G(Q)$. Indeed if $br_Q(i)f = br_Q(i)$ and if $a \in (\mathcal{O}G)^P$ is invertible, then

$$br_Q({}^a i)f = br_Q(a)br_Q(i)f\,br_Q(a)^{-1} = br_Q(a)br_Q(i)br_Q(a)^{-1} = br_Q({}^a i),$$

so that $br_Q(i')f = br_Q(i')$ for every $i' \in \gamma$. It is easy to see that this property is equivalent to the equality of sets $br_Q(\gamma)f = br_Q(\gamma)$, using the fact that a primitive idempotent $j \in kC_G(Q)$ satisfies either $jf = j$ or $jf = 0$.

For the equivalence between (a) and (c), we choose $i \in \gamma$ and we first note that the primitive idempotents appearing in a decomposition of $r_Q^P(i)$ lie exactly in the points $\delta \in \mathcal{P}((\mathcal{O}G)^Q)$ such that $Q_\delta \leq P_\gamma$. If δ is not local, then it is mapped to zero under br_Q, and therefore the primitive idempotents appearing in a decomposition of $br_Q(i)$ lie precisely in the points $br_Q(\delta) \in \mathcal{P}(kC_G(Q))$ such that Q_δ is local and $Q_\delta \leq P_\gamma$. Statement (c) says that every primitive idempotent appearing in a decomposition of $br_Q(i)$ is associated with f. By the above remarks, this is equivalent to condition (a). □

For simplicity of notation we shall not write the inclusion maps r_Q^P throughout this section. Thus $br_Q(i)$ has to be understood as being $br_Q\, r_Q^P(i)$, as in the above lemma. A thorough understanding of the subsequent arguments requires us to think at each step that a primitive idempotent i of $(\mathcal{O}G)^P$ is first considered as a (not necessarily primitive) idempotent of $(\mathcal{O}G)^Q$ and then is mapped to $kC_G(Q)$ by the Brauer homomorphism br_Q. Thus $br_Q(i)$ is a sum of primitive idempotents and, for instance, condition (c) of Lemma 40.1 asserts that each of them is associated with f.

We shall need to relate br_Q and br_P in the special case where Q is a normal subgroup of P. Since P normalizes $C_G(Q)$ (because it normalizes Q), $kC_G(Q)$ is a P-algebra. But Q acts trivially by definition of $C_G(Q)$, and we view $kC_G(Q)$ as a (P/Q)-algebra. It is a permutation (P/Q)-algebra (because P/Q acts on the canonical basis of $kC_G(Q)$), and this allows us to describe the Brauer homomorphism. For simplicity of notation, we only write $br_{P/Q}$ for the Brauer homomorphism

$$br_{P/Q} = br_{P/Q}^{kC_G(Q)} : (kC_G(Q))^{P/Q} \longrightarrow kC_G(P)\,.$$

By Proposition 27.6, the image of $br_{P/Q}$ is indeed $kC_G(P)$, because $C_G(P)$ is contained in $C_G(Q)$ and is exactly the set of (P/Q)-fixed elements. Every (P/Q)-orbit outside $C_G(P)$ is non-trivial, and so the corresponding orbit sum is mapped to zero under $br_{P/Q}$. Thus $br_{P/Q}$ is in fact the restriction to $(kC_G(Q))^P$ of the Brauer homomorphism br_P^{kG} for kG, but for the sake of clarity we keep the notation br_P for $br_P^{\mathcal{O}G}$, and $br_{P/Q}$ for the above map. Note finally that the composite of the inclusion r_Q^P followed by br_Q maps $(\mathcal{O}G)^P$ to the set of (P/Q)-fixed elements $kC_G(Q)^{P/Q}$.

(40.2) LEMMA. *Let P be a p-subgroup of G and let Q be a normal subgroup of P.*

(a) With the notation above, the Brauer homomorphism br_P is equal to the composite map

$$(\mathcal{O}G)^P \xrightarrow{\;br_Q\, r_Q^P\;} (kC_G(Q))^{P/Q} \xrightarrow{\;br_{P/Q}\;} kC_G(P)\,.$$

In other words for every $a \in (\mathcal{O}G)^P$, we have $br_{P/Q}\, br_Q(a) = br_P(a)$.

(b) The first map of the above composite is surjective, that is, we have $br_Q((\mathcal{O}G)^P) = (kC_G(Q))^{P/Q}$.

Proof. Since there is an invariant basis, the Brauer homomorphism just selects the fixed elements of an invariant basis and maps every other orbit sum to zero (Proposition 27.6). The result is an easy consequence of this. Details are left as an exercise for the reader. □

In the proof of the main result, we shall also need the following lemma.

(40.3) LEMMA. *Let N be a p-group and let A be a permutation N-algebra over k. For every subgroup $S \leq N$, consider the restriction to A^N of the Brauer homomorphism br_S. Then*

$$\bigcap_{1<S\leq N} \mathrm{Ker}(br_S) = A_1^N .$$

Proof. Let X be an N-invariant k-basis of A and let $a \in A^N$. Then a is a linear combination of N-orbit sums and we can write

$$a = \sum_{x\in[N\backslash X]} \lambda_x \sum_{g\in[N/N_x]} {}^g x ,$$

where $\lambda_x \in k$ and N_x denotes the stabilizer of x. By Proposition 27.6, $br_S(X^S)$ is a basis of $\overline{A}(S)$. Suppose that $a \in \bigcap_{1<S\leq N} \mathrm{Ker}(br_S)$. For each $y \in X$, we have $y \in X^{N_y}$, and therefore the basis element $br_{N_y}(y)$ appears with coefficient λ_y in the expression of $br_{N_y}(a)$. Since we have $br_{N_y}(a) = 0$ if $N_y > 1$, it follows that $\lambda_y = 0$ in that case. Therefore a is a linear combination of orbit sums with trivial stabilizers. Clearly such an orbit sum is a relative trace $t_1^N(x)$, and so a is in the image of the relative trace map t_1^N.

The other inclusion $A_1^N \subseteq \bigcap_{1<S\leq N} \mathrm{Ker}(br_S)$ follows from the easy observation that $A_1^N \subseteq A_1^S$. □

Now we come to the main result.

(40.4) THEOREM. *Let (P,e) be a Brauer pair of G and let Q be a subgroup of P.*

(a) *There exists a unique block f of $kC_G(Q)$ with the following property: for every local pointed group P_γ associated with e, every local pointed group Q_δ with $Q_\delta \leq P_\gamma$ is associated with f; moreover there exists at least one local pointed group $Q_\delta \leq P_\gamma$. In particular we have $(P,e) \geq (Q,f)$.*

(b) *If Q is normal in P, the block f is the unique block of $kC_G(Q)$ which is invariant under P/Q and such that $br_{P/Q}(f)e = e$.*

Proof. We first prove the theorem in the case where Q is a normal subgroup of P. The Brauer homomorphism $br_{P/Q} : kC_G(Q)^{P/Q} \to kC_G(P)$ maps $(ZkC_G(Q))^{P/Q}$ into $ZkC_G(P)$, because the image of a central element under a surjection is central. Since $(ZkC_G(Q))^{P/Q}$ is commutative, there is a unique primitive decomposition of 1 in $(ZkC_G(Q))^{P/Q}$ (Corollary 4.2). Its image under $br_{P/Q}$ is a decomposition of 1 in $ZkC_G(P)$, and e is primitive in $ZkC_G(P)$. Therefore there exists a unique primitive idempotent f of $(ZkC_G(Q))^{P/Q}$ such that $br_{P/Q}(f)e = e$.

We now show that f remains primitive in $ZkC_G(Q)$, so that it is a block of $kC_G(Q)$. Let f' be a block of $ZkC_G(Q)$ appearing in the unique primitive decomposition of f in $ZkC_G(Q)$. Then for every $u \in P/Q$, the idempotent ${}^u f'$ is again a block of $ZkC_G(Q)$, and so ${}^u f'$ is either equal to f' or orthogonal to f' (Corollary 4.2). Moreover ${}^u f'$ also appears in the primitive decomposition of f, because ${}^u f = f$. It follows that the whole orbit of f' appears in the primitive decomposition of f, and if S is the stabilizer of f' in P/Q, the orbit sum $t_S^{P/Q}(f')$ belongs to $(ZkC_G(Q))^{P/Q}$. This forces $t_S^{P/Q}(f')$ to be equal to f because f is primitive in $(ZkC_G(Q))^{P/Q}$. Now $br_{P/Q}(t_S^{P/Q}(f')) = br_{P/Q}(f) \neq 0$ by definition of f, and this is only possible if $S = P/Q$. Therefore $f = f'$, proving the primitivity of f in $ZkC_G(Q)$.

Now let P_γ be any local pointed group associated with e and let $i \in \gamma$. Since $br_Q((\mathcal{O}G)^P) = kC_G(Q)^{P/Q}$ by Lemma 40.2, $br_Q(i)$ is either primitive in $kC_G(Q)^{P/Q}$ or zero (Theorem 3.2). Now using Lemma 40.2, we have

$$\begin{aligned} br_{P/Q}(br_Q(i)f) &= br_P(i)br_{P/Q}(f) = br_P(i)e\, br_{P/Q}(f) \\ &= br_P(i)e = br_P(i) \neq 0\,, \end{aligned}$$

and so $br_Q(i)f \neq 0$. Therefore $br_Q(i)$ is primitive in $kC_G(Q)^{P/Q}$ and $br_Q(i)f = br_Q(i)$ (because $br_Q(i) = br_Q(i)f + br_Q(i)(1-f)$ is an orthogonal decomposition). By Lemma 40.1, the equation $br_Q(i)f = br_Q(i)$ means that every local pointed group Q_δ with $Q_\delta \leq P_\gamma$ is associated with f. The fact that there exists at least one local pointed group $Q_\delta \leq P_\gamma$ is equivalent to the equation $br_Q(i) \neq 0$ (because any primitive idempotent appearing in a decomposition of $br_Q(i)$ defines such a point δ, as in the proof of Lemma 40.1). This completes the proof of (a) in the case where Q is a normal subgroup of P. Moreover by construction, f is the unique block of $kC_G(Q)$ invariant under P/Q (that is, lying in $(ZkC_G(Q))^{P/Q}$) and such that $br_{P/Q}(f)e = e$. This proves (b).

For the proof of (a) in the general case, we proceed by induction on $|P:Q|$ and we may assume that Q is a proper subgroup of P. For every subgroup S with $Q < S \leq P$, there exists by induction a unique block e_S of $kC_G(S)$ such that

(40.5) $\qquad br_S(\gamma)e_S = br_S(\gamma) \quad$ for every P_γ associated with e.

Here and in the rest of the proof, the conclusion of the theorem is stated in the form given by Lemma 40.1. Note also that another consequence of the induction hypothesis is that there exists at least one local pointed group $S_\sigma \leq P_\gamma$, or in other words $br_S(\gamma) \neq 0$.

Let $N = N_P(Q)$. Then $Q < N$ (because $Q < P$ and P is a p-group), and so we have the block e_N just constructed. If $Q < S \leq N$, we can also apply induction to the subgroups S and N. Thus there exists a unique block e'_S of $kC_G(S)$ such that

$$br_S(\varepsilon)e'_S = br_S(\varepsilon) \quad \text{for every } N_\varepsilon \text{ associated with } e_N\,, \tag{40.6}$$

and moreover $br_S(\varepsilon) \neq 0$. It is easy to prove that $e'_S = e_S$. This is in fact exactly the transitivity of the relation $\leq$ between Brauer pairs, which will be a consequence of the theorem. Indeed let P_γ be a local pointed group associated with e. Since $br_N(\gamma) \neq 0$ and $br_N(\gamma)e_N = br_N(\gamma)$ by 40.5, there exists at least one local pointed group N_ε such that $N_\varepsilon \leq P_\gamma$, and N_ε is associated with e_N. Similarly by 40.6, there exists at least one local pointed group S_σ such that $S_\sigma \leq N_\varepsilon$, and S_σ is associated with e'_S. Therefore $S_\sigma \leq P_\gamma$, forcing S_σ to be associated with e_S by 40.5. As a local pointed group is associated with a single block, we have $e'_S = e_S$.

Since Q is normal in N, we can apply the first part of the proof. Thus there exists a unique block f of $kC_G(Q)$ such that $br_Q(\varepsilon)f = br_Q(\varepsilon)$ for every N_ε associated with e_N. Therefore by 40.6 and the fact that $e'_S = e_S$, we have

$$\begin{aligned} br_{S/Q}br_Q(\varepsilon)br_{S/Q}(f)e_S &= br_{S/Q}(br_Q(\varepsilon)f)e_S = br_{S/Q}br_Q(\varepsilon)e_S \\ &= br_S(\varepsilon)e_S = br_S(\varepsilon) \neq 0\,, \end{aligned}$$

proving that $br_{S/Q}(f)e_S \neq 0$. Since $br_{S/Q}(f)$ is central in $kC_G(S)$ (because the surjection $br_{S/Q}$ maps $(ZkC_G(Q))^{S/Q}$ into $ZkC_G(S)$), and since e_S is primitive in $ZkC_G(S)$, we obtain

$$br_{S/Q}(f)e_S = e_S\,. \tag{40.7}$$

(This is just the conclusion of the theorem for the Brauer pairs (S, e_S) and (Q, f), in the form of statement (b), and it could also be deduced as above from the transitivity and uniqueness argument for the triple of subgroups $Q < S \leq N$.)

Now we choose a local pointed group P_γ associated with e and we choose $i \in \gamma$. We have to prove that $br_Q(i)f = br_Q(i)$. We first show that

$$br_Q(i)(1-f) \in \bigcap_{Q<S\leq N} \mathrm{Ker}(br_{S/Q})\,.$$

In order to emphasize that this makes sense, we note that $br_Q(i)(1-f)$ belongs to $(kC_G(Q))^{N/Q}$, because i is P-fixed, hence N-fixed, and on the other hand f is invariant under N/Q by (b) (which has already been proved for $Q \trianglelefteq N$). The computation is easy:

$$br_{S/Q}(br_Q(i)(1-f)) = br_S(i)br_{S/Q}(1-f) = br_S(i)e_S\, br_{S/Q}(1-f) = 0\,,$$

because $e_S\, br_{S/Q}(1-f)=0$ by property 40.7. This proves the above claim about $br_Q(i)(1-f)$. Applying Lemma 40.3 to the (N/Q)-algebra $kC_G(Q)$ we deduce that $br_Q(i)(1-f) \in (kC_G(Q))_1^{N/Q}$. But by Proposition 11.9 we have

$$br_Q((\mathcal{O}G)_Q^P) = \overline{\mathcal{O}G}(Q)_1^{\overline{N}_P(Q)} = (kC_G(Q))_1^{N/Q}\,.$$

Therefore $br_Q(i)(1-f) \in br_Q((\mathcal{O}G)_Q^P)$. Multiplying by $br_Q(i)$ on both sides, we obtain

$$br_Q(i)(1-f) \in br_Q(i(\mathcal{O}G)_Q^P i) = br_Q((i\mathcal{O}Gi)_Q^P)\,.$$

Since γ is local, $\{i\}$ is a local point of $(i\mathcal{O}Gi)^P$ (Proposition 15.1), and so $i \notin (i\mathcal{O}Gi)_Q^P$ because $Q<P$. Since $i\mathcal{O}Gi$ is a primitive P-algebra, $J((i\mathcal{O}Gi)^P)$ is the unique maximal ideal of $(i\mathcal{O}Gi)^P$, and therefore we have $(i\mathcal{O}Gi)_Q^P \subseteq J((i\mathcal{O}Gi)^P)$. Thus we obtain

$$br_Q(i)(1-f) \in br_Q(J((i\mathcal{O}Gi)^P)) = br_Q(iJ((\mathcal{O}G)^P)i) \subseteq br_Q(J((\mathcal{O}G)^P))\,.$$

But there exists a positive integer n such that $J((\mathcal{O}G)^P)^n \subseteq \mathfrak{p}(\mathcal{O}G)^P$ (Theorem 2.7), and on the other hand $\mathfrak{p}(\mathcal{O}G)^P \subseteq \mathfrak{p}(\mathcal{O}G)^Q \subseteq \mathrm{Ker}(br_Q)$. Since $br_Q(i)(1-f)$ is an idempotent, it follows that

$$br_Q(i)(1-f) = (br_Q(i)(1-f))^n \in br_Q(J((\mathcal{O}G)^P)^n) \subseteq br_Q(\mathfrak{p}(\mathcal{O}G)^Q) = 0\,.$$

Therefore $br_Q(i)(1-f)=0$, or in other words $br_Q(i)f = br_Q(i)$. This is precisely what we needed to prove.

Finally we have to prove the additional statement that there exists a local pointed group $Q_\delta \leq P_\gamma$, or in other words that $br_Q(\gamma) \neq 0$. But $br_{N/Q}br_Q(\gamma) = br_N(\gamma)$ and this is non-zero by induction since $Q<N$. □

This theorem has several important consequences. The first is about the order relation between Brauer pairs and was already mentioned.

(40.8) COROLLARY. *Let* (Q, f) *and* (P, e) *be Brauer pairs of* G *.*

(a) We have $(Q, f) \leq (P, e)$ *if and only if, for every local pointed group* P_γ *on* $\mathcal{O}G$ *associated with* e *, all local pointed groups* $Q_\delta \leq P_\gamma$ *are associated with* f *.*

(b) The relation $\leq$ *between Brauer pairs of* G *is transitive.*

Proof. (a) Suppose that $(Q, f) \leq (P, e)$, so that by definition there exist on $\mathcal{O}G$ local pointed groups P_{γ_0} associated with e and Q_{δ_0} associated with f such that $Q_{\delta_0} \leq P_{\gamma_0}$. By the theorem, for every local pointed group P_γ associated with e , all the local pointed groups $Q_\delta \leq P_\gamma$ are associated with the same Brauer pair, which must be (Q, f) since Q_{δ_0} is one of them. The converse implication is obvious.

(b) This is an easy consequence of (a) and the transitivity of the order relation between pointed groups. □

(40.9) COROLLARY. *Let* (P, e) *be a Brauer pair of* G *.*

(a) If $Q \leq P$ *, there exists a unique block* f *of* $kC_G(Q)$ *such that* $(Q, f) \leq (P, e)$ *.*

(b) The map $(Q, f) \mapsto Q$ *is an isomorphism between the poset of Brauer pairs contained in* (P, e) *and the poset of subgroups of* P *.*

Proof. In view of Corollary 40.8, (a) is just a restatement of Theorem 40.4. Clearly (b) is a restatement of (a). □

It should be noted that there is no similar uniqueness statement for the poset of Brauer pairs lying above (Q, f) : if $Q \leq P$, there are in general several Brauer pairs (P, e) such that $(Q, f) \leq (P, e)$. This can occur for instance when $Q \trianglelefteq P$, because in that case we have $br_{P/Q}(f)e = e$ and every block e appearing in a decomposition of $br_{P/Q}(f)$ defines a Brauer pair $(P, e) \geq (Q, f)$.

We have used local pointed groups for the definition of the order relation between Brauer pairs, but the relation can be described directly using only blocks of centralizers. We already know this in the normal case: if $Q \trianglelefteq P$ and if $(Q, f) \leq (P, e)$, then by Theorem 40.4 the block f is the unique block of $kC_G(Q)$ which is invariant under P/Q and such that $br_{P/Q}(f)e = e$. In that case we say that (Q, f) is *normal* in (P, e) , or that (P, e) *normalizes* (Q, f) , and we write $(Q, f) \trianglelefteq (P, e)$. The direct description of the relation $\leq$ in the general case follows from the normal case, in view of the following result.

(40.10) COROLLARY. *The order relation* $\leq$ *between Brauer pairs is the transitive closure of the relation* $\trianglelefteq$.

Proof. Suppose that $(Q,f) \leq (P,e)$. Since P is a p-group, there exists a sequence of subgroups

$$Q = Q_0 \trianglelefteq Q_1 \trianglelefteq \ldots \trianglelefteq Q_{n-1} \trianglelefteq Q_n = P\,,$$

each being normal in the next. By Corollary 40.9 and induction on i , there exists a unique Brauer pair (Q_i, e_i) such that $(Q_i, e_i) \leq (Q_{i+1}, e_{i+1})$, where $e_n = e$. By transitivity we have $(Q, e_0) \leq (P, e)$, and by uniqueness it follows that $(Q, e_0) = (Q, f)$. Since $Q_i \trianglelefteq Q_{i+1}$, we necessarily have $(Q_i, e_i) \trianglelefteq (Q_{i+1}, e_{i+1})$. This proves that the given relation $(Q,f) \leq (P,e)$ is obtained by a sequence of relations $\trianglelefteq$, as required. □

If P is a p-subgroup of G and if $Q < P$, it is well-known that Q is a proper subgroup of $N_P(Q)$. The analogous result has already been proved for local pointed groups (Corollary 20.5). As a consequence of Corollary 40.10, it also holds for Brauer pairs, as follows.

(40.11) COROLLARY. *Let* (Q,f) *and* (P,e) *be two Brauer pairs such that* $(Q,f) < (P,e)$. *If* g *is the unique block of* $kC_G(N_P(Q))$ *such that* $(N_P(Q), g) \leq (P,e)$, *then we have* $(Q,f) \triangleleft (N_P(Q), g) \leq (P,e)$ *and* $(Q,f) \neq (N_P(Q), g)$.

In our last application of Theorem 40.4, we take $Q = 1$. For every Brauer pair (P,e) , there is a unique block $\overline{b}$ of $kC_G(1) = kG$ such that $(1, \overline{b}) \leq (P,e)$. This gives one way of associating a block of G to a Brauer pair. We say that (P,e) is *associated* with b , or also that e is a *Brauer correspondent* of b , if the equivalent conditions of the following lemma hold.

(40.12) LEMMA. *Let* b *be a block of* $\mathcal{O}G$ *and let* $\overline{b}$ *be its image in* kG . *Let* (P,e) *be a Brauer pair of* G *and let* P_γ *be any local pointed group associated with* (P,e) . *The following conditions are equivalent.*

(a) $(1, \overline{b}) \leq (P,e)$.

(b) $br_P(b)e = e$.

(c) $P_\gamma \leq G_{\{b\}}$.

Proof. (a) $\Rightarrow$ (b). If $(1,\bar{b}) \leq (P,e)$, we have $(1,\bar{b}) \trianglelefteq (P,e)$ since the trivial subgroup is normal, and therefore $br_P^{kG}(\bar{b})e = e$ (Theorem 40.4). But clearly $br_P^{\mathcal{O}G}(b) = br_P^{kG}(\bar{b})$.

(b) $\Rightarrow$ (c). Let $i \in \gamma$. Since P_γ is associated with e, we have $e\,br_P(i) = br_P(i)$. If $br_P(b)e = e$, then

$$br_P(bi) = br_P(b)br_P(i) = br_P(b)e\,br_P(i) = e\,br_P(i) = br_P(i) \neq 0\,,$$

so that $bi \neq 0$. Since i is primitive in $(\mathcal{O}G)^P$ and decomposes as $i = bi + (1-b)i$, we have $bi = i$. This relation means that $P_\gamma \leq G_{\{b\}}$.

(c) $\Rightarrow$ (a). Let $i \in \gamma$. If $P_\gamma \leq G_{\{b\}}$, we have $bi = i$ and so

$$br_P(b)e\,br_P(i) = br_P(b)br_P(i) = br_P(bi) = br_P(i) \neq 0\,.$$

Therefore $br_P(b)e \neq 0$. But e is primitive in $ZkC_G(P)$ and we have $br_P(b) \in ZkC_G(P)$ (because the surjection br_P necessarily maps ZkG into $ZkC_G(P)$). This forces the equality $br_P(b)e = e$. Thus $br_P^{kG}(\bar{b})e = e$ and by Theorem 40.4 this relation means that $(1,\bar{b}) \leq (P,e)$. □

Condition (b) in the above lemma means that e appears in a decomposition of $br_P(b)$. Thus (P,e) is associated with b if and only if b acts as the identity on e via the Brauer homomorphism br_P.

Note that if P_γ is associated with a block e of $kC_G(P)$, and if (P,e) is associated with a block b of $\mathcal{O}G$, then P_γ is associated with b, showing that the notions are consistent. In other words, if e is a Brauer correspondent of b, the irreducible representations of $kC_G(P)$ associated with e can also be associated with b. Explicity, a simple $kC_G(P)$-module V is associated with b if $br_P(b)$ acts as the identity on V.

We already know that the blocks of G partition the poset of pointed groups on $\mathcal{O}G$ as a disjoint union. The above observations show that the blocks of G also partition the blocks of $kC_G(P)$: with each block b of $\mathcal{O}G$ are associated the Brauer correspondents of b. The poset of Brauer pairs is the disjoint union over the blocks b of G of the posets of Brauer pairs associated with b. We shall see below that the maximal elements in one component are all conjugate.

We also emphasize that a block b of $\mathcal{O}G$ defines a Brauer pair $(1,\bar{b})$, where $\bar{b}$ is the image of b in kG. Thus the blocks of G correspond to the trivial subgroup in the theory of Brauer pairs, whereas they correspond to the whole group G in the theory of pointed groups (since $G_{\{b\}}$ is a pointed group). This may seem surprising at first, but can be better understood if a Brauer pair (P,e) is informally thought of as being the collection of all irreducible representations of $kC_G(P)$ belonging to e. Thus if $P = 1$, the Brauer pair $(1,\bar{b})$ corresponds to the collection of simple kG-modules belonging to b, which in turn correspond indeed to the pointed groups 1_δ associated with b.

We consider now maximal Brauer pairs.

(40.13) PROPOSITION. *Let b be a block of $\mathcal{O}G$.*

(a) The maximal Brauer pairs associated with b are conjugate under G.

(b) If (P,e) is a maximal Brauer pair associated with b, there is a unique local pointed group P_γ associated with (P,e) and P_γ is a defect of b. In particular P is a defect group of b.

(c) If (P,e) is a maximal Brauer pair associated with b, the block e of $kC_G(P)$ has defect group $Z(P)$. The defect multiplicity module $V(\gamma)$ of b is the unique simple $kC_G(P)e$-module, and is projective as a module over $k\overline{C}_G(P)$.

(d) The map $(P,e) \mapsto P_\gamma$ defined by (b) is a bijection between the set of all maximal Brauer pairs associated with b and the set of all defects of b. In particular $N_G(P_\gamma) = N_G(P,e)$.

Proof. Let (P,e) be a maximal Brauer pair associated with b and let P_γ be a local pointed group associated with (P,e). By construction of the order relation, P_γ is a maximal local pointed group, that is, a defect of some block b' of $\mathcal{O}G$. By Lemma 40.12, (P,e) is associated with b', so that $b' = b$. Since all defects of b are conjugate, so are the maximal Brauer pairs associated with b, proving (a).

We have just seen that P_γ is a defect of b, so that $V(\gamma)$ is a defect multiplicity module of b. We know that $V(\gamma)$ is both simple and projective over $k\overline{C}_G(P)$ (Theorem 37.9). Therefore, by Theorem 39.1, $V(\gamma)$ belongs to a block $\overline{e}$ of defect zero of $k\overline{C}_G(P)$. By Corollary 39.3, $\overline{e}$ lifts to a block of $kC_G(P)$ with defect group $Z(P)$. Since this block has $V(\gamma)$ as a simple module, it must be equal to e, because $V(\gamma)$ belongs to e by definition. This shows that e has defect group $Z(P)$, completing the proof of (c).

By Proposition 39.2, $V(\gamma)$ is the unique simple $kC_G(P)e$-module, because the defect group $Z(P)$ is central. This means that P_γ is the unique local pointed group associated with (P,e), completing the proof of (b). Statement (d) is an immediate consequence of (b). □

We return to Brauer's first main theorem and give another version of the result, using only blocks.

(40.14) THEOREM (Brauer's first main theorem). *Let P be a p-subgroup of G. There is a bijection between the set of all blocks of $\mathcal{O}G$ with defect group P and the set of all $N_G(P)$-conjugacy classes of blocks of $kC_G(P)$ with defect group $Z(P)$ whose inertial subgroup I in $N_G(P)$ is such that $|I/PC_G(P)|$ is prime to p. The bijection maps a block b to the unique $N_G(P)$-conjugacy class of blocks e such that (P,e) is a (maximal) Brauer pair associated with b.*

Proof. In our previous version of Brauer's first main theorem (Theorem 37.12), the target of the bijection was a set of $\overline{N}_G(P)$-conjugacy classes of projective simple $k\overline{C}_G(P)$-modules, and the image of a block b was the conjugacy class of the defect multiplicity modules $V(\gamma)$. As observed in Section 39, any such module $V(\gamma)$ corresponds uniquely to a block $\overline{e}$ of defect zero of $k\overline{C}_G(P)$. By Corollary 39.3, $\overline{e}$ lifts uniquely to a block e of $kC_G(P)$ with defect group $Z(P)$. This provides a bijection between the two sets of the statement. By Proposition 40.13 above, the block e just constructed is a Brauer correspondent of b (that is, (P,e) is associated with b). Therefore the bijection is indeed given by the map described in the statement. □

A useful property of p-subgroups is that all maximal p-subgroups normalizing a given p-subgroup Q are conjugate, because they are the Sylow p-subgroups of $N_G(Q)$. We now show that this also holds for Brauer pairs. Recall that a Brauer pair (P,e) normalizes (Q,f) if $(Q,f) \leq (P,e)$ and $Q \trianglelefteq P$; in that case f is (P/Q)-invariant (Theorem 40.4), so that $P \leq N_G(Q,f)$.

(40.15) PROPOSITION. *Let (Q,f) be a Brauer pair of G and let $N_G(Q,f)$ be its inertial subgroup.*

(a) *(Q,f) is also a Brauer pair of the group $N_G(Q,f)$. Moreover the set of all Brauer pairs of G normalizing (Q,f) coincides with the set of all Brauer pairs of $N_G(Q,f)$ containing (Q,f).*

(b) *All the Brauer pairs of G which are maximal with respect to the property of normalizing (Q,f) are conjugate under $N_G(Q,f)$.*

Proof. (a) Write $N = N_G(Q,f)$. Since $C_N(Q) = C_G(Q)$, it is clear that (Q,f) is also a Brauer pair of N. Moreover for every Brauer pair (P,e) normalizing (Q,f), we have $P \leq N$ and on the other hand $C_G(P) \leq C_G(Q) \leq N$ so that $C_N(P) = C_G(P)$. Thus (P,e) is also a Brauer pair of N. The containment relation $(Q,f) \trianglelefteq (P,e)$ says that f is (P/Q)-invariant and that $br_{P/Q}(f)e = e$. Since both Brauer homomorphisms

$$br_{P/Q} : kC_G(Q)^{P/Q} \longrightarrow kC_G(P) \qquad \text{and}$$
$$br_{P/Q} : kC_N(Q)^{P/Q} \longrightarrow kC_N(P)$$

are the same map, the relation $(Q,f) \trianglelefteq (P,e)$ also holds as Brauer pairs of N. Conversely, the same arguments show that if (P,e) is a Brauer pair of N containing (Q,f), then (P,e) is a Brauer pair of G normalizing (Q,f).

(b) This follows from (a) and the fact that all maximal Brauer pairs of N containing (Q,f) are conjugate under N (Proposition 40.13), because they are all necessarily associated with the same block of kN (which is in fact equal to f itself by Exercise 40.2). □

The set of all Brauer pairs of G normalizing (Q, f) and the set of all Brauer pairs of $N_G(Q, f)$ containing (Q, f) also coincide as posets (Exercise 40.2). Moreover f is in fact a block of $kN_G(Q, f)$ and all the Brauer pairs of $N_G(Q, f)$ containing (Q, f) are associated with f, that is, they contain $(1, f)$ as Brauer pairs of $N_G(Q, f)$ (Exercise 40.2).

We end this section with the description of the Brauer pairs associated with the principal block. Recall that the principal block b of $\mathcal{O}G$ is the unique block containing the trivial (simple) module k. If X is a subset of G, we define

$$\mathcal{S}X = \sum_{x \in X} x \ \in \mathcal{O}G .$$

We use this notation for the following characterization of the principal block.

(40.16) LEMMA. *Let b be a block of $\mathcal{O}G$. The following conditions are equivalent.*
(a) b is the principal block.
(b) $b\mathcal{S}G \neq 0$.
(c) $b\mathcal{S}G = \mathcal{S}G$.

Proof. Since $g\cdot\mathcal{S}G = \mathcal{S}G$ if $g \in G$, the $\mathcal{O}$-submodule $\mathcal{O}\cdot\mathcal{S}G$ of the group algebra is invariant under left multiplication by G and is isomorphic to the trivial lattice $\mathcal{O}$. Clearly the trivial lattice is associated with the principal block since its reduction modulo $\mathfrak{p}$ is. Thus b is the principal block if and only if the action of b on the trivial lattice is the identity (that is, $b\mathcal{S}G = \mathcal{S}G$), or equivalently is non-zero (that is, $b\mathcal{S}G \neq 0$). □

(40.17) THEOREM (Brauer's third main theorem). *Let b be the principal block of $\mathcal{O}G$ and let Q be any p-subgroup of G.*
(a) The idempotent $br_Q(b)$ is primitive in $ZkC_G(Q)$ and is equal to the principal block of $kC_G(Q)$.
(b) If e is a block of $kC_G(Q)$, then (Q, e) is a Brauer pair associated with b if and only if e is the principal block of $kC_G(Q)$.
(c) The map $(Q, e) \mapsto Q$ is an isomorphism between the poset of Brauer pairs associated with b and the poset of all p-subgroups of G.

Proof. For every p-subgroup R of G, let us write e_R for the principal block of $kC_G(R)$.

(a) First note that by Proposition 37.5, we have $br_Q(\mathcal{S}G) = \mathcal{S}C_G(Q)$. It follows that

$$br_Q(b)\mathcal{S}C_G(Q) = br_Q(b\mathcal{S}G) = br_Q(\mathcal{S}G) = \mathcal{S}C_G(Q) ,$$

so that e_Q appears in a decomposition of $br_Q(b)$ in $ZkC_G(Q)$. In other words e_Q is always associated with b. In particular this holds for a Sylow p-subgroup P of G, and therefore (P, e_P) is a maximal Brauer pair associated with b. If (P, f) is any Brauer pair associated with b, then (P, f) is maximal. Therefore by Proposition 40.13, (P, f) is conjugate to (P, e_P), that is, $f = {}^g(e_P)$ for some $g \in N_G(P)$. Since ${}^g(C_G(P)) = C_G(P)$, we have

$$ {}^g(e_P)\mathcal{S}C_G(P) = {}^g(e_P\mathcal{S}C_G(P)) = {}^g(\mathcal{S}C_G(P)) = \mathcal{S}C_G(P) , $$

so that ${}^g(e_P) = e_P$ by Lemma 40.16. This shows that e_P is the unique block of $kC_G(P)$ appearing in a decomposition of $br_P(b)$ in $ZkC_G(P)$, that is, $br_P(b) = e_P$. Thus (a) holds for a Sylow p-subgroup P.

Now we prove (a) by descending induction. Since the order relation between Brauer pairs is the transitive closure of the relation $\trianglelefteq$ (Corollary 40.10), it suffices to prove that if $(R, f) \trianglelefteq (Q, e_Q)$, then $f = e_R$. Indeed this implies that e_R is the unique block of $kC_G(R)$ associated with b, so that $br_R(b) = e_R$. Now $br_{Q/R}(f)e_Q = e_Q$ by definition of the relation $\trianglelefteq$, and since $br_{Q/R}(\mathcal{S}C_G(R)) = \mathcal{S}C_G(Q)$ we have

$$ \begin{aligned} br_{Q/R}(f\mathcal{S}C_G(R))e_Q &= br_{Q/R}(f)\mathcal{S}C_G(Q)e_Q = br_{Q/R}(f)e_Q\mathcal{S}C_G(Q) \\ &= e_Q\mathcal{S}C_G(Q) = \mathcal{S}C_G(Q) \neq 0 , \end{aligned} $$

and so $f\mathcal{S}C_G(R) \neq 0$. Thus f is the principal block, as required.

(b) This is a restatement of (a). Indeed by Lemma 40.12, (P, e) is associated with b if and only if e appears in a decomposition of $br_P(b)$ in $ZkC_G(P)$.

(c) If $R \trianglelefteq Q$, then by Lemma 40.2 we have

$$ br_{Q/R}(e_R) = br_{Q/R}br_R(b) = br_Q(b) = e_Q , $$

so that $(R, e_R) \trianglelefteq (Q, e_Q)$. By transitivity (Corollary 40.10), it follows that $(R, e_R) \leq (Q, e_Q)$ if and only if $R \leq Q$. This proves (c). □

We deduce as a corollary a result which was already proved in Exercise 37.7.

(40.18) COROLLARY. *The defect groups of the principal block of $\mathcal{O}G$ are the Sylow p-subgroups of G.*

Proof. If b is the principal block and P is a Sylow p-subgroup of G, then $br_P(b) \neq 0$ by the theorem, and the result follows (Proposition 18.5). Alternatively note that by the theorem, the pair (P, e_P) is a maximal pair associated with b (where e_P is the principal block of $kC_G(P)$). □

The defect multiplicity modules of the principal block b of $\mathcal{O}G$ are also easy to describe. If P is a Sylow p-subgroup of G, then the trivial one-dimensional $k\overline{N}_G(P)$-module is a defect multiplicity module of b (Exercise 40.7).

Exercises

(40.1) Prove Lemma 40.2.

(40.2) Let (Q, f) be a Brauer pair of G and let $N = N_G(Q, f)$.
(a) Prove that the set of all Brauer pairs of G normalizing (Q, f) and the set of all Brauer pairs of N containing (Q, f) coincide as posets.
(b) Prove that f is a block of kN. [Hint: Use Exercise 37.8.] Deduce that f is a block of $C_N(R)$ for every subgroup $R \leq Q$ and that we have $(1, f) \leq (R, f) \leq (Q, f)$ as Brauer pairs of N.
(c) Show that the Brauer pairs of N containing (Q, f) are associated with the block f of N.

(40.3) Let (Q, f) be a Brauer pair of G. We say that a Brauer pair (R, g) centralizes (Q, f) if $(Q, f) \leq (R, g)$ and $R \leq QC_G(Q)$.
(a) Prove that (Q, f) is also a Brauer pair of $QC_G(Q)$ and that the set of all Brauer pairs of G centralizing (Q, f) coincides with the set of all Brauer pairs of $QC_G(Q)$ containing (Q, f).
(b) Prove that all maximal Brauer pairs centralizing (Q, f) are conjugate under $QC_G(Q)$.
(c) State and prove results analogous to those of Exercise 40.2, with $QC_G(Q)$ instead of $N_G(Q, f)$.

(40.4) Let (Q, f) be a Brauer pair of G. Prove that if (Q, f) is maximal as a Brauer pair of $N_G(Q, f)$, then (Q, f) is maximal as a Brauer pair of G. Deduce that if Q is a Sylow p-subgroup of $N_G(Q)$, then Q is a Sylow p-subgroup of G.

(40.5) Let (R, g), (Q, f), and (P, e) be Brauer pairs of G such that $(R, g) \leq (P, e)$, $(Q, f) \leq (P, e)$, and $R \leq Q$. Prove that $(R, g) \leq (Q, f)$.

(40.6) Let P_γ be a local pointed group on $\mathcal{O}G$ and let Q be a subgroup of P. Prove that there exists at least one local pointed group Q_δ such that $Q_\delta \leq P_\gamma$. [Hint: Use induction to reduce to the case where $Q \lhd P$ and then use Lemma 40.2.]

(40.7) Let b be the principal block of $\mathcal{O}G$ and let P_γ be a defect of b (so that P is a Sylow p-subgroup of G).

(a) Prove that the defect multiplicity module $V(\gamma)$ is the trivial one-dimensional $k\overline{C}_G(P)$-module.

(b) Prove that $N_G(P_\gamma) = N_G(P)$ and that γ is the unique local point of $(\mathcal{O}Gb)^P$.

(c) Prove that the twisted group algebra $k_\sharp\widehat{\overline{N}}_G(P)$ is isomorphic to the ordinary group algebra $k\overline{N}_G(P)$ and that the $k\overline{N}_G(P)$-module structure of $V(\gamma)$ is trivial.

(d) Let (P, e) be a maximal Brauer pair associated with b. Prove that $kC_G(P)e \cong kP$. [Hint: Use Exercise 39.5.]

Notes on Section 40

The concept of Brauer pair was first introduced by Brauer [1974], but only in the special case of self-centralizing Brauer pairs (defined in the next section). The notion of Brauer correspondent of a block was an earlier concept introduced by Brauer [1959]. The general treatment of the order relation between Brauer pairs is due to Alperin and Broué [1979], who use Corollary 40.10 as definition. The connection with local pointed groups explained in Theorem 40.4 is due to Broué and Puig [1980a] and is in fact the origin of the subsequent work of Puig [1981] on pointed groups. Instead of the original approach of Alperin–Broué, it is the Broué–Puig result which enables us to define the order relation using pointed groups. Brauer's third main theorem is of course due to Brauer [1964], but we have followed Alperin and Broué [1979]. Another short proof of Brauer's third main theorem appears in Külshammer [1991b].

The poset of Brauer pairs was analysed or used in a large variety of cases: p-soluble groups (Puig [1980]), extensions by p-groups (Cabanes [1987, 1988a]), symmetric groups (Puig [1987a]), covering groups of symmetric groups (Cabanes [1988b]), general linear groups and unitary groups (Broué [1986], Broué and Olsson [1986]), arbitrary finite reductive groups (Fong and Srinivasan [1989], Cabanes and Enguehard [1992, 1993]), and finally blocks with dihedral or quaternion defect groups (Cabanes and Picaronny [1992]).

§ 41 SELF-CENTRALIZING LOCAL POINTED GROUPS

We discuss in this section several properties of self-centralizing local pointed groups on $\mathcal{O}G$. We define an analogous notion for Brauer pairs and we show that it is equivalent to the corresponding notion for local pointed groups. Finally we prove a result on vertices of simple modules, which shows a connection with the self-centralizing property.

Recall that a p-subgroup P of G is called self-centralizing if it is a Sylow p-subgroup of $PC_G(P)$, or equivalently if $Z(P)$ is a Sylow p-subgroup of $C_G(P)$. By analogy, a Brauer pair (P,e) is called *self-centralizing* if $Z(P)$ is a defect group of the block e. Blocks with this property were considered in Corollary 39.3. We first establish the connection with the corresponding notion for local pointed groups.

(41.1) PROPOSITION. *Let (P,e) be a Brauer pair of G and let P_γ be a local pointed group associated with (P,e).*
(a) (P,e) is self-centralizing if and only if P_γ is self-centralizing.
(b) If (P,e) is self-centralizing, P_γ is the unique local pointed group associated with (P,e). In other words there is, up to isomorphism, a unique simple $kC_G(P)$-module V associated with the block e. This simple module is projective as a module over $k\overline{C}_G(P)$ and is isomorphic to the defect multiplicity module of e. Moreover the image of e in $k\overline{C}_G(P)$ is a block of defect zero (having V as unique projective simple module).

Proof. Suppose first that (P,e) is self-centralizing. By Corollary 39.3, e maps to a block $\overline{e}$ of defect zero of $\overline{C}_G(P)$. The unique simple module V for $\overline{e}$ is projective over $k\overline{C}_G(P)$, and V is a simple $kC_G(P)$-module belonging to e. Thus $V = V(\delta)$ is the multiplicity module of some local pointed group P_δ associated with (P,e). Now $Z(P)$ acts trivially on every simple $kC_G(P)$-module (Corollary 21.2), so that every simple $kC_G(P)e$-module is in fact a module for $k\overline{C}_G(P)\overline{e}$, which has only one simple module up to isomorphism. Therefore there is only one simple $kC_G(P)e$-module and one local pointed group associated with (P,e), that is, $P_\delta = P_\gamma$. By construction P_γ is self-centralizing since its multiplicity module $V(\gamma) = V$ is projective over $k\overline{C}_G(P)$ (Lemma 37.8). By Corollary 39.3 again, we know that $V(\gamma)$ is also the defect multiplicity module of the block e. This proves one implication in (a) and completes the proof of (b).

Suppose now that P_γ is self-centralizing, and let $V(\gamma)$ be the multiplicity module of γ (which is a simple $k\overline{C}_G(P)$-module by Corollary 37.6). Since P_γ is self-centralizing, $V(\gamma)$ is also a projective $k\overline{C}_G(P)$-module (Lemma 37.8). Therefore, by Theorem 39.1, $V(\gamma)$ belongs to a block $\overline{e}$ of defect zero of $k\overline{C}_G(P)$, and $V(\gamma)$ is, up to isomorphism, the unique simple module for this block. By Corollary 39.3, $\overline{e}$ lifts to a block of $kC_G(P)$ with defect group $Z(P)$. Since this block has $V(\gamma)$ as a simple module, it must be equal to e. Indeed $V(\gamma)$ belongs to e since P_γ is associated with (P, e). The fact that e has defect group $Z(P)$ means that (P, e) is self-centralizing. □

If (P, e) is a self-centralizing Brauer pair associated with a block b of $\mathcal{O}G$, then the image $\overline{e}$ of e in $k\overline{C}_G(P)$ is a block of defect zero of $k\overline{C}_G(P)$. In this situation, we shall also say that $\overline{e}$ is *associated* with b.

Note that the block e in a self-centralizing Brauer pair (P, e) can also be viewed as a block of $PC_G(P)$ with defect group P (by Exercise 37.8). The proposition shows that the concept of self-centralizing Brauer pair is in fact equivalent to that of self-centralizing local pointed group. This observation includes the order relation, as follows.

(41.2) COROLLARY. *There is an isomorphism between the poset of all self-centralizing Brauer pairs of G and the poset of all self-centralizing local pointed groups on $\mathcal{O}G$, mapping a self-centralizing Brauer pair (P, e) to the unique self-centralizing local pointed group P_γ associated with (P, e).*

We can specialize to maximal Brauer pairs, which are self-centralizing since maximal local pointed groups are self-centralizing. The fact that there is a unique local pointed group P_γ associated with a maximal Brauer pair (P, e) has already been proved in Proposition 40.13. In fact the above proof of Proposition 41.1 is the same as the one given for maximal Brauer pairs.

We now turn to an important group theoretical characterization of self-centralizing local pointed groups, which shows that the terminology is particularly well adapted to the concept.

(41.3) PROPOSITION. *Let Q_δ be a local pointed group on $\mathcal{O}G$. The following conditions are equivalent.*

(a) Q_δ is self-centralizing.

(b) For every local pointed group P_γ on $\mathcal{O}G$ such that $Q_\delta \leq P_\gamma$, we have $C_P(Q) \leq Q$.

Proof. (a) ⇒ (b). Let P_γ be local and such that $Q_\delta \leq P_\gamma$, and let $R = QC_P(Q)$. If Q_δ is associated with a Brauer pair (Q, f) and if P_γ is associated with a Brauer pair (P, e), then there exists a Brauer pair (R, g) such that $(Q, f) \leq (R, g) \leq (P, e)$ (Corollary 40.9). By definition of the order relation between Brauer pairs, there exists a local pointed group R_ε associated with (R, g) and a local pointed group $Q_{\delta'}$ associated with (Q, f) such that $Q_{\delta'} \leq R_\varepsilon$. Since (Q, f) is self-centralizing by assumption, there is a unique local pointed group associated with it (Proposition 41.1), and so $\delta' = \delta$. Thus $Q_\delta \leq R_\varepsilon$.

Since $R \leq QC_G(Q)$, there exists a point α of $(\mathcal{O}G)^{QC_G(Q)}$ such that $R_\varepsilon \leq (QC_G(Q))_\alpha$ (Exercise 13.5), and so $Q_\delta \leq R_\varepsilon \leq (QC_G(Q))_\alpha$. But by Proposition 37.7, α is the unique point such that $Q_\delta \leq (QC_G(Q))_\alpha$, and since Q_δ is self-centralizing, it is a defect of $(QC_G(Q))_\alpha$ by definition. By the maximality of defect pointed groups, it follows that $Q_\delta = R_\varepsilon$, because R_ε is local. Thus $Q = R$, so that $C_P(Q) \leq Q$.

(b) $\Rightarrow$ (a). Let α be the unique point of $(\mathcal{O}G)^{QC_G(Q)}$ such that $Q_\delta \leq (QC_G(Q))_\alpha$ (Proposition 37.7), and let P_γ be a defect of $(QC_G(Q))_\alpha$ such that $Q_\delta \leq P_\gamma$. By assumption, we have $C_P(Q) \leq Q$. On the other hand we have $P = QC_P(Q)$, because $P \leq QC_G(Q)$ and $P \geq Q$. It follows that $P = Q$, so that $Q_\delta = P_\gamma$ is a defect of $(QC_G(Q))_\alpha$. This means that Q_δ is self-centralizing. □

Of course the inclusion relation in (b) could also be rewritten as $C_P(Q) = Z(Q)$. An important consequence of the proposition is the following.

(41.4) COROLLARY. *Let Q_δ be a self-centralizing local pointed group on $\mathcal{O}G$ and let P_γ be a local pointed group such that $Q_\delta \leq P_\gamma$. Then P_γ is self-centralizing.*

Proof. We use the criterion of Proposition 41.3. Let R_ε be a local pointed group such that $P_\gamma \leq R_\varepsilon$. Then $Q_\delta \leq R_\varepsilon$ and so $C_R(Q) \leq Q$. It follows that $C_R(P) \leq C_R(Q) \leq Q \leq P$, and this shows that P_γ is self-centralizing. □

(41.5) COROLLARY. *Let b be a block of $\mathcal{O}G$ with an abelian defect group. Then the defects of b are the only self-centralizing local pointed groups associated with b.*

Proof. Let Q_δ be a self-centralizing local pointed group associated with b and let P_γ be a defect of b such that $Q_\delta \leq P_\gamma$. Then we have $C_P(Q) \leq Q$ by Proposition 41.3. But since P is abelian by assumption, we also have $P \leq C_P(Q)$. It follows that $Q = P$ and so $Q_\delta = P_\gamma$. □

By Proposition 37.3, a vertex Q of an indecomposable $\mathcal{O}G$-module M associated with a block b is contained in a defect group of b. We want to show that if M is a simple module, then Q is not arbitrary. More generally we work with a primitive interior G-algebra A having a simple defect multiplicity module.

(41.6) THEOREM. *Let b be a block of $\mathcal{O}G$, let A be a primitive interior G-algebra associated with b such that a defect multiplicity module of A is simple, and let Q be a defect group of A.*
(a) There exists a block of defect zero of $k\overline{C}_G(Q)$ associated with b.
(b) There exists a point δ of $(\mathcal{O}Gb)^Q$ such that Q_δ is a self-centralizing local pointed group.
(c) For some defect group P of b, we have $Q \leq P$ and $C_P(Q) \leq Q$.

Proof. (a) Since a defect multiplicity module V of A is simple (and projective), its restriction to $\overline{C}_G(Q)$ is a direct sum of projective simple $k\overline{C}_G(Q)$-modules (Lemma 26.10). If W is any such projective simple $k\overline{C}_G(Q)$-module, then W belongs to a block $\overline{e}$ of defect zero, and $\overline{e}$ lifts to a block e of $kC_G(Q)$ (Corollary 39.3). Since A is associated with b, so are V, W, and e. Indeed, by passing to the Brauer quotient (see 11.6), the structural homomorphism $\mathcal{O}Gb \to A$ induces a map

$$kC_G(Q)br_Q(b) \longrightarrow \overline{A}(Q),$$

and by Lemma 14.4 the defect multiplicity algebra $\mathrm{End}_k(V)$ is a quotient of $\overline{A}(Q)$; therefore since b acts on A as the identity, $br_Q(b)$ acts as the identity on V, hence also on W. Since $br_Q(b)$ is a sum of blocks of $kC_G(Q)$, the block e corresponding to W appears in a decomposition of $br_Q(b)$, and this means that e is associated with b. Therefore $\overline{e}$ is associated with b.

(b) This is a restatement of (a). Indeed if W is the unique simple module belonging to a block $\overline{e}$ of defect zero of $k\overline{C}_G(Q)$, then W is the multiplicity module $W = V(\delta)$ of a local pointed group Q_δ on $\mathcal{O}G$ (Corollary 37.6). Moreover Q_δ is associated with b if $V(\delta)$ is associated with b. Since $V(\delta)$ is projective (because $\overline{e}$ has defect zero), Q_δ is self-centralizing (Lemma 37.8).

(c) This is a consequence of (b) and Proposition 41.3 applied to a defect P_γ of b such that $Q_\delta \leq P_\gamma$. □

(41.7) COROLLARY (Knörr's theorem). *Let b be a block of $\mathcal{O}G$, let M be an $\mathcal{O}Gb$-lattice such that* $\mathrm{End}_{\mathcal{O}G}(M) \cong \mathcal{O}$*, and let Q be a vertex of M. Then the conclusions (a), (b), and (c) of Theorem 41.6 hold.*

Proof. The assumption on M implies in particular that M is indecomposable. By Proposition 26.8, a defect multiplicity module of M is simple. Thus the primitive interior G-algebra $A = \mathrm{End}_{\mathcal{O}}(M)$ satisfies the assumptions of Theorem 41.6. □

By Schur's lemma, this corollary applies in two cases of interest: when $\mathcal{O} = k$ and M is a simple kGb-module or when $\mathcal{O}$ is a domain with field of fractions K and M is such that $K \otimes_{\mathcal{O}} M$ is an absolutely simple KGb-module.

(41.8) COROLLARY. *Let b be a block of $\mathcal{O}G$ with an abelian defect group P. Then P is a vertex of any $\mathcal{O}Gb$-lattice M such that $\mathrm{End}_{\mathcal{O}G}(M) \cong \mathcal{O}$. In particular P is a vertex of any simple kG-module associated with b.*

Proof. This follows from part (b) of Theorem 41.6 and Corollary 41.5. The special case follows by taking $\mathcal{O} = k$ and using Schur's lemma. □

Exercises

(41.1) Let Q_δ be a self-centralizing local pointed group on $\mathcal{O}G$. Prove that the structural map $Z(Q) \to (\mathcal{O}G)_\delta^Q$ induces an isomorphism of k-algebras $kZ(Q) \cong \overline{(\mathcal{O}G)_\delta}(Q)$. [Hint: Follow the proof of Proposition 38.10.]

(41.2) Let (Q, f) be a Brauer pair of G. Prove that every maximal Brauer pair normalizing (Q, f) is self-centralizing. [Hint: Use Proposition 40.15.]

(41.3) Let R_ε, Q_δ, and P_γ be local pointed groups on $\mathcal{O}G$ such that $R_\varepsilon \le P_\gamma$, $Q_\delta \le P_\gamma$, and $R \le Q$. If R_ε is self-centralizing, prove that $R_\varepsilon \le Q_\delta$. [Hint: Use Exercise 40.5.]

Notes on Section 41

Self-centralizing Brauer pairs were first considered by Brauer [1974]. The results on self-centralizing pointed groups are due to Puig. Corollary 41.7 is due to Knörr [1979] (with a different proof). The generalization of Knörr's result given in Theorem 41.6 (and in particular the relevance of the simplicity of the defect multiplicity module) is due to a remark of Puig [1981], which was extended by Picaronny and Puig [1987] and Barker [1994a].

§ 42 CHARACTER THEORY

At the heart of representation theory is character theory, which we review in this section. We give no proofs, for the results appear in many textbooks and our main goal is only to prepare the grounds for the next section about generalized decomposition numbers. For proofs and additional information, we refer the reader to the books by Serre [1971], Curtis–Reiner [1981] and Feit [1982].

In order to make the connection between characteristic zero and characteristic p, we need to make a special choice for the base ring $\mathcal{O}$. Thus we replace our assumption 2.1 by the following, which was already used in Section 33 (Assumption 33.1).

(42.1) ASSUMPTION. As a base ring, we take a complete discrete valuation ring $\mathcal{O}$ with maximal ideal $\mathfrak{p}$ generated by π. We assume that the field of fractions K of $\mathcal{O}$ has characteristic zero, and that the residue field $k = \mathcal{O}/\mathfrak{p}$ is algebraically closed with non-zero characteristic p.

Then of course $\mathcal{O}$ also satisfies Assumption 2.1. By Hensel's lemma, all roots of unity of order prime to p lie in $\mathcal{O}$, because they lie in k as k is algebraically closed. As one often needs all $|G|$-th roots of unity, one can always add p^r-th roots of unity by considering an extension of $\mathcal{O}$ as follows. If $f(X)$ is the minimal polynomial over K of a primitive p^r-th root of unity ζ, then the coefficients of $f(X)$ lie in $\mathcal{O}$ (because ζ is integral over $\mathcal{O}$). Then $\mathcal{O}' = \mathcal{O}[\zeta] \cong \mathcal{O}[X]/(f(X))$ is again a complete discrete valuation ring, with fraction field $K' = K[\zeta] \cong K[X]/(f(X))$. The residue field of $\mathcal{O}'$ is again k (because the extension K' of K is totally ramified); moreover the reduction modulo $\mathfrak{p}$ of $f(X)$ divides $X^{p^r} - 1 = (X-1)^{p^r}$ over $k[X]$, so that any power of ζ is mapped to 1_k by reduction modulo $\mathfrak{p}$. More details can be found in Serre's book [1962].

(42.2) EXAMPLE. Let $\mathbb{Q}_p$ be the field of p-adic numbers and $\mathbb{Z}_p$ the ring of p-adic integers. Then $\mathbb{Z}_p$ is a complete discrete valuation ring, its maximal ideal is generated by p, and its residue field is the finite field $\mathbb{F}_p$ with p elements. If k is an algebraic closure of $\mathbb{F}_p$, then, up to isomorphism, there exists a unique unramified extension $\mathcal{O}$ of $\mathbb{Z}_p$ with residue field k. To say that $\mathcal{O}$ is unramified means that p is again a generator of the maximal ideal of $\mathcal{O}$. This is the smallest possible base ring satisfying Assumption 42.1. The smallest possible base ring containing p^r-th roots of unity is $\mathcal{O}' = \mathcal{O}[\zeta]$, where ζ is a primitive p^r-th root of unity, with minimal polynomial

$$\frac{t^{p^r}-1}{t^{p^{r-1}}-1} = t^{p^{r-1}(p-1)} + t^{p^{r-1}(p-2)} + \ldots + t^{p^{r-1}} + 1\,.$$

The maximal ideal of $\mathcal{O}'$ is generated by $\pi = \zeta - 1$. These facts will be proved in Lemma 52.1.

Since K has characteristic zero, the order of the group G is invertible in K and therefore the group algebra KG is semi-simple (Maschke's theorem, Exercise 17.6). For a suitable finite extension L of K , the group algebra $LG \cong L \otimes_K KG$ is split (Proposition 1.12). By a theorem of Brauer, LG is split if L contains all $|G|$-th roots of unity, but we do not need this explicit choice of L . Throughout this section, we assume that K is large enough, in the sense that KG is split. In other words we assume that every simple KG-module is absolutely simple.

Any KG-module M decomposes according to the blocks of $\mathcal{O}G$

$$M = \bigoplus_{\text{block } b} bM \, ,$$

and M is said to *belong* to b , or to be *associated* with b , if $M = bM$. In particular any simple KG-module is associated with some block b . For another way of seeing this, notice that the decomposition of $\mathcal{O}G$ as the direct product of the block algebras $\mathcal{O}Gb$ yields a decomposition

$$KG \cong \prod_{\text{block } b} KGb \, ,$$

and since KG is semi-simple, so is KGb . Thus KGb decomposes as the direct product of the simple algebras $\operatorname{End}_K(M)$, where M runs over all simple KG-modules belonging to b (up to isomorphism). In other words b , which is primitive in $Z\mathcal{O}G$, decomposes in ZKG as $b = \sum_M e_M$, where $e_M = 1_{\operatorname{End}_K(M)}$ is the primitive idempotent of the centre $ZKGb$ corresponding to the simple factor $\operatorname{End}_K(M)$. In fact b remains primitive in ZKG only when b has defect zero, as we shall see below.

For later use, we observe that, if $i\mathcal{O}Gi$ is a source algebra of a block b , the Morita equivalence between $\mathcal{O}Gb$ and $i\mathcal{O}Gi$ extends to K (see Exercise 9.7). Explicitly, the $(KGb, iKGi)$-bimodule KGi and the $(iKGi, KGb)$-bimodule iKG realize the equivalence.

If M is a KG-module, the *character* χ_M of M is the map

$$\chi_M : G \longrightarrow K \, , \qquad \chi_M(g) = \operatorname{tr}(g; M) \, ,$$

where $\operatorname{tr}(g; M)$ denotes the trace of the endomorphism g acting on the K-vector space M . Explicitly, relative to some K-basis of M , the endomorphism g is given by a matrix $\rho(g)$, the trace $\chi_M(g)$ is the sum of all diagonal entries of $\rho(g)$, and this is independent of the choice of basis. Clearly χ_M extends to a K-linear map $\chi_M : KG \to K$ defined by $\chi_M(a) = \mathrm{tr}(a; M)$ for every $a \in KG$. By elementary properties of the trace map, we have $\chi_M(gh) = \chi_M(hg)$ for all $g, h \in G$, and therefore $\chi_M(hgh^{-1}) = \chi_M(g)$. Every function $f : G \to K$ which is constant on conjugacy classes (that is, $f(hgh^{-1}) = f(g)$ for all $g, h \in G$) is called a *central function* on G (or also a *class function*). Thus characters are central functions. Note that $\chi_M(1)$ is the trace of the identity matrix, so that $\chi_M(1) = \dim_K(M)$.

If $M \cong M'$, then $\chi_M = \chi_{M'}$. On the other hand, the character of a direct sum $M \oplus N$ is equal to $\chi_{M\oplus N} = \chi_M + \chi_N$. Since every KG-module is semi-simple, this reduces to the case of a simple KG-module. The character χ_M of a simple KG-module M is called an *irreducible ordinary character* of G. For completeness, we recall the following classical result of ordinary representation theory. The proof can be found in Serre [1971], Curtis–Reiner [1981] or Feit [1982].

(42.3) THEOREM. *Let K be a field of characteristic zero such that KG is split. Let $\mathcal{F}(G, K)$ be the K-vector space of all central functions $G \to K$.*

(a) The set of all irreducible ordinary characters of G is a K-basis of the space $\mathcal{F}(G, K)$.

(b) The number $|\mathrm{Irr}(KG)|$ of irreducible ordinary characters of G (or in other words, the number of simple KG-modules up to isomorphism) is equal to the number of conjugacy classes of G.

The character of a tensor product $M \otimes N$ of two KG-modules M and N is equal to $\chi_{M\otimes N} = \chi_M \cdot \chi_N$, where the product of two K-valued functions is defined pointwise in K, that is, $(\chi_M \cdot \chi_N)(a) = \chi_M(a) \cdot \chi_N(a)$. Thus $\mathcal{F}(G, K)$ is a ring, and the character of the one-dimensional trivial representation is the unity element of this ring.

By Theorem 42.3, the values of irreducible characters form a square matrix $(\chi_M(g))$, where M runs over simple KG-modules (up to isomorphism) and g runs over elements of G up to conjugation. This matrix is called the *character table* of G. We also wish to recall a formula for the primitive central idempotents of KG, which will be used later for a characterization of blocks of defect zero. If we identify the semi-simple algebra KG with $\prod_M \mathrm{End}_K(M)$, where M runs over all simple KG-modules up to isomorphism, the unity element of the simple factor $\mathrm{End}_K(M)$ corresponding to M is a primitive idempotent e_M of the centre ZKG, and $1_{KG} = \sum_M e_M$. In other words $KGe_M = \mathrm{End}_K(M)$. We also write $e_M = e_\chi$ where $\chi = \chi_M$ is the corresponding irreducible character. The formula for e_χ is the following.

(42.4) PROPOSITION. *Let K be a field of characteristic zero such that KG is split. Let χ be an irreducible ordinary character of G and let e_χ be the corresponding primitive idempotent of ZKG. Then*

$$e_\chi = \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g^{-1}) g \,.$$

The orthogonality relations for ordinary characters can be deduced from this proposition, as follows. Since e_χ acts as the identity on the simple KG-module with character χ, but annihilates every other simple KG-module, we have $\psi(e_\chi) = \delta_{\psi,\chi}\psi(1)$ if ψ is an irreducible character. We immediately obtain from this the following orthogonality relations.

(42.5) COROLLARY. *Let K be a field of characteristic zero such that KG is split. Let χ and ψ be two irreducible ordinary characters of G. Then*

$$\frac{1}{|G|} \sum_{g \in G} \chi(g^{-1})\psi(g) = \begin{cases} 1 & \text{if } \chi = \psi, \\ 0 & \text{if } \chi \neq \psi. \end{cases}$$

One of the main purposes of modular representation theory is to obtain more information about values of characters by fixing a prime number p, connecting K with a field of characteristic p, and considering p-subgroups of G (in particular cyclic subgroups generated by an element of p-power order).

In order to make the connection with characteristic p, we first need to realize every KG-module over $\mathcal{O}$. Our next result shows that this is always possible, but we emphasize that there is no uniqueness (see Exercise 42.4).

(42.6) PROPOSITION. *Let M be a KG-module. Then there exists an $\mathcal{O}G$-lattice L such that $K \otimes_{\mathcal{O}} L \cong M$.*

Proof. Let X be a K-basis of M, which is finite (by our finite generation assumptions) and let L be the $\mathcal{O}G$-submodule of M generated by X. Then L is finitely generated as an $\mathcal{O}$-module (generated by all elements $g \cdot x$, where $g \in G$ and $x \in X$). Since L is torsion free as an $\mathcal{O}$-module (because $L \subseteq M$) and since $\mathcal{O}$ is a principal ideal domain, L is free over $\mathcal{O}$ (Proposition 1.5). Thus L is an $\mathcal{O}G$-lattice.

Any $\mathcal{O}$-basis Y of L is a K-basis of M, because on the one hand L generates M as a K-vector space (by our choice of X), and on the other hand any K-linear relation among the elements of Y yields an $\mathcal{O}$-linear relation by clearing the denominators. It follows that the surjective map

$$K \otimes_{\mathcal{O}} L \longrightarrow M \,, \qquad \lambda \otimes v \mapsto \lambda v$$

is an isomorphism, because both KG-modules are K-vector spaces of the same dimension. $\square$

Consequently the character χ_M of a KG-module M has values in $\mathcal{O}$ on elements $g \in G$. Indeed the trace of g acting on an $\mathcal{O}G$-lattice necessarily has values in $\mathcal{O}$. Therefore $\chi_M(a) \in \mathcal{O}$ for every $a \in \mathcal{O}G$. This is also a consequence of the following more precise result.

(42.7) LEMMA. *Let χ_M be the character of a KG-module M, let $g \in G$, and let n be the order of g. Then $\chi_M(g)$ is a sum of n-th roots of unity. Moreover $\chi_M(g) \in \mathcal{O}$.*

Proof. Since $g^n = 1$, the minimal polynomial of the action of g on M divides $X^n - 1$. Thus the eigenvalues of g are n-th roots of unity and the result follows since the trace of g is a sum of eigenvalues. For the additional statement, note that any root of unity is integral over $\mathbb{Z}$, hence over $\mathcal{O}$. Therefore $\chi_M(g)$ lies in $\mathcal{O}$ since $\mathcal{O}$ is integrally closed (because $\mathcal{O}$ is a principal ideal domain). Alternatively let L be an $\mathcal{O}G$-lattice such that $K \otimes_{\mathcal{O}} L \cong M$ (Proposition 42.6) and compute $\chi_M(g)$ with respect to an $\mathcal{O}$-basis of L. Then clearly $\chi_M(g) = \mathrm{tr}(g; L) \in \mathcal{O}$. □

If ζ is root of unity in $\mathcal{O}$, we define $\overline{\zeta} = \zeta^{-1}$ and extend this by $\mathbb{Z}$-linearity to an automorphism $a \mapsto \overline{a}$ of the subring $\mathbb{Z}[\zeta]$. This is just complex conjugation on $\mathbb{Z}[\zeta]$. Then the character χ_{M^*} of the dual module $M^* = \mathrm{Hom}_K(M, K)$ satisfies $\chi_{M^*}(g) = \chi_M(g^{-1}) = \overline{\chi_M(g)}$ (Exercise 42.1).

Our next task is to define modular characters. Let V be a kG-module. The trace of $g \in G$ acting on V does not yield a sufficiently well-behaved function because if some eigenvalue ζ appears with multiplicity p, then its contribution to the trace is $p \cdot \zeta = 0$ because k has characteristic p. The way to overcome this problem is to restrict to elements of order prime to p, for which one can lift everything to $\mathcal{O}$.

An element $s \in G$ is called *p-regular* if its order is prime to p. The set of p-regular elements of G is written G_{reg}. If $s \in G_{\mathrm{reg}}$, the cyclic group $S = <s>$ generated by s has order prime to p and the group algebra $\mathcal{O}S$ is $\mathcal{O}$-semi-simple (Theorem 17.5). By Corollary 17.6, every kS-module V lifts to an $\mathcal{O}S$-lattice L which is unique up to isomorphism. Thus one can consider the ordinary character of L, which has values in $\mathcal{O}$.

If V is a kG-module, the *modular character* ϕ_V of V (also called *Brauer character*) is the map

$$\phi_V : G_{\mathrm{reg}} \longrightarrow \mathcal{O}, \qquad \phi_V(s) = \chi_L(s),$$

where L is an $\mathcal{O}<s>$-lattice such that $L/\mathfrak{p}L \cong \mathrm{Res}^G_{<s>}(V)$ (unique up to isomorphism), and where $\chi_L(s)$ denotes the ordinary character of L, that is, the trace of the endomorphism s acting on L. Note that if p does not divide $|G|$, then V, with its full kG-module structure, lifts uniquely to an $\mathcal{O}G$-lattice L (Corollary 17.6) and ϕ_V coincides with the ordinary character χ_L.

A conjugate $t = gsg^{-1}$ of a p-regular element s is again p-regular. If L is an $\mathcal{O}{<}s{>}$-lattice such that $L/\mathfrak{p}L \cong \mathrm{Res}^G_{<s>}(V)$, then the conjugate lattice ${}^gL$ is an $\mathcal{O}{<}t{>}$-lattice such that ${}^gL/\mathfrak{p}({}^gL) \cong \mathrm{Res}^G_{<t>}(V)$. It follows easily from this that $\phi_V(s) = \phi_V(t)$ (Exercise 42.2), so that ϕ_V is constant on each p-regular conjugacy class. In other words ϕ_V is a central function on G_{reg}.

If W is a submodule of a kG-module V, then $\phi_V = \phi_W + \phi_{V/W}$ (Exercise 42.2). By induction, it follows that ϕ_V only depends on the composition factors of V. This reduces to the case of a simple kG-module. The modular character ϕ_V of a simple kG-module V is called an *irreducible modular character* of G. In analogy with ordinary characters, we mention for completness the following result about modular characters. The proof can be found in Serre [1971], Curtis–Reiner [1981] or Feit [1982].

(42.8) THEOREM. *Let $\mathcal{F}(G_{\mathrm{reg}}, K)$ be the K-vector space of all central functions $G_{\mathrm{reg}} \to K$.*

(a) The set of all irreducible modular characters of G is a K-basis of the space $\mathcal{F}(G_{\mathrm{reg}}, K)$.

(b) The number $|\,\mathrm{Irr}(kG)|$ of irreducible modular characters of G (or in other words, the number of simple kG-modules up to isomorphism) is equal to the number of p-regular conjugacy classes of G.

One can in fact prove more precisely that the set of all irreducible modular characters of G is an $\mathcal{O}$-basis of the $\mathcal{O}$-module $\mathcal{F}(G_{\mathrm{reg}}, \mathcal{O})$ of all central functions $G_{\mathrm{reg}} \to \mathcal{O}$.

There are also orthogonality relations for modular characters. Every simple kG-module V has a projective cover P_V and we consider the modular character ϕ_{P_V} of P_V. The modular orthogonality relations are the following.

(42.9) PROPOSITION. *Let V and W be two simple kG-modules, and let P_V be the projective cover of V. Then*

$$\frac{1}{|G|} \sum_{g \in G_{\mathrm{reg}}} \phi_{P_V}(g)\phi_W(g^{-1}) = \begin{cases} 1 & \text{if } V \cong W, \\ 0 & \text{if } V \ncong W. \end{cases}$$

The next result is an important property of projective modules. Every projective kG-module $\overline{P}$ can be lifted to a projective $\mathcal{O}G$-lattice P (Corollary 5.2). By definition of modular characters, $\phi_{\overline{P}}(s) = \chi_P(s)$, so that $\phi_{\overline{P}}$ is just the restriction to G_{reg} of the ordinary character χ_P. If

$\overline{P} = \overline{P}_V$ is the projective cover of a simple kG-module V, then P_V is the projective cover of V as an $\mathcal{O}G$-module. Every projective $\mathcal{O}G$-lattice is a direct sum of such indecomposable projective modules P_V. A proof of the first statement in the following proposition will be given in Exercise 43.2.

(42.10) PROPOSITION. *Let $\mathcal{F}(G|G_{\mathrm{reg}}, K)$ be the K-vector space of all central functions $G \to K$ which vanish outside G_{reg}.*

(a) For every projective $\mathcal{O}G$-lattice P, the character χ_P vanishes outside G_{reg}. In other words we have $\chi_P \in \mathcal{F}(G|G_{\mathrm{reg}}, K)$.

(b) The set of all characters χ_P is a K-basis of $\mathcal{F}(G|G_{\mathrm{reg}}, K)$, where P runs over the set of all indecomposable projective $\mathcal{O}G$-lattices (up to isomorphism).

We now introduce the decomposition numbers. Let M be a simple KG-module with character χ. By Proposition 42.6, there exists an $\mathcal{O}G$-lattice L such that $K \otimes_{\mathcal{O}} L \cong M$ (but L is not uniquely determined up to isomorphism, see Exercise 42.4). Then $\overline{L} = L/\mathfrak{p}L$ is a kG-module. For any simple kG-module V, we let $d(M, V)$ be the multiplicity of V as a composition factor of $\overline{L}$. We are going to see below that $d(M, V)$ does not depend on the choice of the $\mathcal{O}G$-lattice L. If ϕ is the modular character of V, we also write $d(\chi, \phi) = d(M, V)$. When M runs over the simple KG-modules up to isomorphism, and V runs over the simple kG-modules up to isomorphism, the integers $d(M, V)$ are called the *decomposition numbers* of G, and the matrix $(d(M, V))$ is called the *decomposition matrix.* For the important interpretation of $(d(M, V))$ as the matrix of a linear map between Grothendieck groups (called the decomposition map), we refer the reader to Exercise 42.5 and to the books by Serre [1971], Curtis–Reiner [1981] or Feit [1982].

It is easy to interpret the decomposition numbers in terms of characters. Let s be a p-regular element of G. Since L lifts $\overline{L}$, the value at s of the modular character of $\overline{L}$ is by construction the value at s of the ordinary character of L, which is just the character χ of $M \cong K \otimes_{\mathcal{O}} L$. In other words the modular character $\phi_{\overline{L}}$ of $\overline{L}$ is the restriction of χ to p-regular elements, which we write $d(\chi)$ and call the decomposition of χ. Then $d(\chi) = \phi_{\overline{L}}$ is the sum over all composition factors V of $\overline{L}$ of the irreducible modular characters ϕ_V. In other words

$$d(\chi) = \sum_{\phi} d(\chi, \phi)\phi\,,$$

where ϕ runs over the irreducible modular characters of G. By the linear independence of modular characters (Theorem 42.8), the integers $d(\chi, \phi)$ are uniquely determined as the coefficients of this linear combination. This shows that $d(\chi, \phi)$ only depends on χ (or M), not on the choice of L.

If the simple KG-module M belongs to a block b of $\mathcal{O}G$, then the $\mathcal{O}G$-lattice L also belongs to b, and so does $\overline{L}$ and every composition factor of $\overline{L}$. Thus the only modular characters occurring in $d(\chi)$ belong to b if χ belongs to b, or in other words $d(\chi,\phi)=0$ if χ and ϕ belong to distinct blocks. When χ and ϕ run over irreducible characters associated with b, the numbers $d(\chi,\phi)$ are called the decomposition numbers of the block b. Thus the decomposition matrix decomposes into "blocks" according to the blocks of G: each diagonal "block" is the decomposition matrix of a block of G and each entry outside the diagonal "blocks" is zero.

We already know that the Cartan matrix of a block algebra $kG\overline{b}$ is symmetric (Exercise 6.5), because $kG\overline{b}$ is a symmetric algebra. We now extend considerably this property and state without proof another basic result of modular representation theory. As usual the proof can be found in the books by Serre [1971], Curtis–Reiner [1981] or Feit [1982]. Note that the Cartan matrix of $kG\overline{b}$ is indexed by the simple $kG\overline{b}$-modules (up to isomorphism), and so it can also be indexed by the irreducible modular characters associated with b. We denote by D^t the transpose of a matrix D.

(42.11) THEOREM. *Suppose that K is large enough in order that KG be split. Let b be a block of $\mathcal{O}G$ and let $\overline{b}$ be its image in kG. Let D be the decomposition matrix of b and let C be the Cartan matrix of $kG\overline{b}$.*
(a) We have $D^tD=C$. In particular C is symmetric.
(b) C is non-singular and has determinant a power of p.
(c) For every irreducible modular character ϕ associated with b, there exist integers n_χ such that $\phi=\sum_\chi n_\chi d(\chi)$, where χ runs over the set of irreducible ordinary characters associated with b.

By summing up over all blocks of $\mathcal{O}G$, the same result holds for the full decomposition matrix of $\mathcal{O}G$ and the full Cartan matrix of kG. Statement (c) is best interpreted as the surjectivity of the decomposition map between Grothendieck groups. Note that the decomposition matrix is not a square matrix: it has rows indexed by the ordinary characters χ belonging to b, and columns indexed by the modular characters ϕ in b. The non-singularity of C implies that the rank of D is maximum, and equal to the number of columns. In particular this number is less than or equal to the number of rows.

As an application of this result (and in order to prove something in this section!), we end with a characterization of blocks of defect zero in terms of ordinary representation theory. We let $|G|_p$ be the p-part of the order of the group, or in other words the order of a Sylow p-subgroup of G.

(42.12) PROPOSITION. *Suppose that* K *is large enough in order that* KG *be split. Let* M *be a simple* KG*-module belonging to a block* b *of* $\mathcal{O}G$. *The following conditions are equivalent.*

(a) b *is a block of defect zero.*

(b) $|G|_p$ *divides* $\dim_K(M)$.

(c) M *is the unique simple* KGb*-module (up to isomorphism).*

Proof. Let $\overline{b}$ denote the image of b in kG.

(a) $\Rightarrow$ (b). There exists an $\mathcal{O}G$-lattice L such that $K \otimes_{\mathcal{O}} L \cong M$ (Proposition 42.6), and we let $\overline{L} = L/\mathfrak{p}L$. Since b has defect zero, $kG\overline{b}$ is a simple k-algebra (Theorem 39.1), and so every $kG\overline{b}$-module is projective. By Exercise 21.2, $|G|_p$ divides the dimension of every projective kG-module. Thus $|G|_p$ divides $\dim_k(\overline{L}) = \dim_{\mathcal{O}}(L) = \dim_K(M)$.

(b) $\Rightarrow$ (c). By Proposition 42.4, the primitive idempotent of ZKG corresponding to M is

$$e_\chi = \frac{\chi(1)}{|G|} \sum_{g\in G} \chi(g^{-1})g\,,$$

where χ is the character of M. Since $|G|_p$ divides $\chi(1)$ by assumption, the denominator of the rational number $\chi(1)/|G|$ is prime to p, hence invertible in $\mathcal{O}$. Thus $\chi(1)/|G| \in \mathcal{O}$ and it follows that $e_\chi \in \mathcal{O}G$. Hence e_χ is an idempotent of $Z\mathcal{O}G$, necessarily primitive since it is primitive in ZKG. In other words $e_\chi = b$. Therefore $KGb = KGe_\chi$ consists of a single simple factor of KG. In other words M is the unique simple KGb-module (up to isomorphism).

(c) $\Rightarrow$ (a). The decomposition matrix D of the block b has only one row by assumption. Thus it has only one column by a remark above, and $D = (m)$ for some positive integer m. By the third statement of Theorem 42.11, there exists an integer n such that $nm = 1$. Thus $m = 1$ and it follows from Theorem 42.11 that $C = (1)$. This means that the unique projective $kG\overline{b}$-module is simple. Hence every $kG\overline{b}$-module is projective and so $kG\overline{b}$ is a simple k-algebra. By Theorem 39.1, b has defect zero. □

Exercises

Throughout these exercises, $\mathcal{O}$ denotes a discrete valuation ring of characteristic zero satisfying Assumption 42.1, K is the field of fractions of $\mathcal{O}$, and k is the residue field of $\mathcal{O}$.

(42.1) Let M be a KG-module, let $M^* = \mathrm{Hom}_K(V, K)$ be the dual module, and let χ_M and χ_{M^*} be the ordinary characters of M and M^* respectively. Prove that $\chi_{M^*}(g) = \chi_M(g^{-1}) = \overline{\chi_M(g)}$ for every $g \in G$ (where $\overline{a}$ denotes the complex conjugate of the complex number a).

(42.2) Let V be a kG-module and let ϕ_V be its modular character.
 (a) Show that $\phi_V(gsg^{-1}) = \phi_V(s)$, where $s \in G_{\mathrm{reg}}$ and $g \in G$.
 (b) If W is a submodule of V, show that $\phi_V = \phi_W + \phi_{V/W}$.

(42.3) Prove Theorems 42.3, 42.8 and 42.11. [Hint: Read other textbooks.]

(42.4) Let G be the symmetric group on 3 letters, generated by an element u of order 3 and an element s of order 2. Take $p = 3$. This example is a complement to Example 26.5.
 (a) Consider the 2-dimensional $\mathcal{O}G$-lattice L given by the representation

$$u \mapsto \begin{pmatrix} -1/2 & 3/2 \\ -1/2 & -1/2 \end{pmatrix}, \qquad s \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

 Prove that $K \otimes_{\mathcal{O}} L$ is a simple KG-module.
 (b) Consider the 2-dimensional $\mathcal{O}G$-lattice L' given by the representation

$$u \mapsto \begin{pmatrix} -1/2 & -1/2 \\ 3/2 & -1/2 \end{pmatrix}, \qquad s \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

 Prove that $K \otimes_{\mathcal{O}} L' \cong K \otimes_{\mathcal{O}} L$. [Hint: In $K \otimes_{\mathcal{O}} L$, multiply the first basis element by 3 and change the sign of the second.]
 (c) Prove that $L \not\cong L'$ by showing that $L'/\mathfrak{p}L'$ has a one-dimensional trivial submodule, while $L/\mathfrak{p}L$ does not.
 (d) Check that $L/\mathfrak{p}L$ and $L'/\mathfrak{p}L'$ have the same composition factors.

(42.5) Let A be an $\mathcal{O}$-algebra which is free as an $\mathcal{O}$-module.
 (a) Let $R(K \otimes_{\mathcal{O}} A)$ be the Grothendieck group of $K \otimes_{\mathcal{O}} A$, that is, the quotient of the free abelian group on isomorphism classes $[M]$ of finitely generated $K \otimes_{\mathcal{O}} A$-modules M by the subgroup generated by all expressions $[M] - [M'] - [M'']$ where $0 \to M' \to M \to M'' \to 0$ is an exact sequence. Prove that $R(K \otimes_{\mathcal{O}} A)$ is free abelian generated by the isomorphism classes of simple $K \otimes_{\mathcal{O}} A$-modules. Prove the

similar result for the Grothendieck group $R(k \otimes_{\mathcal{O}} A)$. [Hint: Use the Jordan–Hölder theorem.]

(b) Prove that for any $K \otimes_{\mathcal{O}} A$-module M, there exists an A-lattice L such that $K \otimes_{\mathcal{O}} L \cong M$. [Hint: Use an $\mathcal{O}$-basis of A and a K-basis of M. Proceed as in Proposition 42.6.]

(c) For every $K \otimes_{\mathcal{O}} A$-module M, choose an A-lattice L such that $K \otimes_{\mathcal{O}} L \cong M$, let $\overline{L} = L/\mathfrak{p}L \cong k \otimes_{\mathcal{O}} L$, and define the *decomposition map*

$$d : R(K \otimes_{\mathcal{O}} A) \longrightarrow R(k \otimes_{\mathcal{O}} A)$$

by $d([M]) = [\overline{L}] \in R(k \otimes_{\mathcal{O}} A)$. Prove that $[\overline{L}]$ is independent of the choice of L and that d is a well-defined group homomorphism. [Hint: Read Serre [1971], Section 15, or Curtis–Reiner [1981], Section 16C, or Feit [1982], Section I.17.]

(d) Prove that if $A = \mathcal{O}G$, then the matrix of d, with respect to the bases of part (a), is the decomposition matrix of $\mathcal{O}G$.

(e) Let B be another $\mathcal{O}$-algebra, free as an $\mathcal{O}$-module, and assume that A and B are Morita equivalent. Prove that the Morita equivalence induces group isomorphisms $R(K \otimes_{\mathcal{O}} A) \xrightarrow{\sim} R(K \otimes_{\mathcal{O}} B)$ as well as $R(k \otimes_{\mathcal{O}} A) \xrightarrow{\sim} R(k \otimes_{\mathcal{O}} B)$ such that the following diagram commutes

$$\begin{array}{ccc} R(K \otimes_{\mathcal{O}} A) & \xrightarrow{\sim} & R(K \otimes_{\mathcal{O}} B) \\ \downarrow d_A & & \downarrow d_B \\ R(k \otimes_{\mathcal{O}} A) & \xrightarrow{\sim} & R(k \otimes_{\mathcal{O}} B), \end{array}$$

where d_A and d_B denote the respective decomposition maps. [Hint: Remember that a Morita equivalence preserves exact sequences. Use also Exercise 9.7.]

Notes on Section 42

All the results about modular characters are classical results of Brauer. Proposition 42.12 goes back to Brauer and Nesbitt [1941].

§ 43 GENERALIZED DECOMPOSITION NUMBERS

The purpose of this section is to describe the values of ordinary characters in terms of p-elements and their centralizers, by means of modular characters and generalized decomposition numbers. A crucial result asserts that these numbers for a block b can be computed from a source algebra of b. We continue with a complete discrete valuation ring $\mathcal{O}$ of characteristic zero, satisfying Assumption 42.1, and we let K be the field of fractions of $\mathcal{O}$. Moreover we assume that K is large enough in order that KG be split.

We define a *pointed element* on a G-algebra A to be a pair (u, δ), always written u_δ, where $u \in G$ and $\delta \in \mathcal{P}(A^{<u>})$. Here $<u>$ denotes the cyclic subgroup generated by u. If moreover δ is a local point, then u_δ is called a *local pointed element*. This notion is slightly different from the corresponding notion of pointed group $<u>_\delta$. Indeed two distinct generators u and u' of $<u>$ give rise to two distinct pointed elements u_δ and u'_δ, but there is only one pointed group $<u>_\delta$. Clearly G acts by conjugation on the set of pointed elements on A, by defining ${}^g(u_\delta) = ({}^g u)_{{}^g\delta}$.

An element of G is called a *p-element* if its order is a power of p. Note that local pointed elements u_δ exist only when u is a p-element, because $<u>$ has to be a p-group. For the group algebra $\mathcal{O}G$, a local pointed element u_δ on $\mathcal{O}G$ corresponds to an irreducible representation of $kC_G(u)$ (by Corollary 37.6). Moreover u_δ is said to be *associated* with a block b of $\mathcal{O}G$ if the corresponding pointed group $<u>_\delta$ is associated with b.

If u_δ is a pointed element and H_α is a pointed group on A, we write $u_\delta \in H_\alpha$ if the relation $<u>_\delta \leq H_\alpha$ holds. All p-elements of G are contained in some Sylow p-subgroup of G. In analogy, if b is a block of $\mathcal{O}G$, then all local pointed elements u_δ on $\mathcal{O}Gb$ satisfy $u_\delta \in P_\gamma$ for some defect P_γ of b (because the defects are the maximal local pointed groups on $\mathcal{O}Gb$ by Theorem 18.3).

If χ_M is the character of a KG-module M and if u_δ is a pointed element on $\mathcal{O}G$, the value of χ_M on u_δ is defined to be

$$\chi_M(u_\delta) = \chi_M(uj)\,,$$

where $j \in \delta$. This definition is independent of the choice of j because, for $a \in (\mathcal{O}G^{<u>})^*$, we have $\chi_M(uaja^{-1}) = \chi_M(auja^{-1}) = \chi_M(uj)$. Since u commutes with j, we also have $\chi_M(u_\delta) = \chi_M(ju)$. Note that it is essential here to view characters as functions defined on the whole of KG, not just on the basis elements. However, the next easy result shows that $\chi_M(uj)$ can also be defined as the value of another character at the basis element u. Instead of working with $<u>$, we state the result for an arbitrary subgroup H.

(43.1) LEMMA. *Let* χ_M *be the character of a* KG*-module* M, *let* H *be a subgroup of* G, *and let* $j \in (\mathcal{O}G)^H$ *be an idempotent. Then* jM *is a direct summand of* $\mathrm{Res}^G_H(M)$ *and* $\chi_M(uj) = \chi_{jM}(u)$ *for all* $u \in H$.

Proof. Since the action of j is the identity on jM and zero on $(1-j)M$, we have

$$\begin{aligned}\chi_M(uj) &= \mathrm{tr}(uj; jM \oplus (1-j)M) = \mathrm{tr}(uj; jM) + \mathrm{tr}(uj; (1-j)M) \\ &= \mathrm{tr}(u; jM) = \chi_{jM}(u),\end{aligned}$$

as required. □

We also have the following elementary result.

(43.2) LEMMA. *Let* M *be a* KG*-module and let* u_δ *be a pointed element on* $\mathcal{O}G$.

(a) *If* M *belongs to a block* b *and if* u_δ *is not associated with* b, *then* $\chi_M(u_\delta) = 0$.

(b) *If* $g \in G$, *then* $\chi_M({}^g(u_\delta)) = \chi_M(u_\delta)$.

Proof. (a) Let $j \in \delta$. To say that u_δ is not associated with b means that $jb = 0$. On the other hand the action of j on M is equal to the action of jb, because b acts as the identity. Therefore $\chi_M(uj) = \chi_M(ujb) = 0$.

(b) Let $j \in \delta$. Then

$$\chi_M({}^g(u_\delta)) = \chi_M(({}^gu)_{{}^g\delta}) = \mathrm{tr}({}^gu\,{}^gj; M) = \mathrm{tr}({}^g(uj); M) = \mathrm{tr}(uj; M),$$

and the result follows. □

The next basic fact is that the values $\chi_M(u_\delta)$ vanish if the point δ is not local.

(43.3) PROPOSITION. *Let* M *be a* KG*-module and let* u_δ *be a pointed element on* $\mathcal{O}G$. *If the point* δ *is not local, then* $\chi_M(u_\delta) = 0$.

Proof. Let $j \in \delta$ and $U = \langle u \rangle$. Since δ is not local, we have $j \in \mathfrak{p}(\mathcal{O}G)^U + \sum_{V<U}(\mathcal{O}G)^U_V$, and therefore by Rosenberg's lemma (Proposition 4.9), $j \in (\mathcal{O}G)^U_V$ for some proper subgroup $V < U$ (note that $j \notin \mathfrak{p}(\mathcal{O}G)^U$ since $\mathfrak{p}(\mathcal{O}G)^U \subseteq J((\mathcal{O}G)^U)$). Since U is a p-group, we can apply the primitivity theorem for idempotents (Theorem 23.1). Thus there exists an idempotent $i \in (\mathcal{O}G)^V$ such that $j = t^U_V(i)$ and ${}^xi\,i = 0$ for every $x \in U - V$. The orthogonal decomposition $j = \sum_{x\in[U/V]} {}^x i$ in $\mathcal{O}G$ yields a decomposition of the KU-module jM as a K-vector space

$$jM = \bigoplus_{x\in[U/V]} {}^x iM = \bigoplus_{x\in[U/V]} xiM \,,$$

(and therefore $jM \cong \mathrm{Ind}_V^U(iM)$). Since U is a cyclic group generated by u , the proper subgroup V is generated by u^m for some $m \geq 2$, and the direct sum runs over $x = u^r$, for $0 \leq r \leq m-1$. Thus u permutes cyclically the direct summands of the decomposition. Therefore, choosing a basis of M consisting of the union of bases of the direct summands, we see that the matrix of the action of u on jM has zeros on the diagonal. It follows that $\mathrm{tr}(u; jM) = 0$, and by Lemma 43.1, we obtain $\chi_M(uj) = \chi_{jM}(u) = 0$. □

Clearly $\chi_M(u_\delta)$ behaves additively with respect to M, and so it suffices to consider the numbers $\chi_M(u_\delta)$ when M is a simple KG-module. If M is a simple KG-module associated with a block b and u_δ is a local pointed element associated with b , the number $\chi_M(u_\delta)$ is called a *generalized decomposition number* of b . The *generalized decomposition matrix* of b is the matrix $(\chi(u_\delta))$, where χ runs over the irreducible ordinary characters of the block b , and u_δ runs over representatives of the G-conjugacy classes of local pointed elements on $\mathcal{O}G$ associated with b . Note that this makes sense since χ is constant on G-conjugacy classes by Lemma 43.2.

For the whole group algebra $\mathcal{O}G$, the *generalized decomposition matrix* of $\mathcal{O}G$ is the matrix $(\chi(u_\delta))$, where χ runs over the irreducible ordinary characters of G , and u_δ runs over the local pointed elements on $\mathcal{O}G$ up to G-conjugation. Lemma 43.2 implies that this matrix decomposes into “blocks”, with zero entries outside the diagonal “blocks”, each diagonal “block” being the generalized decomposition matrix of a block of $\mathcal{O}G$. Later in this section, we shall prove that the generalized decomposition matrix of a block b is a square matrix, and that it can be computed from a source algebra of b .

Note that every generalized decomposition number $\chi_M(u_\delta)$ is a sum of p^m-th roots of unity where p^m is the order of u . Indeed $\chi_M(u_\delta) = \chi_{jM}(u)$ by Lemma 43.1 and every eigenvalue of the action of u on jM is a p^m-th root of unity.

In the special case $u = 1$, we obtain the ordinary decomposition numbers of b defined in the previous section. This is not clear yet, but will be a consequence of Brauer's second main theorem below. This theorem gives a decomposition of the values of ordinary characters in terms of generalized decomposition numbers and modular characters.

The problem is to find a decomposition of the value $\chi(us)$, where χ is an ordinary character, u is a p-element of G, and s is a p-regular element of $C_G(u)$. Recall that any element $g \in G$ can be written uniquely as a product $g = us$ with u and s as above. Indeed let n be the order of g and let $n = qm$, where q is a power of p and m is prime to p. Then $aq + bm = 1$ for some integers a and b, and so $g = g^{bm}g^{aq}$. Then $u = g^{bm}$ has order q (because g^m has order q and b is prime to q). Similarly $s = g^{aq}$ has order m and centralizes u. When u runs over representatives of conjugacy classes of p-elements of G and s runs over representatives of p-regular conjugacy classes of $C_G(u)$, then us runs over representatives of conjugacy classes of G.

Every local pointed element u_δ corresponds to a simple $kC_G(u)$-module, namely the multiplicity module $V(\delta)$ (by Corollary 37.6). We denote by ϕ_δ the modular character of $V(\delta)$. It is an irreducible modular character of $kC_G(u)$. With this notation, we can now prove the main result of this section. We state it for an arbitrary character χ, but of course the numbers $\chi(u_\delta)$ are the generalized decomposition numbers only in the case of an irreducible character. In fact the result for irreducible characters implies the general result by linearity.

(43.4) THEOREM (Brauer's second main theorem). *Let χ be the character of a KG-module, let u be a p-element of G, and let s be a p-regular element of $C_G(u)$. Then*

$$\chi(us) = \sum_{\delta \in \mathcal{LP}((\mathcal{O}G)^{<u>})} \chi(u_\delta)\phi_\delta(s)\,,$$

where ϕ_δ denotes the modular character of the $kC_G(u)$-module $V(\delta)$.

Proof. Let $U = <u>$ and $S = <s>$. Since s is p-regular, p does not divide $|S|$ and therefore $\mathcal{O}S$ is $\mathcal{O}$-semi-simple (Theorem 17.5). Thus $\mathcal{O}S$ is an $\mathcal{O}$-semi-simple subalgebra of $(\mathcal{O}G)^U$ (because $S \le C_G(U)$). By Theorem 7.3, there exists a maximal $\mathcal{O}$-semi-simple subalgebra T of $(\mathcal{O}G)^U$ containing $\mathcal{O}S$. Writing $T(\delta)$ for the $\mathcal{O}$-simple factor of T corresponding to the point δ of $(\mathcal{O}G)^U$, we have

$$T = \prod_{\delta \in \mathcal{P}((\mathcal{O}G)^U)} T(\delta)\,,$$

and $T(\delta)$ maps onto the simple k-algebra $S(\delta)$, the multiplicity algebra of δ.

Let $e_\delta = 1_{T(\delta)}$, so that $1_{\mathcal{O}G} = 1_T = \sum_{\delta \in \mathcal{P}((\mathcal{O}G)^U)} e_\delta$. The algebra $e_\delta(\mathcal{O}G)^U e_\delta$ has a unique point (which we identify with δ) and $T(\delta)$ is an $\mathcal{O}$-simple subalgebra of $e_\delta(\mathcal{O}G)^U e_\delta$. By Proposition 7.5, there is an isomorphism

$$(43.5)\qquad T(\delta)\otimes_{\mathcal{O}} C(T(\delta)) \xrightarrow{\sim} e_\delta(\mathcal{O}G)^U e_\delta\,, \qquad t\otimes a\mapsto ta\,,$$

where $C(T(\delta))$ denotes the centralizer of $T(\delta)$ in $e_\delta(\mathcal{O}G)^U e_\delta$.

After this preparation, we can start decomposing χ . Let M be a KG-module with character $\chi_M = \chi$ and let L be an $\mathcal{O}G$-lattice such that $K\otimes_{\mathcal{O}} L\cong M$. We view L as an $(\mathcal{O}G)^U$-module by restriction, which we denote by L again for simplicity. Then we have a decomposition

$$L=\bigoplus_{\delta\in\mathcal{P}((\mathcal{O}G)^U)} e_\delta L\,,$$

and $e_\delta L$ is an $e_\delta(\mathcal{O}G)^U e_\delta$-module. By Proposition 7.6, the tensor product decomposition 43.5 has its counterpart for modules. More precisely, if j is a primitive idempotent of $T(\delta)$ (so that $j\in\delta$), there is an isomorphism

$$T(\delta)j\otimes_{\mathcal{O}} jL \xrightarrow{\sim} e_\delta L\,, \qquad t\otimes m\mapsto tm\,.$$

Here $T(\delta)j$ is a $T(\delta)$-module and jL is a $C(T(\delta))$-module.

We have to compute the trace of us acting on L . But we have $us=\sum_{\delta\in\mathcal{P}((\mathcal{O}G)^U)} use_\delta$, and $use_\delta = e_\delta us$; indeed e_δ commutes with u because $e_\delta\in(\mathcal{O}G)^U$, and e_δ commutes with s because e_δ is a central idempotent of T and $s\in T$ by the choice of T . Thus $use_\delta\in e_\delta(\mathcal{O}G)^U e_\delta$ and we only have to consider its action on $e_\delta L$ (since its action on $e_{\delta'}L$ is obviously zero if $\delta'\neq\delta$). The image of use_δ under the inverse isomorphism 43.5 is equal to $se_\delta\otimes ue_\delta$; indeed $ue_\delta\in C(T(\delta))$ because u is central in $(\mathcal{O}G)^U$ by definition, $se_\delta\in T(\delta)$ since $s\in T$, and finally the image of $se_\delta\otimes ue_\delta$ under the isomorphism 43.5 is equal to $se_\delta ue_\delta = sue_\delta = use_\delta$. Thus we have to consider the action of se_δ on the $T(\delta)$-module $T(\delta)j$, tensored with the action of ue_δ on jL .

Summarizing our analysis so far, we have

$$\begin{aligned}\chi(us)=\operatorname{tr}(us;L) &= \sum_{\delta\in\mathcal{P}((\mathcal{O}G)^U)} \operatorname{tr}(use_\delta;e_\delta L)\\ &= \sum_{\delta\in\mathcal{P}((\mathcal{O}G)^U)} \operatorname{tr}(se_\delta\otimes ue_\delta;T(\delta)j\otimes jL)\\ &= \sum_{\delta\in\mathcal{P}((\mathcal{O}G)^U)} \operatorname{tr}(se_\delta;T(\delta)j)\cdot\operatorname{tr}(ue_\delta;jL)\,,\end{aligned}$$

because the trace behaves multiplicatively with respect to tensor products. Now the second factor in each product is easy to deal with:

$$\operatorname{tr}(ue_\delta;jL)=\operatorname{tr}(ue_\delta j;L)=\operatorname{tr}(uj;L)=\chi(uj)=\chi(u_\delta)\,.$$

By Proposition 43.3, $\chi(u_\delta) = 0$ if δ is not local, and therefore the sum now runs only over local points of $(\mathcal{O}G)^U$:

$$\chi(us) = \sum_{\delta \in \mathcal{LP}((\mathcal{O}G)^U)} \operatorname{tr}(se_\delta; T(\delta)j) \cdot \chi(u_\delta) .$$

Thus we are only left with the proof that $\operatorname{tr}(se_\delta; T(\delta)j) = \phi_\delta(s)$ for each local point δ .

By construction, $T(\delta)$ is an $\mathcal{O}$-simple lift in $(\mathcal{O}G)^U$ of the multiplicity algebra $S(\delta)$, which is an interior $C_G(U)$-algebra. Since $s \in T$ by construction of T , its image se_δ in $T(\delta)$ maps to $s{\cdot}1_{S(\delta)} \in S(\delta)$. Thus on restriction to S , the multiplicity algebra $S(\delta)$ lifts over $\mathcal{O}$ to the interior S-algebra $T(\delta)$. Turning now to modules, the multiplicity module $V(\delta)$ is isomorphic to $S(\delta)\overline{j}$, where $\overline{j}$ is the image of j (a primitive idempotent of $S(\delta)$). Thus, still on restriction to S , the $\mathcal{O}S$-lattice $T(\delta)j$ is a lift of $S(\delta)\overline{j}$. By construction of modular characters, $\operatorname{tr}(se_\delta; T(\delta)j) = \operatorname{tr}(s; T(\delta)j)$ is the value at s of the modular character of the $kC_G(U)$-module $V(\delta) \cong S(\delta)\overline{j}$. This is the definition of $\phi_\delta(s)$, as was to be shown. □

We can now prove that the ordinary decomposition numbers are the generalized decomposition numbers for $u = 1$. Indeed $C_G(u) = G$ in this case and, if χ is an irreducible character of G , the theorem for $u = 1$ says that

$$\chi(s) = \sum_\delta \chi(1_\delta)\phi_\delta(s) ,$$

and ϕ_δ runs over the modular characters of G . Now the decomposition $d(\chi)$ of χ is the restriction of χ to p-regular elements of G , and so $d(\chi) = \sum_\delta \chi(1_\delta)\phi_\delta$. By the linear independence of modular characters (Theorem 42.8), the coefficients $\chi(1_\delta)$ are precisely the decomposition numbers $d(\chi, \phi_\delta)$.

We shall prove below that the generalized decomposition numbers of a block b can be computed from a source algebra of b , and this implies that many blocks of various finite groups G have the same generalized decomposition matrix. Indeed many blocks may have the same source algebra, in which case we say that they have the same local structure. Thus the information given by the generalized decomposition numbers is “local”. In contrast, the values $\phi_\delta(s)$ of modular characters of $C_G(u)$ depend essentially on G and can vary considerably when a block runs over an equivalence class of blocks with the same local structure. Thus the values $\phi_\delta(s)$ are not part of the local information. In this way, Theorem 43.4 can be viewed as a decomposition of character values into a local part and a non-local part.

For instance, the local information given by the generalized decomposition numbers has the following consequence.

(43.6) COROLLARY. *Let χ be the character of a KG-module, let u be a p-element of G, and let s be a p-regular element of $C_G(u)$.*
(a) If χ belongs to a block b with defect group P and if no conjugate of u belongs to P, then $\chi(us) = 0$.
(b) If χ is the (unique) irreducible character belonging to a block b of defect zero, then χ vanishes outside G_{reg}.

Proof. (a) Let P_γ be a defect of b and let δ be any local point of $(\mathcal{O}G)^{<u>}$. If u_δ were associated with b, then there would exist $g \in G$ such that ${}^g(u_\delta) \in P_\gamma$, because all maximal local pointed groups on $\mathcal{O}Gb$ are conjugate (Theorem 18.3). Then ${}^gu \in P$ against our assumption. Thus every local pointed element u_δ is associated with a block b' different from b, and by Lemma 43.2, $\chi(u_\delta) = 0$. Therefore $\chi(us) = 0$ by Theorem 43.4.

(b) This is a special case of (a). Indeed let $g = us$, with u and s as in the statement. Then $g \notin G_{\text{reg}}$ if and only if $u \neq 1$. In that case u does not belong to the trivial group and (a) applies. □

Note that statement (b) is also a consequence of Proposition 42.10 (see also Exercise 43.2), because every $\mathcal{O}Gb$-lattice is projective, so that χ is the character of a projective $\mathcal{O}G$-lattice.

(43.7) REMARK. Let χ be an irreducible ordinary character of G. For a fixed p-element u, the function $s \mapsto \chi(us)$ is constant on conjugacy classes of p-regular elements of $C_G(u)$. By Theorem 42.8, this function can be uniquely written as a K-linear combination of modular characters ϕ_δ of $C_G(u)$. Brauer's classical approach consists in *defining* the generalized decomposition numbers as the coefficients in this linear combination, and then showing that the coefficient of ϕ_δ is zero if u_δ is not associated with the block b. This is the classical statement of Brauer's second main theorem. In contrast, our definition implies immediately that $\chi(u_\delta) = 0$ if u_δ is not associated with the block b (Lemma 43.2), and then the linear combination of Theorem 43.4 becomes the main statement, which we still call Brauer's second main theorem. The advantage of our definition is that it gives a direct expression for the generalized decomposition numbers. Moreover this expression will be crucial for the determination of generalized decomposition numbers from a source algebra.

The product of the decomposition matrix and its transpose is the Cartan matrix (Theorem 42.11). In order to state a similar result for the generalized decomposition matrix, we first need to define the generalized Cartan integers.

Let b be a block of $\mathcal{O}G$. If Q_δ and Q_ε are two local pointed groups on $\mathcal{O}Gb$ corresponding to the same p-subgroup Q, then $br_Q(\delta)$ and $br_Q(\varepsilon)$ are two points of $kC_G(Q)br_Q(b)$. For simplicity, we write $c_{\delta,\varepsilon}$ for the Cartan integers of this algebra. Explicitly, if $i \in \delta$ and $j \in \varepsilon$, then

$$c_{\delta,\varepsilon} = c_{br_Q(\delta),br_Q(\varepsilon)} = \dim_k(br_Q(i)kC_G(Q)br_Q(j))$$

by Proposition 5.12. We use this notation in the following definition (thus only when $Q = <u>$ is cyclic). The *generalized Cartan integers* of b are the integers

$$c(u_\delta, v_\varepsilon) = \begin{cases} 0 & \text{if the } p\text{-elements } u \text{ and } v \text{ are not conjugate,} \\ c_{\delta,\varepsilon} & \text{if } u = v, \end{cases}$$

where u_δ and v_ε run over representatives of the G-conjugacy classes of local pointed elements on $\mathcal{O}Gb$. The matrix $(c(u_\delta, v_\varepsilon))$ of generalized Cartan integers is called the *generalized Cartan matrix* of b. If we choose some ordering of local pointed elements on $\mathcal{O}Gb$ in such a way that, for every p-element u, all pointed elements u_δ are consecutive, then the generalized Cartan matrix decomposes into "blocks", with zero entries outside the diagonal "blocks", each diagonal "block" being the Cartan matrix of $kC_G(u)br_{<u>}(b)$ (with u running over representatives of conjugacy classes of p-elements). Note that each diagonal "block" decomposes in turn as the "direct sum" of all Cartan matrices of $kC_G(u)e$, where e runs over the blocks of $kC_G(u)$ appearing in a decomposition of $br_{<u>}(b)$ (that is, over the Brauer correspondents of b).

We also need some notation. If ζ is root of unity in $\mathcal{O}$, we define $\overline{\zeta} = \zeta^{-1}$ and extend this by $\mathbb{Z}$-linearity to an automorphism $a \mapsto \overline{a}$ of $\mathbb{Z}[\zeta]$. This is just complex conjugation on $\mathbb{Z}[\zeta]$. Since every generalized decomposition number is a sum of roots of unity, we can apply this automorphism to each entry of the matrix $D = (\chi(u_\delta))$, and we write $\overline{D}$ for this conjugate matrix. Also D^t denotes the transpose of D.

With this notation, we can state the result. The proof can be found in the book of Feit [1982].

(43.8) THEOREM. *Let b be a block of $\mathcal{O}G$, let D be the generalized decomposition matrix of b, and let C be the generalized Cartan matrix of b. Then $\overline{D}^t D = C$.*

For the whole group algebra $\mathcal{O}G$, the generalized Cartan matrix is defined similarly and decomposes into "blocks" according to the blocks of $\mathcal{O}G$. By summing up over all blocks of $\mathcal{O}G$, the same theorem holds for the generalized decomposition matrix of $\mathcal{O}G$ and the generalized Cartan matrix of $\mathcal{O}G$.

We use Theorem 43.8 to prove that D is a square matrix and is non-singular.

(43.9) PROPOSITION. *Let b be a block of $\mathcal{O}G$. The number of irreducible ordinary characters associated with b is equal to the number of G-conjugacy classes of pointed elements on $\mathcal{O}Gb$. In other words the generalized decomposition matrix D of b is a square matrix. Moreover D is non-singular.*

Proof. We first prove this for the generalized decomposition matrix $D_{\mathcal{O}G}$ of $\mathcal{O}G$, which is decomposed into diagonal "blocks" D according to the blocks of $\mathcal{O}G$ (Lemma 43.2). Let us first fix a p-element u. The number of local points δ of $(\mathcal{O}G)^{<u>}$ is equal to the number of irreducible modular characters ϕ_δ of $kC_G(u)$, that is, the number of conjugacy classes of p-regular elements s of $kC_G(u)$ (Theorem 42.8). Now, taking one p-element u in each conjugacy class of p-elements, we obtain that the number of conjugacy classes of pointed elements u_δ is equal to the number of pairs (u,s) where s is a p-regular element of $C_G(u)$ up to conjugation. But this number is clearly the number of conjugacy classes of G (because any $g \in G$ can be written uniquely as $g = us$), that is, the number of irreducible ordinary characters of G (Theorem 42.3). This proves the result for $\mathcal{O}G$.

Since the generalized decomposition matrix $D_{\mathcal{O}G}$ of $\mathcal{O}G$ is a square matrix, since $\overline{D}^t_{\mathcal{O}G} D_{\mathcal{O}G}$ is a direct sum of Cartan matrices (by Theorem 43.8 above), and since every Cartan matrix is non-singular by Theorem 42.11, $D_{\mathcal{O}G}$ is non-singular. Now if a square matrix is decomposed into "blocks" D with zero entries outside the diagonal "blocks", then each diagonal "block" D must be a square matrix in order that the full matrix be non-singular. This proves that the generalized decomposition matrix D of a block is a square matrix, and that it is non-singular. □

We want to prove that the generalized decomposition numbers of a block b can be determined from a source algebra of b. To this end we introduce an ad hoc equivalence relation between local pointed elements. Let A be an interior G-algebra, assume that A is free as an $\mathcal{O}$-module, and consider the K-algebra $K \otimes_{\mathcal{O}} A$. The *character* χ_M of a $K \otimes_{\mathcal{O}} A$-module M is defined as before by $\chi_M(a) = \mathrm{tr}(a; M)$ for every $a \in K \otimes_{\mathcal{O}} A$, and χ_M is called *irreducible* if M is simple. Also, for every local pointed element u_δ on A, we define $\chi_M(u_\delta) = \chi_M(uj)$ where $j \in \delta$, and this is independent of the choice of j. Now two local pointed elements u_δ and v_ε on A are said to be *equivalent* if $\chi(u_\delta) = \chi(v_\varepsilon)$ for every irreducible character χ of $K \otimes_{\mathcal{O}} A$.

Now we can show how to compute generalized decomposition numbers from a source algebra.

(43.10) PROPOSITION. *Let* b *be a block of* $\mathcal{O}G$ *with defect* P_γ , *source algebra* $(\mathcal{O}Gb)_\gamma$, *and associated embedding* $\mathcal{F}_\gamma : (\mathcal{O}Gb)_\gamma \to \mathrm{Res}^G_P(\mathcal{O}Gb)$.

(a) *Let* χ_M *be the character of a simple* KGb*-module* M *and let* χ_N *be the character of the simple* $K \otimes_{\mathcal{O}} (\mathcal{O}Gb)_\gamma$*-module* N , *where* N *is the Morita correspondent of* M . *Let* u_δ *be a local pointed element on* $(\mathcal{O}Gb)_\gamma$ *and let* $u_{\delta'}$ *be its image in* $\mathcal{O}Gb$. *Then*

$$\chi_M(u_{\delta'}) = \chi_N(u_\delta) .$$

(b) *Consider the matrix* $D = (\chi(u_\delta))$, *where* χ *runs over the set of irreducible characters of* $K \otimes_{\mathcal{O}} (\mathcal{O}Gb)_\gamma$ *and* u_δ *runs over representatives of equivalence classes of pointed elements on* $(\mathcal{O}Gb)_\gamma$. *Then* D *is the generalized decomposition matrix of* b .

Proof. (a) We can choose $(\mathcal{O}Gb)_\gamma = i\mathcal{O}Gi$, where $i \in \gamma$, and take for $\mathcal{F}_\gamma$ the exomorphism containing the inclusion $i\mathcal{O}Gi \to \mathcal{O}Gb$. For every $\mathcal{O}Gb$-module M , the Morita correspondent of M is the $i\mathcal{O}Gi$-module $N = iM$, and the same holds for the Morita equivalence between KGb and $iKGi \cong K \otimes_{\mathcal{O}} i\mathcal{O}Gi$. Let $j \in \delta$, so that $ji = ij = j$ (because $j \in i\mathcal{O}Gi$). Since $\mathcal{F}_\gamma$ contains the inclusion, we also have $j \in \delta'$, and therefore

$$\chi_M(u_{\delta'}) = \mathrm{tr}(uj; M) = \mathrm{tr}(uji; M) = \mathrm{tr}(uj; iM) = \chi_N(u_\delta) ,$$

as was to be shown.

(b) Let D' be the generalized decomposition matrix of b . By (a), every entry of D is an entry of D' . Thus the main problem is to prove that the rows and columns of D and D' are indexed by sets which are in bijection. This is clear for the rows, because the Morita equivalence induces a bijection between isomorphism classes of simple KGb-modules and isomorphism classes of simple $iKGi$-modules. Turning now to columns, let us write $\mathcal{LPE}(A)$ for the set of local pointed elements on a G-algebra A . The columns of D' are indexed by the set $\mathcal{LPE}(\mathcal{O}Gb)/G$ of G-conjugacy classes of local pointed elements on $\mathcal{O}Gb$, while those of D are indexed by the set $\mathcal{LPE}(i\mathcal{O}Gi)/\!\sim$ of equivalence classes of local pointed elements on $i\mathcal{O}Gi$. The embedding $\mathcal{F}_\gamma$ induces an injective map

$$\phi : \mathcal{LPE}(i\mathcal{O}Gi) \longrightarrow \mathcal{LPE}(\mathcal{O}Gb) , \qquad u_\delta \mapsto u_{\delta'} .$$

This induces an injective map

$$\overline{\phi} : \mathcal{LPE}(i\mathcal{O}Gi)/\!\sim \;\longrightarrow\; \mathcal{LPE}(\mathcal{O}Gb)/\!\sim ,$$

because two local pointed elements u_δ and v_ε on $i\mathcal{O}Gi$ are equivalent if and only if their images $u_{\delta'}$ and $v_{\varepsilon'}$ are equivalent. Indeed, by part (a), $\chi_M(u_{\delta'}) = \chi_M(v_{\varepsilon'})$ for every simple KGb-module M if and only if $\chi_N(u_\delta) = \chi_N(v_\varepsilon)$ for every simple $iKGi$-module N.

To prove that the map $\overline{\phi}$ is also surjective, we first note that, since all maximal local pointed groups on $\mathcal{O}Gb$ are G-conjugate (Theorem 18.3), any local pointed element on $\mathcal{O}Gb$ is conjugate to some $u_{\delta'} \in P_\gamma$ and $u_{\delta'}$ is the image of some $u_\delta \in \mathcal{LPE}(i\mathcal{O}Gi)$. Moreover G-conjugacy clearly implies equivalence (because characters are constant on G-conjugacy classes, see Lemma 43.2). Thus any local pointed element on $\mathcal{O}Gb$ is equivalent to some $u_{\delta'}$ in the image of ϕ, proving the surjectivity of $\overline{\phi}$.

Finally we prove that $\mathcal{LPE}(\mathcal{O}Gb)/{\sim} = \mathcal{LPE}(\mathcal{O}Gb)/G$. We have already observed that G-conjugacy implies equivalence. Conversely, if two local pointed elements on $\mathcal{O}Gb$ are not G-conjugate, then they cannot be equivalent, otherwise two distinct columns of the matrix D' would be equal; this is impossible since D' is a non-singular matrix by Proposition 43.9.

This completes the proof that the map $\phi : u_\delta \mapsto u_{\delta'}$ induces a bijection between $\mathcal{LPE}(i\mathcal{O}Gi)/{\sim}$ and $\mathcal{LPE}(\mathcal{O}Gb)/G$. Now the statement of part (a) asserts exactly that the entries of D and D' are equal. □

Instead of using the above definition of equivalence of local pointed elements, it is possible to replace it by a suitable conjugation relation within the source algebra $(\mathcal{O}Gb)_\gamma$. We shall return to this at the end of Section 47.

(43.11) EXAMPLE. We illustrate the computation of generalized decomposition numbers from a source algebra in the easy case of blocks with a central defect group. Let b be a block of $\mathcal{O}G$ with a central defect group P. Then $\mathcal{O}P$ is a source algebra of b (Theorem 39.4). By Proposition 21.1, the only non-zero idempotent of $\mathcal{O}P$ is $1_{\mathcal{O}P}$. Therefore for every subgroup $Q \leq P$, there is a unique point $\delta = \{1\}$ of $(\mathcal{O}P)^Q$, which is local because the quotient algebra $\overline{\mathcal{O}P}(Q) = kC_P(Q)$ is non-zero, so that it must have at least one point (which is unique).

For every simple module M over $K \otimes_{\mathcal{O}} \mathcal{O}P \cong KP$, let λ_M be the character of M. We have to compute the value of λ_M at a local pointed element u_δ on $\mathcal{O}P$. But $\delta = \{1\}$ by the above observation, and it follows that $\lambda_M(u_\delta) = \lambda_M(u)$. Therefore in this case, the generalized decomposition matrix is just the ordinary character table of KP.

Blocks with a central defect group are examples of nilpotent blocks, to be studied in detail in the next chapter. The computation of this example will be generalized to the case of nilpotent blocks, for which the same result holds except that some crucial signs have to be introduced.

Since the generalized decomposition numbers of a block b can be computed from a source algebra of b, the same result holds for the generalized Cartan integers by Theorem 43.8. However, there is a more direct way of seeing this.

(43.12) PROPOSITION. *Let b be a block of $\mathcal{O}G$ with defect P_γ and let $\mathcal{F}_\gamma : (\mathcal{O}Gb)_\gamma \to \mathrm{Res}^G_P(\mathcal{O}Gb)$ be an associated embedding. Let u_δ and u_ε be two local pointed elements on $(\mathcal{O}Gb)_\gamma$ and denote by $u_{\delta'}$ and $u_{\varepsilon'}$ their images in $\mathcal{O}Gb$ under the embedding $\mathcal{F}_\gamma$. Then the generalized Cartan integer $c(u_{\delta'}, u_{\varepsilon'})$ is equal to the Cartan integer $c_{br_{<u>}(\delta), br_{<u>}(\varepsilon)}$, where $br_{<u>}(\delta)$ and $br_{<u>}(\varepsilon)$ are points of the k-algebra $\overline{(\mathcal{O}Gb)_\gamma}(<u>)$.*

Proof. Let $A = \mathcal{O}Gb$. By Proposition 15.6, the associated embedding $\mathcal{F}_\gamma$ induces an embedding

$$\overline{\mathcal{F}_\gamma}(<u>) : \overline{A_\gamma}(<u>) \longrightarrow \overline{A}(<u>)$$

such that $\overline{\mathcal{F}_\gamma}(<u>)\, br^{A_\gamma}_{<u>} = br^A_{<u>}\, \mathcal{F}^{<u>}_\gamma$, where $\mathcal{F}^{<u>}_\gamma : A^{<u>}_\gamma \to A^{<u>}$ is induced by $\mathcal{F}_\gamma$. By Exercise 8.4, the ordinary Cartan integers are preserved by embeddings, so that one can replace the points $br^{A_\gamma}_{<u>}(\delta)$ and $br^{A_\gamma}_{<u>}(\varepsilon)$ by their images via $\overline{\mathcal{F}_\gamma}(<u>)$. But

$$\overline{\mathcal{F}_\gamma}(<u>)\, br^{A_\gamma}_{<u>}(\delta) = br^A_{<u>}\, \mathcal{F}^{<u>}_\gamma(\delta) = br^A_{<u>}(\delta'),$$

and similarly with ε. It follows that

$$c_{br^{A_\gamma}_{<u>}(\delta), br^{A_\gamma}_{<u>}(\varepsilon)} = c_{br^A_{<u>}(\delta'), br^A_{<u>}(\varepsilon')},$$

and this is the definition of the generalized Cartan integer $c(u_{\delta'}, u_{\varepsilon'})$. □

Let $A = \mathcal{O}Gb$ with defect P_γ and let Q be a subgroup of P. The argument of the proposition shows more generally that if Q_δ and Q_ε are local pointed groups on A_γ, and if $Q_{\delta'}$ and $Q_{\varepsilon'}$ are their images in A, then the Cartan integer $c_{br^A_Q(\delta'), br^A_Q(\varepsilon')}$ of $\overline{A}(Q) = kC_G(Q)br_Q(b)$ can be computed from the source algebra A_γ: it is equal to the Cartan integer $c_{br^{A_\gamma}_Q(\delta), br^{A_\gamma}_Q(\varepsilon)}$ of $\overline{A_\gamma}(Q)$. We warn the reader that, whereas A_γ and A are Morita equivalent, the embedding $\overline{\mathcal{F}_\gamma}(Q) : \overline{A_\gamma}(Q) \to \overline{A}(Q)$ does not induce a Morita equivalence, because there are in general more points in $\overline{A}(Q)$. For example if $Q = P$ is a defect group, then $\overline{A_\gamma}(P)$ has a unique point $br_P(\gamma)$, while $\mathcal{P}(\overline{A}(P))$ consists of all the $N_G(P)$-conjugates of $br_P(\gamma)$ (their number being $|N_G(P) : N_G(P_\gamma)|$, which may be larger than 1). However, the existence of the embedding $\overline{\mathcal{F}_\gamma}(Q)$ suffices for the preservation of Cartan integers, as in the above proof.

Exercises

(43.1) Show that the generalized decomposition matrix of a p-group P is the character table of P.

(43.2) Let χ_M be the character of a projective $\mathcal{O}G$-module M. Prove the first statement of Proposition 42.10, namely that χ_M vanishes outside G_{reg}. [Hint: Prove that if u_δ is a local pointed element on $\mathcal{O}G$ with $u \neq 1$ and if $j \in \delta$, then $\chi_M(u_\delta) = \chi_{jM}(u)$ is zero, by showing that $\text{Res}_{<u>}(M)$ and its direct summand jM are projective, hence free.]

(43.3) This exercise generalizes the previous one. Let χ_M be the character of an $\mathcal{O}G$-lattice M which is projective relative to some subgroup H. Let $g \in G$ and let u be the p-part of g (so that $g = us$ with s p-regular in $C_G(u)$). Prove that if no conjugate of u lies in H, then $\chi_M(g) = 0$. [Hint: Let $A = \text{End}_{\mathcal{O}}(M)$ and let $U = <u>$. Use the Mackey decomposition formula 11.3 to show that $A^G = A^G_H \subseteq \sum_{V<U} A^U_V$. If u_δ is a local pointed element on $\mathcal{O}G$ and if $j \in \delta$, then $j{\cdot}id_M \in \sum_{V<U} A^U_V$. Then proceed as in Proposition 43.3, by applying Theorem 23.1 to each primitive idempotent appearing in a decomposition of $j{\cdot}id_M$.]

(43.4) Prove Theorem 43.8. [Hint: Read Feit's book.]

Notes on Section 43

The generalized decomposition numbers were introduced by Brauer and the second main theorem is of course also due to Brauer [1959]. The definition given here and the proof of the second main theorem are due to Puig [1981]. In fact Puig replaces $\mathcal{O}G$ by an arbitrary interior G-algebra A such that A is free as an $\mathcal{O}$-module and proves a more general theorem about the decomposition of the character of an A-module. Instead of characters, it is also possible to decompose modules, viewed as elements of the Green ring of all $\mathcal{O}G$-modules; this far-reaching generalization of Brauer's second main theorem appears in Puig [1988a]. Finally Exercise 43.3 is due to Green [1962].

§ 44 THE MODULE STRUCTURE OF SOURCE ALGEBRAS

In this section we analyse in more detail the $\mathcal{O}(P\times P)$-module structure of a source algebra of a block (where P is a defect group). This will be used in the next section to compute a source algebra of a block with a normal defect group.

Let P_γ be a defect of a block b of $\mathcal{O}G$ and let the interior P-algebra $(\mathcal{O}Gb)_\gamma$ be a source algebra of b. Recall that $P\times P$ acts on $(\mathcal{O}Gb)_\gamma$ via $(u,v)\cdot a = u\cdot a\cdot v^{-1}$ (where $u,v\in P$ and $a\in(\mathcal{O}Gb)_\gamma$). We have proved in Proposition 38.7 that $(\mathcal{O}Gb)_\gamma$ has a $(P\times P)$-invariant basis (containing $1_{(\mathcal{O}Gb)_\gamma}$). We first make this observation more precise.

(44.1) LEMMA. *Let P_γ be a defect of a block b of $\mathcal{O}G$, let the interior P-algebra $(\mathcal{O}Gb)_\gamma$ be a source algebra of b, and let X be a $(P\times P)$-invariant basis of $(\mathcal{O}Gb)_\gamma$.*

(a) For every $x\in X$, the $\mathcal{O}(P\times P)$-submodule $\mathcal{O}P\cdot x\cdot P$ generated by the orbit of x is an indecomposable direct summand of $(\mathcal{O}Gb)_\gamma$.

(b) For every $x\in X$, the direct summand $\mathcal{O}P\cdot x\cdot P$ is isomorphic (as an $\mathcal{O}(P\times P)$-module) to a summand $\mathcal{O}PgP$ of $\mathcal{O}G$, for some $g\in G$.

(c) There is an isomorphism $\mathcal{O}PgP\cong \mathrm{Ind}_{Q_g}^{P\times P}(\mathcal{O})$, where Q_g denotes the subgroup $Q_g=\{\,(u,{}^{g^{-1}}u)\in P\times P \mid u\in P\cap {}^gP\,\}$.

(d) If $g\in N_G(P)$, the dimension of $\mathcal{O}PgP=\mathcal{O}Pg$ is equal to $|P|$. If $g\notin N_G(P)$, the dimension of $\mathcal{O}PgP$ is a power of p strictly larger than $|P|$.

(e) If $g,h\in N_G(P)$, then $\mathcal{O}Pg\cong\mathcal{O}Ph$ if and only if $g^{-1}h\in PC_G(P)$.

Proof. (a) For a p-group, any permutation module on a single orbit is indecomposable (Lemma 27.1).

(b) We know that $(\mathcal{O}Gb)_\gamma$ is isomorphic as an $\mathcal{O}(P\times P)$-module to a direct summand of $\mathcal{O}G$ (see the proof of Proposition 38.7). Thus any direct summand of $(\mathcal{O}Gb)_\gamma$ is isomorphic to a direct summand of $\mathcal{O}G$. But G is a $(P\times P)$-invariant basis of $\mathcal{O}G$, so that every orbit PgP generates an indecomposable direct summand of $\mathcal{O}G$. By the Krull–Schmidt theorem, every indecomposable direct summand of $\mathcal{O}G$ is isomorphic to some summand of the form $\mathcal{O}PgP$.

(c) Since $\mathcal{O}PgP$ is a permutation module on the $(P\times P)$-set PgP, which is transitive, there is an isomorphism $\mathcal{O}PgP\cong\mathrm{Ind}_Q^{P\times P}(\mathcal{O})$ where Q is the stabilizer of an element. Choosing this element to be g, and considering the action of $(u,v)\in P\times P$, we have $(u,v)\in Q$ if and only if $ugv^{-1}=g$, that is, $v=g^{-1}ug$. Thus $Q=Q_g$.

(d) The dimension of $\mathcal{O}PgP$ is the index of Q_g in $P\times P$. Moreover projection onto the first component induces an isomorphism between Q_g and $P\cap {}^gP$, so that $|(P\times P):Q_g|=|P|\cdot|P:P\cap {}^gP|$, which is a power of p. If $g \in N_G(P)$, then Q_g is isomorphic to P and has index $|P|$. If $g \notin N_G(P)$, then $|P : P \cap {}^gP| > 1$ and Q_g has index strictly larger than $|P|$.

(e) If $g^{-1}h \in PC_G(P)$, then we can write $h = gvc$ with $v \in P$ and $c \in C_G(P)$. It follows that $Q_h = (1, v^{-1})Q_g(1, v)$, because for $u \in P$ we have ${}^{h^{-1}}u = {}^{c^{-1}v^{-1}g^{-1}}u = v^{-1}\,{}^{g^{-1}}uv$. Therefore there is an isomorphism $\mathrm{Ind}_{Q_h}^{P\times P}(\mathcal{O}) \cong \mathrm{Ind}_{Q_g}^{P\times P}(\mathcal{O})$. Alternatively, right multiplication by the element $c = v^{-1}g^{-1}h$ yields an explicit isomorphism $\mathcal{O}Pg \to \mathcal{O}Ph$ (as $\mathcal{O}(P \times P)$-modules).

Conversely if $\mathrm{Ind}_{Q_h}^{P\times P}(\mathcal{O}) \cong \mathrm{Ind}_{Q_g}^{P\times P}(\mathcal{O})$, then Q_h is conjugate to Q_g. Indeed Q_h is a vertex of $\mathrm{Ind}_{Q_h}^{P\times P}(\mathcal{O})$ (Lemma 27.1) and the vertices of an indecomposable module are conjugate (Theorem 18.3). Let $(v, w) \in P \times P$ be such that ${}^{(v,w)}Q_h = Q_g$. Then ${}^{(v,w)}(u, {}^{h^{-1}}u) = ({}^vu, {}^{wh^{-1}}u) \in Q_g$ for all $u \in P$, and so ${}^{g^{-1}v}u = {}^{wh^{-1}}u$. Therefore $c = v^{-1}gwh^{-1}$ centralizes P and it follows that $gh^{-1} = {}^gw^{-1}vc \in PC_G(P)$. □

Our aim is to determine the summands of the source algebra $(\mathcal{O}Gb)_\gamma$ which are isomorphic to $\mathcal{O}Pg$ for some $g \in N_G(P)$ and to determine their multiplicity. A complete answer to this question will be given, and this will allow us in the next section to describe the source algebra when P is normal. In contrast, the summands of $(\mathcal{O}Gb)_\gamma$ isomorphic to $\mathcal{O}PgP$ for some $g \notin N_G(P)$ seem much more difficult to handle.

We start with a crucial general result, which will be improved later in Section 47.

(44.2) PROPOSITION. *Let A be an interior G-algebra, let P_γ be a pointed group on A, and let $g \in N_G(P)$.*

(a) *We have $g \in N_G(P_\gamma)$ if and only if there exists $a \in A_\gamma^*$ such that $a{\cdot}u{\cdot}a^{-1} = {}^gu{\cdot}1_{A_\gamma}$ for every $u \in P$.*

(b) *If $g \in N_G(P_\gamma)$, then the element $a \in A_\gamma^*$ in part (a) is unique up to right multiplication by an element of $(A_\gamma^P)^*$.*

Proof. (a) Let $i \in \gamma$ and choose $A_\gamma = iAi$. If $g \in N_G(P_\gamma)$, then ${}^gi \in \gamma$ so that there exists $c \in (A^P)^*$ such that ${}^gi = cic^{-1}$. Then $a = ic^{-1}{\cdot}g = c^{-1}{\cdot}g{\cdot}i$ belongs to iAi and its inverse in iAi is equal to $a^{-1} = g^{-1}{\cdot}ci = i{\cdot}g^{-1}{\cdot}c$. For all $u \in P$, we have

$$a{\cdot}u{\cdot}a^{-1} = ic^{-1}{\cdot}gug^{-1}{\cdot}ci = ic^{-1}c{\cdot}\,{}^gu{\cdot}i = {}^gu{\cdot}i\,,$$

as required.

The proof of the converse follows from some general results proved earlier (see Exercise 44.1), but we give here a direct argument. If $a \in (iAi)^*$

satisfies $a{\cdot}u{\cdot}a^{-1} = {}^g u{\cdot}i$ for all $u \in P$, then we define $d = g^{-1}{\cdot}a$ and $d' = a^{-1}{\cdot}g$. Note that a^{-1} is not the inverse of a in A, so that d' is not the inverse of d (unless $i = 1_A$). Let $j = {}^{g^{-1}}i$. Since P centralizes i and $a = iai$, we have for all $u \in P$

$$d{\cdot}u{\cdot}i = g^{-1}{\cdot}a{\cdot}u{\cdot}a^{-1}a = g^{-1}{\cdot}\,{}^g u{\cdot}ia = u{\cdot}j{\cdot}g^{-1}{\cdot}a = u{\cdot}jd\,,$$

and similarly $u{\cdot}id' = d'{\cdot}u{\cdot}j$. In particular $di = jd$ and $id' = d'j$. Note that $di, id' \in A^P$, because for all $u \in P$ we have

$$di{\cdot}u = d{\cdot}u{\cdot}i = u{\cdot}jd = u{\cdot}di \quad \text{and} \quad u{\cdot}id' = d'{\cdot}u{\cdot}j = d'j{\cdot}u = id'{\cdot}u\,.$$

Now we compute the product of di and id' in both orders:

$$\begin{aligned} diid' &= g^{-1}{\cdot}aia^{-1}{\cdot}g = g^{-1}{\cdot}i{\cdot}g = j\,,\\ id'di &= ia^{-1}{\cdot}gg^{-1}{\cdot}ai = ia^{-1}ai = i\,. \end{aligned}$$

By Exercise 3.2, it follows that i and j are conjugate in A^P. Therefore ${}^{g^{-1}}i = j \in \gamma$ and so $g^{-1} \in N_G(P_\gamma)$. Thus $g \in N_G(P_\gamma)$, as was to be shown.

(b) If $a' \in A_\gamma^*$ also satisfies $a'{\cdot}u{\cdot}(a')^{-1} = {}^g u{\cdot}1_{A_\gamma}$ for all $u \in P$, then $a'{\cdot}u{\cdot}(a')^{-1} = a{\cdot}u{\cdot}a^{-1}$ and therefore $c = a^{-1}a'$ commutes with P. Thus $c \in (A_\gamma^P)^*$ and $a' = ac$. □

In the special case of the source algebra of a block, we shall soon improve Proposition 44.2 by dropping the assumption that the element $a \in A_\gamma$ be invertible and assuming merely that $a{\cdot}u = {}^g u{\cdot}a$ for all $u \in P$.

Proposition 44.2 gives a characterization of $N_G(P_\gamma)$ in terms of the localization A_γ and in terms of the group $N_G(P)$ (which depends on G). Indeed $N_G(P)$ acts by conjugation on P, and $N_G(P_\gamma)$ is the inverse image via $N_G(P) \to \mathrm{Aut}(P)$ of the subgroup of all automorphisms ψ of P satisfying $\psi(u){\cdot}1_{A_\gamma} = a{\cdot}u{\cdot}a^{-1}$ for some $a \in A_\gamma^*$. When P_γ is a local pointed group on a block algebra $\mathcal{O}Gb$, we shall see in Section 47 that the group $N_G(P_\gamma)/C_G(P)$ can even be determined from a source algebra of b without reference to $N_G(P)$, hence completely independently of G.

We can now state the result on the direct summands of a source algebra. If $g \in N_G(P_\gamma)$, we denote by $a_g \in (\mathcal{O}Gb)_\gamma^*$ an element satisfying $a_g{\cdot}u{\cdot}a_g^{-1} = {}^g u{\cdot}1_{(\mathcal{O}Gb)_\gamma}$ for all $u \in P$. The existence of a_g follows from Proposition 44.2, but a_g is far from being unique since it can be multiplied by any element of $((\mathcal{O}Gb)_\gamma^P)^*$.

(44.3) THEOREM. *Let P_γ be a defect of a block b of $\mathcal{O}G$ and let the interior P-algebra $(\mathcal{O}Gb)_\gamma$ be a source algebra of b. For every g in a system of coset representatives $[N_G(P_\gamma)/PC_G(P)]$, choose an element $a_g \in (\mathcal{O}Gb)_\gamma^*$ such that $a_g{\cdot}u{\cdot}a_g^{-1} = {}^g u{\cdot}1_{(\mathcal{O}Gb)_\gamma}$ for all $u \in P$.*

(a) *There is a decomposition of $(\mathcal{O}Gb)_\gamma$ as an $\mathcal{O}(P \times P)$-module*

$$(\mathcal{O}Gb)_\gamma = \Big(\bigoplus_{g\in[N_G(P_\gamma)/PC_G(P)]} \mathcal{O}P{\cdot}a_g \Big) \bigoplus N \,,$$

where N is isomorphic to a direct sum of modules of the form $\mathcal{O}PhP$ for some $h \in G - N_G(P)$.

(b) *$\mathcal{O}P{\cdot}a_g \cong \mathcal{O}Pg$ for $g \in [N_G(P_\gamma)/PC_G(P)]$, and these modules are pairwise non-isomorphic indecomposable $\mathcal{O}(P \times P)$-modules.*

Before embarking on the proof, we need some lemmas. First we improve Proposition 44.2.

(44.4) LEMMA. *Let P_γ be a defect of a block b of $\mathcal{O}G$ and let $g \in N_G(P)$. Assume that there exists $a \in (\mathcal{O}Gb)_\gamma$ such that a belongs to a $(P \times P)$-invariant basis of $(\mathcal{O}Gb)_\gamma$ and such that $a{\cdot}u = {}^g u{\cdot}a$ for all $u \in P$. Then $g \in N_G(P_\gamma)$.*

Proof. Let $i \in \gamma$ and choose $(\mathcal{O}Gb)_\gamma = i\mathcal{O}Gi$. As in the proof of Proposition 44.2, we let $d = g^{-1}{\cdot}a$ and $j = {}^{g^{-1}}i$. We have again $d{\cdot}u{\cdot}i = u{\cdot}jd$ for all $u \in P$. Indeed $g^{-1}{\cdot}a{\cdot}u = ug^{-1}{\cdot}a$ by assumption and since i commutes with u, we have

$$d{\cdot}u{\cdot}i = g^{-1}{\cdot}a{\cdot}u = ug^{-1}{\cdot}a = ug^{-1}{\cdot}ia = u{\cdot}\,{}^{g^{-1}}i{\cdot}g^{-1}{\cdot}a = u{\cdot}jd \,.$$

In particular $di = jd$. Moreover P centralizes $d = di$, by the argument used in the proof of Proposition 44.2.

Since $i\mathcal{O}Gi$ is a direct summand of $\mathcal{O}G$ as an $\mathcal{O}(P \times P)$-module, the given $(P \times P)$-invariant basis of $i\mathcal{O}Gi$ containing a is contained in a $(P\times P)$-invariant basis X of $\mathcal{O}G$. Thus $d = g^{-1}{\cdot}a \in g^{-1}{\cdot}X$. But $g^{-1}{\cdot}X$ is still a $(P \times P)$-invariant basis of $\mathcal{O}G$, because $g \in N_G(P)$. Since d is fixed under P and since $br_P((g^{-1}X)^P)$ is a basis of $br_P((\mathcal{O}G)^P)$ (Proposition 27.6), we have $br_P(d) \neq 0$.

Now $br_P(i)$ is a primitive idempotent of $br_P((\mathcal{O}G)^P) = kC_G(P)$, because γ is a local point. Let e be the block of $kC_G(P)$ associated with $br_P(i)$. Then e is also associated with $br_P(j)$ because

$$\begin{aligned} e{\cdot}br_P(jd) &= e{\cdot}br_P(di) = br_P(d)br_P(i)e = br_P(d)br_P(i) \\ &= br_P(di) = br_P(d) \neq 0 \,, \end{aligned}$$

and therefore $e{\cdot}br_P(j) \neq 0$. On restriction to $(PC_G(P))$-fixed elements, the Brauer homomorphism is a surjection

$$br_P : (\mathcal{O}G)^{PC_G(P)} \longrightarrow (kC_G(P))^{PC_G(P)} = ZkC_G(P)\,.$$

We let $f \in (\mathcal{O}G)^{PC_G(P)}$ be a primitive idempotent such that $br_P(f) = e$ (which exists by Theorem 3.2).

The canonical surjection $\pi_\gamma : (\mathcal{O}G)^P \to S(\gamma)$ factorizes as

$$(\mathcal{O}G)^P \xrightarrow{br_P} kC_G(P) \xrightarrow{\overline{\pi}_\gamma} S(\gamma)$$

because γ is local. Since $\overline{\pi}_\gamma(br_P(i)e) = \overline{\pi}_\gamma(br_P(i)) = \pi_\gamma(i)$ is a primitive idempotent of $S(\gamma)$, we have $\overline{\pi}_\gamma(e) \neq 0$ and therefore $\pi_\gamma(f) \neq 0$. This means that $P_\gamma \leq (PC_G(P))_\beta$, where β is the point containing f. Since we also have $br_P(j)e = br_P(j)$ and $j \in {}^{g^{-1}}\gamma$, the same argument shows that $P_{{}^{g^{-1}}\gamma} \leq (PC_G(P))_\beta$.

Since P_γ is maximal local, so is $P_{{}^{g^{-1}}\gamma} = {}^{g^{-1}}(P_\gamma)$, and therefore both pointed groups are defects of $(PC_G(P))_\beta$ (by Theorem 18.3). Consequently P_γ and $P_{{}^{g^{-1}}\gamma}$ are conjugate by some element of $PC_G(P)$. But $PC_G(P)$ acts trivially on the points of $(\mathcal{O}G)^P$ (because P acts trivially and $C_G(P) \subseteq (\mathcal{O}G)^P$ acts by inner automorphisms). Therefore $\gamma = {}^{g^{-1}}\gamma$, so that $g^{-1} \in N_G(P_\gamma)$. Thus $g \in N_G(P_\gamma)$, as required. □

Now we can start analysing the summands of $(\mathcal{O}Gb)_\gamma$.

(44.5) LEMMA. *Let P_γ be a defect of a block b of $\mathcal{O}G$.*

(a) If $g \in N_G(P_\gamma)$ and $a \in (\mathcal{O}Gb)_\gamma^*$ satisfy $a{\cdot}u{\cdot}a^{-1} = {}^gu{\cdot}1_{(\mathcal{O}Gb)_\gamma}$ for all $u \in P$, then $\mathcal{O}P{\cdot}a$ is a direct summand of $(\mathcal{O}Gb)_\gamma$ isomorphic to $\mathcal{O}Pg$ as an $\mathcal{O}(P \times P)$-module.

(b) If a summand of $(\mathcal{O}Gb)_\gamma$ is isomorphic to $\mathcal{O}Pg$ for some $g \in N_G(P)$, then $g \in N_G(P_\gamma)$.

Proof. (a) By Proposition 38.7, there exists a $(P \times P)$-invariant basis of $(\mathcal{O}Gb)_\gamma$ containing $1_{(\mathcal{O}Gb)_\gamma}$. The $\mathcal{O}(P \times P)$-submodule generated by $1_{(\mathcal{O}Gb)_\gamma}$ is equal to $\mathcal{O}P{\cdot}1_{(\mathcal{O}Gb)_\gamma}$ and is a direct summand of $(\mathcal{O}Gb)_\gamma$ isomorphic to $\mathcal{O}P$. In fact this argument proves the result for $g = 1$ and $a = 1_{(\mathcal{O}Gb)_\gamma}$.

Right multiplication by a maps any direct summand M of $(\mathcal{O}Gb)_\gamma$ to a submodule of $(\mathcal{O}Gb)_\gamma$. Indeed the action of $(u,v) \in P \times P$ on $ma \in Ma$ is equal to

$$(u,v)ma = u{\cdot}ma{\cdot}v^{-1} = u{\cdot}ma{\cdot}v^{-1}{\cdot}a^{-1}a = u{\cdot}m{\cdot}{}^g(v^{-1}){\cdot}a \in Ma\,.$$

In fact $Ma \cong {}^{(1,g^{-1})}M$ (the conjugate module), but we do not need this explicit description. It follows that any direct sum decomposition of $(\mathcal{O}Gb)_\gamma$ is mapped by right multiplication by a to another direct sum decomposition. Thus the image $\mathcal{O}P{\cdot}a$ of the summand $\mathcal{O}P{\cdot}1_{(\mathcal{O}Gb)_\gamma}$ is again a direct summand. Finally it is elementary to check that there is an isomorphism of $\mathcal{O}(P \times P)$-modules

$$\mathcal{O}P{\cdot}a \cong \mathcal{O}Pg\,, \qquad u{\cdot}a \mapsto ug\,.$$

This completes the proof of (a).

(b) Let M be a direct summand of $(\mathcal{O}Gb)_\gamma$ isomorphic to $\mathcal{O}Pg$, let $\phi : \mathcal{O}Pg \to M$ be an isomorphism and let $a = \phi(g)$. We prove that a satisfies the assumptions of Lemma 44.4. Firstly, since g is part of a $(P \times P)$-invariant basis of $\mathcal{O}Pg$ (namely Pg), its image a belongs to a $(P \times P)$-invariant basis of M. It follows that a belongs to a $(P \times P)$-invariant basis of $(\mathcal{O}Gb)_\gamma$, because any complementary summand must also have an invariant basis (Corollary 27.2). This proves the first assumption of Lemma 44.4. On the other hand, for all $u \in P$, we have

$$a{\cdot}u = \phi(g){\cdot}u = \phi(g{\cdot}u) = \phi({}^{g}u{\cdot}g) = {}^{g}u{\cdot}\phi(g) = {}^{g}u{\cdot}a\,.$$

By Lemma 44.4, it follows that $g \in N_G(P_\gamma)$. □

(44.6) LEMMA. *Let P_γ be a defect of a block b of $\mathcal{O}G$. In any decomposition of $(\mathcal{O}Gb)_\gamma$ as a direct sum of indecomposable $\mathcal{O}(P\times P)$-modules, there is a unique summand isomorphic to $\mathcal{O}P$.*

Proof. We know that $\mathcal{O}P{\cdot}1_{(\mathcal{O}Gb)_\gamma}$ is a summand isomorphic to $\mathcal{O}P$, by part (a) of Lemma 44.5 applied with $g = 1$ and $a = 1_{(\mathcal{O}Gb)_\gamma}$. We have to prove that its multiplicity is one. Recall that by the Krull–Schmidt theorem, this does not depend on the choice of the decomposition.

Let Δ be the diagonal subgroup of $P \times P$. Then $\Delta \cong P$ and the action of $(u,u) \in \Delta$ coincides with the conjugation action of $u \in P$. The image under br_Δ of any summand isomorphic to $\mathcal{O}P$ is

$$\overline{\mathcal{O}P}(\Delta) \cong kZ(P)\,,$$

because $Z(P)$ is the set of Δ-fixed elements in the basis P of $\mathcal{O}P$. Thus if two summands in a decomposition of $(\mathcal{O}Gb)_\gamma$ were isomorphic to $\mathcal{O}P$, then $\overline{(\mathcal{O}Gb)_\gamma}(\Delta)$ would have at least two summands isomorphic to $kZ(P)$. But the Brauer homomorphism br_Δ coming from the $\mathcal{O}(P\times P)$-module structure coincides with the Brauer homomorphism br_P coming from the P-algebra structure. Therefore by Proposition 38.10, the image of $br_\Delta = br_P$ is equal to

$$\overline{(\mathcal{O}Gb)_\gamma}(\Delta) = \overline{(\mathcal{O}Gb)_\gamma}(P) \cong kZ(P)\,.$$

Thus there is no room for two summands isomorphic to $kZ(P)$, proving the lemma. □

Our final tool for the proof of the main theorem is the following lemma, which allows us to replace some indecomposable direct summands by arbitrary isomorphic ones.

(44.7) LEMMA. *Let B be an $\mathcal{O}$-algebra, let M be a B-module, and let $M = \bigoplus_{i\in I} N_i$ be a direct sum decomposition of M into indecomposable submodules. Let $i_0 \in I$ be such that N_{i_0} appears with multiplicity one (that is, $N_{i_0} \not\cong N_i$ for $i \neq i_0$). Then for any indecomposable direct summand L of M such that $L \cong N_{i_0}$,*

$$M = L \bigoplus \big(\bigoplus_{i\in I-\{i_0\}} N_i \big)$$

is a direct sum decomposition of M (into indecomposable summands).

Proof. Let $\pi_i : M \to N_i$ be the projection map defined by the given decomposition of M and let $\pi_L : M \to L$ be the projection map defined by some decomposition $M = L \oplus L'$, which exists by assumption. Since $\sum_i \pi_i = id_M$, we have $\sum_i \pi_L\pi_i = \pi_L$ and so $\sum_i (\pi_L\pi_i)_{|L} = id_L$ where $(\pi_L\pi_i)_{|L}$ denotes the restriction of $\pi_L\pi_i$ to L. But as L is indecomposable, $\mathrm{End}_B(L)$ has no non-trivial idempotent and so $\mathrm{End}_B(L)$ is a local ring (Corollary 4.6). Therefore there exists $j \in I$ such that $(\pi_L\pi_j)_{|L} \notin J(\mathrm{End}_B(L))$ and so $(\pi_L\pi_j)_{|L}$ is invertible. If ϕ denotes its inverse, then $(\pi_j)_{|L} : L \to N_j$ is injective and has a retraction $\phi\,(\pi_L)_{|N_j}$. This shows that L is isomorphic to a direct summand of N_j. But as N_j is indecomposable, $(\pi_j)_{|L}$ must be an isomorphism. Since $L \cong N_{i_0}$, it follows from our multiplicity assumption that $j = i_0$. Since we have $\bigoplus_{i\in I-\{i_0\}} N_i = \mathrm{Ker}(\pi_{i_0})$, it remains to show that there is a direct sum decomposition $M = L \oplus \mathrm{Ker}(\pi_{i_0})$. Firstly $L \cap \mathrm{Ker}(\pi_{i_0}) = \mathrm{Ker}((\pi_{i_0})_{|L}) = 0$. On the other hand if $x \in M$, then $\pi_{i_0}(x) \in N_{i_0}$ and there exists $y \in L$ such that $\pi_{i_0}(y) = \pi_{i_0}(x)$. Then $x = y + (x - y)$ and $x - y \in \mathrm{Ker}(\pi_{i_0})$, showing that $M = L + \mathrm{Ker}(\pi_{i_0})$. □

We have now paved the way for the proof of Theorem 44.3.

Proof of Theorem 44.3. By Lemma 44.5, $\mathcal{O}P{\cdot}a_g$ is a direct summand isomorphic to $\mathcal{O}Pg$ for every $g \in N_G(P_\gamma)$. Starting now from an arbitrary decomposition of $(\mathcal{O}Gb)_\gamma$ into indecomposable summands, there is at least one summand isomorphic to $\mathcal{O}Pg$, by the Krull–Schmidt theorem. It is easy to check (see Exercise 44.2) that, if two summands in the decomposition were isomorphic to $\mathcal{O}Pg$, then after applying right multiplication by a_g^{-1}, we would obtain two summands isomorphic to $\mathcal{O}P$. This is impossible by Lemma 44.6. Thus each summand isomorphic to $\mathcal{O}Pg$ appears with multiplicity one.

Let $g, g' \in N_G(P_\gamma)$. By Lemma 44.1, $\mathcal{O}Pg \cong \mathcal{O}Pg'$ if and only if $g' = gc$ for some $c \in PC_G(P)$. Thus the direct sum of the summands isomorphic to $\mathcal{O}Pg$ for some $g \in N_G(P_\gamma)$ actually runs over $[N_G(P_\gamma)/PC_G(P)]$.

If a summand is isomorphic to $\mathcal{O}Pg$ for some $g \in N_G(P)$, then $g \in N_G(P_\gamma)$ by Lemma 44.5. Thus all the remaining summands must be isomorphic to $\mathcal{O}PhP$ for some $h \notin N_G(P)$ (using Lemma 44.1).

We have shown that there exists a direct sum decomposition

$$(\mathcal{O}Gb)_\gamma = \Big(\bigoplus_{g\in[N_G(P_\gamma)/PC_G(P)]} M_g\Big) \oplus N$$

where $M_g \cong \mathcal{O}Pg$ and N is isomorphic to a direct sum of modules of the form $\mathcal{O}PhP$ for some $h \in G - N_G(P)$. Since M_g has multiplicity one, we can apply Lemma 44.7 and replace M_g by the summand $\mathcal{O}P{\cdot}a_g$. We obtain in this way the required decomposition of the statement. Statement (b) has already been proved. □

(44.8) COROLLARY. *Let P_γ be a defect of a block b of $\mathcal{O}G$, let $(\mathcal{O}Gb)_\gamma$ be a source algebra of b, and let $E_G(P_\gamma) = N_G(P_\gamma)/PC_G(P)$. Then $|P|$ divides $\dim_\mathcal{O}((\mathcal{O}Gb)_\gamma)$ and*

$$\frac{\dim_\mathcal{O}((\mathcal{O}Gb)_\gamma)}{|P|} \equiv |E_G(P_\gamma)| \pmod{p}.$$

In particular $|P|$ is the exact power of p dividing $\dim_\mathcal{O}((\mathcal{O}Gb)_\gamma)$.

Proof. We use the notation of Theorem 44.3. When $g \in N_G(P_\gamma)$, every summand $\mathcal{O}Pa_g$ has dimension $|P|$, while if $h \notin N_G(P)$ every summand isomorphic to $\mathcal{O}PhP$ has dimension a multiple of $|P|$ by some power of p greater than 1 (see Lemma 44.1). The congruence modulo p follows. The additional statement is a consequence of the fact that $|E_G(P_\gamma)|$ is prime to p, by Theorem 37.9. □

As an application, we prove the following result.

(44.9) PROPOSITION. *Let P_γ be a defect of a block b of $\mathcal{O}G$ and let the interior P-algebra $(\mathcal{O}Gb)_\gamma$ be a source algebra of b. Then there exists a simple $(\mathcal{O}Gb)_\gamma$-module of dimension prime to p.*

Proof. Let $A = (\mathcal{O}Gb)_\gamma$. By Corollary 5.3, we have

$$\dim_{\mathcal{O}}(A) = \sum_{\alpha \in \mathcal{P}(A)} \dim_{\mathcal{O}}(P(\alpha)) \dim_k(V(\alpha)),$$

where $V(\alpha)$ is the simple A-module corresponding to α and $P(\alpha)$ is the indecomposable projective A-module corresponding to α (that is, the projective cover of $V(\alpha)$). By Corollary 38.4, $\mathrm{Res}_P(P(\alpha))$ is a projective $\mathcal{O}P$-module, hence free (Proposition 21.1). Therefore $\dim_{\mathcal{O}}(P(\alpha))$ is a multiple of $|P|$ and we can write

$$\frac{\dim_{\mathcal{O}}(A)}{|P|} = \sum_{\alpha \in \mathcal{P}(A)} \frac{\dim_{\mathcal{O}}(P(\alpha))}{|P|} \dim_k(V(\alpha)).$$

Since the left hand side is prime to p by Corollary 44.8 above, there exists at least one α such that p does not divide $\dim_k(V(\alpha))$. □

Another proof of this proposition will be given in Section 46.

Exercises

(44.1) The purpose of this exercise is to give another proof of Proposition 44.2. Let A be an interior G-algebra, let P_γ be a pointed group on A, let $g \in N_G(P)$, and suppose that there exists $a \in A_\gamma^*$ such that $a{\cdot}u{\cdot}a^{-1} = {}^g u{\cdot}1_{A_\gamma}$ for all $u \in P$. We can choose $A_\gamma = iAi$ where $i \in \gamma$.

(a) Prove that $\mathrm{Conj}(g{\cdot}a^{-1}) : iAi \to {}^g iA\,{}^g i$ is an isomorphism of interior P-algebras.

(b) Let $\mathcal{F}_\gamma : iAi \to \mathrm{Res}^G_P(A)$ and $\mathcal{F}_{{}^g\gamma} : {}^g iA\,{}^g i \to \mathrm{Res}^G_P(A)$ be the embeddings containing the inclusions, and let $\mathcal{C}$ be the exomorphism containing $\mathrm{Conj}(g{\cdot}a^{-1})$. Show that $\mathrm{Res}^P_1(\mathcal{F}_\gamma) = \mathrm{Res}^P_1(\mathcal{F}_{{}^g\gamma})\,\mathrm{Res}^P_1(\mathcal{C})$. [Hint: Show that $b = a + (1_A - i)$ is invertible in A and that $\mathrm{Conj}(g{\cdot}a^{-1})$ extends to $\mathrm{Inn}(g{\cdot}b^{-1})$.]

(c) Show that $\mathcal{F}_\gamma = \mathcal{F}_{{}^g\gamma}\mathcal{C}$ and deduce the existence of $c \in A^P$ such that $\mathrm{Conj}(g{\cdot}a^{-1})$ extends to $\mathrm{Inn}(c)$. [Hint: Remember Proposition 12.1.]

(d) Prove that $g \in N_G(P_\gamma)$. [Hint: $\mathrm{Inn}(c)(i) = {}^g i$.]

(44.2) Let P_γ be a defect of a block b of $\mathcal{O}G$, let M be a direct summand of $(\mathcal{O}Gb)_\gamma$ isomorphic to $\mathcal{O}Pg$ (as $\mathcal{O}(P \times P)$-modules) for some $g \in N_G(P_\gamma)$, and let $a \in (\mathcal{O}Gb)_\gamma^*$ be such that $a{\cdot}u{\cdot}a^{-1} = {}^g u{\cdot}1$ for all $u \in P$. Show that Ma^{-1} is a direct summand of $(\mathcal{O}Gb)_\gamma$ isomorphic to $\mathcal{O}P$.

(44.3) Let P_γ be a defect of a block b of $\mathcal{O}G$ and assume that P is cyclic. Prove that we have $\frac{1}{|P|}\dim_{\mathcal{O}}((\mathcal{O}Gb)_\gamma) \equiv e \pmod p$ for some divisor e of $p-1$.

Notes on Section 44

All the results of this section are due to Puig [1988a].

§ 45 BLOCKS WITH A NORMAL DEFECT GROUP

The purpose of this section is to describe a source algebra of a block with a normal defect group. We use the main result of the previous section to show that a source algebra of any block contains a subalgebra isomorphic to a twisted group algebra $\mathcal{O}_\sharp(P\rtimes\widehat{E}_G(P_\gamma))$. Then we show that this subalgebra is the whole source algebra when P is normal.

Let b be a block of $\mathcal{O}G$ and let P_γ be a defect of b. As usual we let $E_G(P_\gamma) = N_G(P_\gamma)/PC_G(P)$. With the notation of the previous section, our aim is to organize the summands $\mathcal{O}P\cdot a_g$ for $g \in E_G(P_\gamma)$ into a subalgebra of $(\mathcal{O}Gb)_\gamma$. We know that $\mathcal{O}P\cdot 1_{(\mathcal{O}Gb)_\gamma}$ is a subalgebra isomorphic to $\mathcal{O}P$ (Exercise 38.2), so we are left with the proof that the elements a_g for $g \in E_G(P_\gamma)$ can be chosen in a consistent fashion, in order to generate a twisted group algebra. We work more generally with an interior G-algebra A, an arbitrary pointed group P_γ on A such that P is a p-group, and a subgroup E of $N_G(P_\gamma)/PC_G(P)$ of order prime to p. We shall need the following special case of the Schur–Zassenhaus theorem.

(45.1) LEMMA. *Let P be a normal p-subgroup of a finite group X and suppose that the order of the quotient group $E = X/P$ is prime to p. Then the short exact sequence $1 \to P \to X \to E \to 1$ splits and the splitting is unique up to conjugation by an element of P.*

Proof. We proceed by induction on $|P|$, the case $|P| = 1$ being trivial. If $|P| > 1$, then the centre $Z(P)$ is non-trivial (because P is a p-group) and is a characteristic subgroup of P. Thus $Z(P)$ is normal in X and we can consider the group $X/Z(P)$, which has a normal subgroup $P/Z(P)$ with quotient isomorphic to E. By induction, there exists a splitting $s : E \to X/Z(P)$ and we let $F = s(E)$. Then there is a short exact sequence

$$1 \longrightarrow Z(P) \longrightarrow Y \longrightarrow F \longrightarrow 1,$$

where Y is the inverse image of F in X. Since $Z(P)$ is abelian, it is endowed with an F-module structure (coming from the conjugation action of Y), and the above extension corresponds to an element of the cohomology group $H^2(F, Z(P))$ (Proposition 1.18). But $|F|$ and $|Z(P)|$ are coprime by assumption, so that $H^2(F, Z(P)) = 0$ by Proposition 1.18. Therefore the extension splits by a group homomorphism $s' : F \to Y$. Then the composite $s's$ is a splitting of the original sequence. The proof of the uniqueness statement is left as an exercise for the reader. □

(45.2) COROLLARY. *Let A be an interior G-algebra, let P_γ be a pointed group on A such that P is a p-group, and let*

$$q : N_G(P_\gamma)/C_G(P) \longrightarrow N_G(P_\gamma)/PC_G(P)$$

be the quotient map. If E is a subgroup of $N_G(P_\gamma)/PC_G(P)$ of order prime to p, there exists a group homomorphism $s : E \to N_G(P_\gamma)/C_G(P)$ such that $qs = id_E$. Moreover s is unique up to conjugation by an element of $PC_G(P)/C_G(P)$.

Proof. Let X be the inverse image of E in $N_G(P_\gamma)/C_G(P)$. Then there is a short exact sequence

$$1 \longrightarrow PC_G(P)/C_G(P) \longrightarrow X \longrightarrow E \longrightarrow 1,$$

and the result follows from Lemma 45.1. □

In the sequel, we choose a homomorphism s as in the corollary. In fact we shall construct in this section several homomorphisms which will always be unique up to some conjugation. The proof of each uniqueness statement will be left to the reader (see the exercises).

We continue with a pointed group on A such that P is a p-group. We have seen in Proposition 44.2 that for any element $g \in N_G(P_\gamma)$, there exists $a_g \in A_\gamma$ such that $a_g \cdot u \cdot a_g^{-1} = {}^g u \cdot 1_{A_\gamma}$ for all $u \in P$. Moreover a_g is unique up to right multiplication by an element of $(A_\gamma^P)^*$. For any interior P-algebra B, we define

$$N_B(P) = \{\, b \in B^* \mid b \cdot u \cdot b^{-1} \in P \cdot 1_B \text{ for all } u \in P \,\}.$$

This is the *normalizer* in B^* of the image of P, while the centralizer of the image of P is clearly $(B^P)^*$. The element a_g above belongs to $N_{A_\gamma}(P)$ and since it is defined up to an element of $(A_\gamma^P)^*$, its class in

$N_{A_\gamma}(P)/(A_\gamma^P)^*$ is now uniquely defined by g. Thus we have constructed a canonical group homomorphism

$$\phi : N_G(P_\gamma)/C_G(P) \longrightarrow N_{A_\gamma}(P)/(A_\gamma^P)^* \tag{45.3}$$

mapping the class of g to the class of a_g. It is clear that if $g \in P$, then we can choose $a_g = g{\cdot}1_A$. Therefore the homomorphism ϕ is an extension of the map $PC_G(P)/C_G(P) \to N_{A_\gamma}(P)/(A_\gamma^P)^*$ induced by the structural homomorphism $P \to N_{A_\gamma}(P)$.

Continuing with a given subgroup E of $N_G(P_\gamma)/PC_G(P)$ of order prime to p, we let $E' = s(E)$, a subgroup of $N_G(P_\gamma)/C_G(P)$. We still write ϕ for the restriction of ϕ to the subgroup E'. In the situation where P_γ is a defect of a block, it follows from Theorem 44.3 that $\phi : E' \to N_{A_\gamma}(P)/(A_\gamma^P)^*$ is injective, but this may not be the case in general. We let $F = \phi(E')$, a subgroup of $N_{A_\gamma}(P)/(A_\gamma^P)^*$ of order prime to p. Our aim is to lift F to a subgroup F' of $N_{A_\gamma}(P)/k^*$. Then the inverse image of F' in $N_{A_\gamma}(P)$ will be a central extension of F' with kernel k^*.

Recall that the short exact sequence $1 \to 1+\mathfrak{p} \to \mathcal{O}^* \to k^* \to 1$ splits uniquely (Lemma 2.3), so that one can regard k^* as a subgroup of $\mathcal{O}^*$. Consequently, for any $\mathcal{O}$-algebra A, one can regard k^* as a subgroup of A^* (Exercise 2.4). Since A_γ is a primitive P-algebra (by definition of localization), $A_\gamma^P/J(A_\gamma^P) \cong k$ and therefore there is a short exact sequence

$$1 \longrightarrow 1 + J(A_\gamma^P) \longrightarrow (A_\gamma^P)^* \longrightarrow k^* \longrightarrow 1 .$$

But since k^* maps uniquely to any $\mathcal{O}$-algebra, this sequence splits and $(A_\gamma^P)^* \cong k^* \times (1 + J(A_\gamma^P))$. The group $N_{A_\gamma}(P)$ normalizes the centralizer of P, namely the algebra A_γ^P, and its multiplicative subgroup $(A_\gamma^P)^*$. Moreover $N_{A_\gamma}(P)$ also normalizes $1 + J(A_\gamma^P)$ and k^*, because for any $a \in N_{A_\gamma}(P)$, the algebra automorphism $\mathrm{Conj}(a)$ of A_γ^P necessarily leaves the Jacobson radical invariant, as well as the scalars k^*.

Our main tool in the sequel is the notion of inverse limit of groups (in a special case). Let X be a group and let $\{X_n \mid n \geq 1\}$ be a family of normal subgroups of X such that $X_{n+1} \subseteq X_n$ for every $n \geq 1$. Then X is said to be the *inverse limit* of the groups X/X_n (written $X = \varprojlim(X/X_n)$) if the following two conditions are satisfied:

(a) $\bigcap_{n\geq 1} X_n = \{1\}$,
(b) For every family $(x_n)_{n\geq 1}$ of elements of X with $x_n \equiv x_{n+1} \bmod X_n$, there exists $x \in X$ such that $x \equiv x_n \bmod X_n$.

The element x is called the *limit* of the sequence $(x_n)_{n\geq 1}$. Note that condition (a) is equivalent to the requirement that x be unique in (b). Indeed if $x' \in X$ also satisfies $x' \equiv x_n \bmod X_n$, then $x'x^{-1} \in \bigcap_{n\geq 1} X_n$.

If $X = \varprojlim(X/X_n)$, then in order to define a group homomorphism $\phi : Y \to X$, it suffices to define group homomorphisms $\phi_n : Y \to X/X_n$ such that $\pi_{n+1,n}\phi_{n+1} = \phi_n$, where $\pi_{n+1,n} : X/X_{n+1} \to X/X_n$ denotes the quotient map. Indeed if $y \in Y$ and if, for each n, we choose $x_n \in X$ mapping to the element $\phi_n(y) \in X/X_n$, then the condition $\pi_{n+1,n}\phi_{n+1}(y) = \phi_n(y)$ implies that $x_n \equiv x_{n+1} \bmod X_n$. Thus there exists $x \in X$ such that $x \equiv x_n \bmod X_n$, and we define $\phi(y) = x$. The fact that ϕ is a group homomorphism follows from the uniqueness of limits. Indeed if $y' \in Y$ and if $x'_n \in X$ is mapped to $\phi_n(y') \in X/X_n$, then both $\phi(yy')$ and $\phi(y)\phi(y')$ are limits of the sequence $(x_n x'_n)_{n\geq 1}$.

(45.4) LEMMA. *Let X be a group, let $\{X_n \mid n \geq 1\}$ be a family of normal subgroups of X such that $X_{n+1} \subseteq X_n$ for every $n \geq 1$, and let Y be a subgroup of X containing X_1. If $Y = \varprojlim(Y/X_n)$, then $X = \varprojlim(X/X_n)$.*

Proof. The condition $\bigcap_{n\geq 1} X_n = \{1\}$ is satisfied by assumption. Let $(x_n)_{n\geq 1}$ be a sequence in X such that $x_n \equiv x_{n+1} \bmod X_n$. Define $y_n = x_1^{-1}x_n$. Since $x_n \equiv x_{n+1} \bmod X_1$, we have

$$x_1 \equiv x_2 \equiv \ldots \equiv x_n \bmod X_1 ,$$

and therefore $y_n \in X_1 \subseteq Y$. Moreover $y_n \equiv y_{n+1} \bmod X_n$, by applying left multiplication by x_1^{-1} to the relation for the sequence (x_n). Since $Y = \varprojlim(Y/X_n)$, there exists $y \in Y$ such that $y \equiv y_n \bmod X_n$ for all n. Letting $x = x_1 y$, we have $x \equiv x_1 y_n = x_n \bmod X_n$. □

Inverse limits of groups occur in the following context. Recall that if A is an $\mathcal{O}$-algebra, then $1 + J(A)$ is the kernel of the group homomorphism $A^* \to (A/J(A))^*$.

(45.5) LEMMA. *Let A be an $\mathcal{O}$-algebra. Then we have*

$$1 + J(A) = \varprojlim\big((1 + J(A))/(1 + J(A)^n)\big) .$$

Proof. If $x \in \bigcap_{n\geq 1}(1 + J(A)^n)$, then $x - 1 \in \bigcap_{n\geq 1} J(A)^n = \{0\}$ (by Exercise 2.3), and so $x = 1$, proving the first condition.

Let $(x_n)_{n\geq 1}$ be a sequence in $1 + J(A)$ such that

$$x_n \equiv x_{n+1} \bmod (1 + J(A)^n) .$$

Then we have $x_n = x_{n+1}(1 + a)$ for some $a \in J(A)^n$ and therefore $x_n - x_{n+1} = x_{n+1}a \in J(A)^n$. It follows that (x_n) is a Cauchy sequence in A, and since A is complete in the $J(A)$-adic topology (Proposition 2.8), (x_n) converges to some element $x \in A$. Then $x - x_n \in J(A)^n$ for each n. Indeed, by definition of convergence, there exists $N \geq n$ such that $x - x_N \in J(A)^n$, and so we have $x \equiv x_N \equiv x_n \bmod J(A)^n$. Therefore $x \equiv x_n \equiv 1 \bmod J(A)$, and so $x \in 1 + J(A)$. Moreover if we write $x = x_n + a$ for some $a \in J(A)^n$, then $x = x_n(1 + x_n^{-1}a) \in x_n(1 + J(A)^n)$. Thus $x \equiv x_n \bmod (1 + J(A)^n)$, as was to be shown. □

By Lemma 45.1, any extension of a group E of order prime to p by a normal p-subgroup P splits. We now prove that the same result holds with $1+J(A)$ instead of P, showing that $1+J(A)$ behaves like a p-group.

(45.6) LEMMA. *Let A be an $\mathcal{O}$-algebra and let X be a group containing $1+J(A)$ as a normal subgroup. Assume that the subgroup $1+J(A)^n$ is normal in X for every $n \geq 1$ and that $E = X/(1+J(A))$ is a finite group of order prime to p. Then the short exact sequence*

$$1 \longrightarrow 1 + J(A) \longrightarrow X \xrightarrow{\rho} E \longrightarrow 1$$

splits. Moreover the splitting is unique up to conjugation by an element of $1 + J(A)$.

Proof. Let $J = J(A)$ for simplicity. By Lemma 45.5, we have $1 + J = \lim\limits_{\leftarrow}\big((1+J)/(1+J^n)\big)$, and since $1 + J^n$ is normal in X by assumption, we also have $X = \lim\limits_{\leftarrow}(X/(1+J^n))$ by Lemma 45.4. Thus the existence of a group homomorphism $\sigma : E \to X$ is equivalent to the existence of group homomorphisms $\sigma_n : E \to X/(1+J^n)$ such that $\pi_{n+1,n}\sigma_{n+1} = \sigma_n$, where $\pi_{n+1,n} : X/(1+J^{n+1}) \to X/(1+J^n)$ denotes the quotient map. Moreover σ is a section of ρ if and only if $\rho_n\sigma_n = id_E$ for all n, where $\rho_n : X/(1+J^n) \to E$ denotes the homomorphism induced by ρ. Note that if σ_n is a section of ρ_n, then we can define σ_k for $k < n$ by $\pi_{k+1,k}\sigma_{k+1} = \sigma_k$, and then σ_k is a section of ρ_k. The existence of σ_1 is obvious since $\rho_1 : X/(1+J) \to E$ is an isomorphism.

Assume by induction that a section σ_n of ρ_n exists. Then $\sigma_n(E)$ is a subgroup of $X/(1+J^n)$ isomorphic to E, and we let F_{n+1} be the inverse image of $\sigma_n(E)$ in $X/(1+J^{n+1})$ under the map $\pi_{n+1,n}$. Thus there is a short exact sequence

$$1 \longrightarrow (1+J^n)/(1+J^{n+1}) \longrightarrow F_{n+1} \xrightarrow{\pi_{n+1,n}} \sigma_n(E) \longrightarrow 1 .$$

We claim that $(1+J^n)/(1+J^{n+1})$ is an abelian group of exponent p. Postponing the proof of the claim, we deduce that the map $a \mapsto a^{|E|}$ is an automorphism of $(1+J^n)/(1+J^{n+1})$, because $|E|$ is prime to p by assumption. This map induces an automorphism of the cohomology group $H^k\big(\sigma_n(E),(1+J^n)/(1+J^{n+1})\big)$ which is multiplication by $|E|$ (in additive notation). But multiplication by $|E|=|\sigma_n(E)|$ is zero in cohomology by Proposition 1.18. It follows that $H^k\big(\sigma_n(E),(1+J^n)/(1+J^{n+1})\big)=0$ for $k\geq 1$.

The vanishing of the second cohomology group implies the existence of a section of the above short exact sequence, that is, a map

$$\tau_{n+1}:\sigma_n(E)\to F_{n+1}\subseteq X/(1+J^{n+1})$$

such that $\pi_{n+1,n}\tau_{n+1}=id$. We let $\sigma_{n+1}=\tau_{n+1}\sigma_n:E\to X/(1+J^{n+1})$ and we have $\pi_{n+1,n}\sigma_{n+1}=\sigma_n$. Moreover σ_{n+1} is a section of ρ_{n+1} because

$$\rho_{n+1}\sigma_{n+1}=\rho_n\pi_{n+1,n}\tau_{n+1}\sigma_n=\rho_n\sigma_n=id_E\,,$$

using the obvious relation $\rho_{n+1}=\rho_n\pi_{n+1,n}$. This shows the existence of the section $\sigma:E\to X$. The additional uniqueness statement is left as an exercise for the reader.

It remains to prove the claim above. If $1+a,1+b\in 1+J^n$, then $(1+a)(1+b)=1+(a+b)+ab$ and $ab\in J^{2n}\subseteq J^{n+1}$. It follows that the map $1+a\mapsto a$ induces an isomorphism between the multiplicative group $(1+J^n)/(1+J^{n+1})$ and the additive group J^n/J^{n+1}, which is clearly abelian. Moreover $p{\cdot}a\in J^{n+1}$ if $a\in J^n$ because $p{\cdot}1_{\mathcal{O}}\in\mathfrak{p}$ (since $k=\mathcal{O}/\mathfrak{p}$ has characteristic p) and $\mathfrak{p}A\subseteq J$. This shows that J^n/J^{n+1} has exponent p. □

We now return to our original lifting problem.

(45.7) COROLLARY. *Let A be an interior G-algebra, let P_γ be a pointed group on A such that P is a p-group, let*

$$r:N_{A_\gamma}(P)/k^*\to N_{A_\gamma}(P)/(A_\gamma^P)^*$$

be the quotient map, and let F be a subgroup of $N_{A_\gamma}(P)/(A_\gamma^P)^*$ of order prime to p. There exists a group homomorphism $t:F\to N_{A_\gamma}(P)/k^*$ such that $rt=id_F$. Moreover t is unique up to conjugation by an element of $1+J(A_\gamma^P)$.

Proof. Since $(A_\gamma^P)^*\cong k^*\times(1+J(A_\gamma^P))$, the kernel of r is isomorphic to $1+J(A_\gamma^P)$. Let X be the inverse image of F in $N_{A_\gamma}(P)/k^*$. Then there is a short exact sequence

$$1\longrightarrow 1+J(A_\gamma^P)\longrightarrow X\longrightarrow F\longrightarrow 1\,,$$

and the result follows from Lemma 45.6. □

We now summarize the whole discussion. Let P_γ be a pointed group on an interior G-algebra A such that P is a p-group. Given a subgroup E of $N_G(P_\gamma)/PC_G(P)$ of order prime to p, we constructed a splitting $s: E \to N_G(P_\gamma)/C_G(P)$ (Corollary 45.2). Letting $E' = s(E)$, we restricted to E' the canonical map $\phi: N_G(P_\gamma)/C_G(P) \to N_{A_\gamma}(P)/(A_\gamma^P)^*$ defined in 45.3 and we defined $F = \phi(E')$. Finally we constructed a splitting $t : F \to N_{A_\gamma}(P)/k^*$ (Corollary 45.7). Now we define ψ to be the composite

$$\psi : E \xrightarrow{s} E' \xrightarrow{\phi} F \xrightarrow{t} N_{A_\gamma}(P)/k^* . \tag{45.8}$$

We note that the non-uniqueness of s and t imply that ψ is not unique, but is uniquely defined up to conjugation by an element of $P{\cdot}(1 + J(A_\gamma^P))$ (Exercise 45.3).

Let $F' = t(F)$, so that F' is the image of ψ, and let $\widehat{F}'$ be the inverse image of F' in $N_{A_\gamma}(P)$. Then $\widehat{F}'$ is a central extension of F' by k^*. The pull-back along ψ defines a central extension $\widehat{E}$ and we have the following commutative diagram.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & k^* & \longrightarrow & \widehat{E} & \longrightarrow & E & \longrightarrow & 1 \\
 & & {\scriptstyle id}\big\downarrow & & {\scriptstyle \widehat{\psi}}\big\downarrow & & {\scriptstyle \psi}\big\downarrow & & \\
1 & \longrightarrow & k^* & \longrightarrow & \widehat{F}' & \longrightarrow & F' & \longrightarrow & 1 \\
 & & {\scriptstyle id}\big\downarrow & & \big\downarrow & & \big\downarrow & & \\
1 & \longrightarrow & k^* & \longrightarrow & N_{A_\gamma}(P) & \longrightarrow & N_{A_\gamma}(P)/k^* & \longrightarrow & 1
\end{array} \tag{45.9}$$

(45.10) REMARKS. (a) We can give a direct description of $\widehat{E}$. The group $N_{A_\gamma}(P)/P{\cdot}(1 + J(A_\gamma^P))$ is a central extension of $N_{A_\gamma}(P)/P{\cdot}(A_\gamma^P)^*$ with kernel k^*. The canonical map ϕ defined in 45.3 induces (by passing to quotients by P) a group homomorphism $\overline{\phi}: E \to N_{A_\gamma}(P)/P{\cdot}(A_\gamma^P)^*$, and this defines by pull-back a central extension $\widehat{E}$ of E, as in the following diagram.

$$\begin{array}{ccc}
\widehat{E} & \longrightarrow & E \\
{\scriptstyle \widehat{\phi}}\big\downarrow & & {\scriptstyle \overline{\phi}}\big\downarrow \\
N_{A_\gamma}(P)/P{\cdot}(1 + J(A_\gamma^P)) & \longrightarrow & N_{A_\gamma}(P)/P{\cdot}(A_\gamma^P)^*
\end{array}$$

The fact that $\widehat{E}$ is the same central extension as above follows from the observation that we can take the pull-back in two steps along the map

$$\overline{\phi} : E \xrightarrow{\psi} N_{A_\gamma}(P)/k^* \longrightarrow N_{A_\gamma}(P)/P{\cdot}(A_\gamma^P)^* .$$

(b) The central extension $\widehat{E}$ has been constructed from the localization A_γ, but it is related with the central extension constructed from the multiplicity algebra. We take for simplicity $E = N_G(P_\gamma)/PC_G(P)$, because one does not need to have $(|E|, p) = 1$ for constructing the pull-back. We know that the multiplicity algebra $S(\gamma)$ has an $\overline{N}_G(P_\gamma)$-algebra structure which is interior on restriction to $PC_G(P)/P$. This defines a central extension $\widehat{\overline{N}}_G(P_\gamma)$ which splits on restriction to $PC_G(P)/P$ (see Example 10.9). Now the central extension $\widehat{E}$ above defines, by pull-back along $\pi : \overline{N}_G(P_\gamma) \to E$, a central extension $\widehat{\overline{N}}'_G(P_\gamma)$, which splits by construction on restriction to $PC_G(P)/P = \mathrm{Ker}(\pi)$. It can be shown that the central extensions $\widehat{\overline{N}}_G(P_\gamma)$ and $\widehat{\overline{N}}'_G(P_\gamma)$ are opposite. This means that there is an isomorphism $\widehat{\overline{N}}_G(P_\gamma) \to \widehat{\overline{N}}'_G(P_\gamma)$ of groups, which induces the identity on the quotient $\overline{N}_G(P_\gamma)$, but which induces on the central subgroup k^* the map $\lambda \mapsto \lambda^{-1}$.

Given any central extension $1 \to k^* \xrightarrow{\phi} \widehat{X} \to X \to 1$, there is a twisted group algebra $k_\sharp \widehat{X}$. This can be lifted to $\mathcal{O}$ as follows. Every $\lambda \in k^*$ lifts to $\lambda' \in \mathcal{O}^*$ via the unique homomorphism $k^* \to \mathcal{O}^*$ of Lemma 2.3. We define $\mathcal{O}_\sharp \widehat{X}$ to be the quotient of the group algebra $\mathcal{O}\widehat{X}$ by the ideal generated by the elements $\phi(\lambda) - \lambda'{\cdot}1$, where $\lambda \in k^*$. Thus the central subgroup k^* is identified with the scalars $k^* \subseteq \mathcal{O}^*$. In order to be consistent with Example 10.4, note that $\mathcal{O}_\sharp \widehat{X}$ can also be defined as the twisted group algebra $\mathcal{O}_\sharp \widehat{X}'$ associated with the central extension $1 \to \mathcal{O}^* \to \widehat{X}' \to X \to 1$ obtained by push-out from the extension above along the map $k^* \to \mathcal{O}^*$ (Exercise 45.5).

Now we come to the main result about source algebras of blocks. We apply all the constructions above to a defect P_γ of a block and to the group $E_G(P_\gamma) = N_G(P_\gamma)/PC_G(P)$, whose order is indeed prime to p by Theorem 37.9.

(45.11) THEOREM. *Let P_γ be a defect of a block b of $\mathcal{O}G$, let $E_G(P_\gamma) = N_G(P_\gamma)/PC_G(P)$, and let $\widehat{\psi} : \widehat{E}_G(P_\gamma) \to N_{(\mathcal{O}Gb)_\gamma}(P)$ be the homomorphism defined in 45.9. Let M be the subgroup of $N_{(\mathcal{O}Gb)_\gamma}(P)$ generated by $P{\cdot}1_{(\mathcal{O}Gb)_\gamma}$ and $\widehat{\psi}(\widehat{E}_G(P_\gamma))$, and let B be the $\mathcal{O}$-linear span of the group M in $(\mathcal{O}Gb)_\gamma$.*

(a) *The homomorphism* $\widehat{\psi}$ *is injective and its image intersects trivially the normal subgroup* $P{\cdot}1_{(\mathcal{O}Gb)_\gamma}$. *In other words* M *is isomorphic to a semi-direct product* $P{\rtimes}\widehat{E}_G(P_\gamma)$.

(b) *The* $\mathcal{O}$*-submodule* B *is a subalgebra and is isomorphic to a twisted group algebra* $\mathcal{O}_\sharp(P{\rtimes}\widehat{E}_G(P_\gamma))$ *(in the sense defined above).*

(c) *As an* $\mathcal{O}(P\times P)$*-module,* B *is a direct summand of* $(\mathcal{O}Gb)_\gamma$ *and is equal to* $B=\bigoplus_{g\in E_G(P_\gamma)}\mathcal{O}P{\cdot}a_g$, *where* $a_g=\widehat{\psi}(\widehat{g})$ *and* $\widehat{g}\in\widehat{E}_G(P_\gamma)$ *is an arbitrary lift of* $g\in E_G(P_\gamma)$.

(d) *Up to conjugation by an element of* $1+J((\mathcal{O}Gb)_\gamma^P)$ *, the subalgebra* B *is the unique interior* P*-subalgebra of* $(\mathcal{O}Gb)_\gamma$ *isomorphic to* $\mathcal{O}_\sharp(P{\rtimes}\widehat{E}_G(P_\gamma))$.

Proof. We first recall that the structural map $P\to P{\cdot}1_{(\mathcal{O}Gb)_\gamma}$ is injective (Exercise 38.2). For every $g\in E_G(P_\gamma)$, choose $\widehat{g}\in\widehat{E}_G(P_\gamma)$ mapping to g and let $a_g=\widehat{\psi}(\widehat{g})$. Then by construction of $\widehat{\psi}$ and by definition of the canonical map ϕ of 45.3, the element a_g satisfies

$$a_g{\cdot}u{\cdot}a_g^{-1}={}^{s(g)}u{\cdot}1_{(\mathcal{O}Gb)_\gamma}\qquad\text{for all } u\in P\,,$$

where $s(g)\in N_G(P_\gamma)/C_G(P)$ is the lift of g obtained in Corollary 45.2. Note here that $E_G(P_\gamma)$ is isomorphic to a group of outer automorphisms of P , so that we first need to use s to end up with genuine automorphisms of P . Therefore

$$B=\sum_{g\in E_G(P_\gamma)}\mathcal{O}P{\cdot}a_g\,.$$

By Theorem 44.3, this sum is direct and is a direct summand of $(\mathcal{O}Gb)_\gamma$. This proves (c).

Let $u,u'\in P$, $g,g'\in E_G(P_\gamma)$ and $\lambda,\lambda'\in k^*$ (identified with a subgroup of $\mathcal{O}^*$), and assume that $u{\cdot}\lambda a_g=u'{\cdot}\lambda' a_{g'}$. Since the above sum is direct and since $P{\cdot}a_g$ is a basis of $\mathcal{O}P{\cdot}a_g$ (see Theorem 44.3), we must have $u=u'$ and $g=g'$, and therefore $\lambda=\lambda'$. This shows the injectivity of $\widehat{\psi}$ and the fact that its image intersects $P{\cdot}1_{(\mathcal{O}Gb)_\gamma}$ trivially. Thus (a) is proved.

For simplicity we identify P with its image in $N_{(\mathcal{O}Gb)_\gamma}(P)$, we identify $\widehat{E}_G(P_\gamma)$ with its image in $N_{(\mathcal{O}Gb)_\gamma}(P)$ via $\widehat{\psi}$, and similarly we identify $E_G(P_\gamma)$ with its image in $N_{(\mathcal{O}Gb)_\gamma}(P)/k^*$ via ψ . This identifies the group M with the semi-direct product $P{\rtimes}\widehat{E}_G(P_\gamma)$. Since P intersects trivially the central subgroup k^* of $\widehat{E}_G(P_\gamma)$, we have a central extension

$$1\longrightarrow k^*\longrightarrow P{\rtimes}\widehat{E}_G(P_\gamma)\longrightarrow P{\rtimes}E_G(P_\gamma)\longrightarrow 1\,,$$

where the surjection is obtained by restriction from the quotient map $N_{(\mathcal{O}Gb)_\gamma}(P) \to N_{(\mathcal{O}Gb)_\gamma}(P)/k^*$. We consider the associated twisted group algebra $\mathcal{O}_\sharp(P \rtimes \widehat{E}_G(P_\gamma))$, as defined above. By $\mathcal{O}$-linearity, there is a surjective algebra homomorphism $\mathcal{O}(P \rtimes \widehat{E}_G(P_\gamma)) \to B$ defined on the whole group algebra $\mathcal{O}(P \rtimes \widehat{E}_G(P_\gamma))$, and since the central subgroup k^* is mapped to the scalars k^* in B^*, this induces in turn a surjective algebra homomorphism

$$\theta : \mathcal{O}_\sharp(P \rtimes \widehat{E}_G(P_\gamma)) \longrightarrow B .$$

The dimension of $\mathcal{O}_\sharp(P \rtimes \widehat{E}_G(P_\gamma))$ is equal to $|P| \cdot |E_G(P_\gamma)|$, and this is also the dimension of B, because $B = \bigoplus_{g \in E_G(P_\gamma)} \mathcal{O}P \cdot a_g$. Therefore θ is an isomorphism, proving (b).

The proof of (d) is left to the reader. □

Finally we come to the result giving its title to this section.

(45.12) THEOREM. *Let P_γ be a defect of a block b of $\mathcal{O}G$. If P is a normal subgroup of G, then $(\mathcal{O}Gb)_\gamma \cong \mathcal{O}_\sharp(P \rtimes \widehat{E}_G(P_\gamma))$.*

Proof. We use the notation of Theorem 45.11. By Theorem 44.3, $B = \bigoplus_{g \in E_G(P_\gamma)} \mathcal{O}P \cdot a_g$ is the whole source algebra when P is a normal subgroup. Therefore $(\mathcal{O}Gb)_\gamma = B \cong \mathcal{O}_\sharp(P \rtimes \widehat{E}_G(P_\gamma))$. □

We recover in particular the case of a central defect group (Theorem 39.4). Indeed we have $E_G(P_\gamma) = 1$ if P is central and therefore $(\mathcal{O}Gb)_\gamma \cong \mathcal{O}P$.

The semi-direct product $P \rtimes \widehat{E}_G(P_\gamma)$ depends on the action of $\widehat{E}_G(P_\gamma)$ on P. First note that this action factorizes through $E_G(P_\gamma)$, because the central subgroup k^* acts trivially. Now $E_G(P_\gamma)$ is isomorphic to a group of outer automorphisms of P, and in order to view it as a group of automorphisms, we have used the homomorphism $s : E_G(P_\gamma) \to N_G(P_\gamma)/C_G(P)$ (see Corollary 45.2). Another choice of s yields another action of $E_G(P_\gamma)$ on P. Thus we may wonder whether the semi-direct product $P \rtimes \widehat{E}_G(P_\gamma)$ depends on this choice, but our next result shows that we always obtain isomorphic groups.

(45.13) LEMMA. *With the notation above, let*

$$q : N_G(P_\gamma)/C_G(P) \longrightarrow N_G(P_\gamma)/PC_G(P) = E_G(P_\gamma)$$

be the canonical surjection and let $s, s' : E_G(P_\gamma) \to N_G(P_\gamma)/C_G(P)$ be two homomorphisms such that $qs = qs' = id$. Let $\widehat{E}$ be a group, let

$\rho : \widehat{E} \to E_G(P_\gamma)$ be a group homomorphism, so that $\widehat{E}$ acts on P via either $s\rho$ or $s'\rho$. Then there exists an isomorphism

$$P \rtimes_{s\rho} \widehat{E} \xrightarrow{\sim} P \rtimes_{s'\rho} \widehat{E}$$

extending some inner automorphism of P.

Proof. By Corollary 45.2, s is unique up to conjugation by an element of $PC_G(P)/C_G(P)$, so that there exists $v \in P$ such that $s'(e) = vs(e)v^{-1}$ for all $e \in E_G(P_\gamma)$. Then the semi-direct products with respect to $s\rho$ and $s'\rho$ are isomorphic via the map

$$P \rtimes_{s\rho} \widehat{E} \longrightarrow P \rtimes_{s'\rho} \widehat{E}\,, \qquad (u, a) \mapsto (vuv^{-1}, a)\,.$$

The verification is left to the reader. □

Exercises

(45.1) Prove the uniqueness statement in Lemma 45.1. [Hint: Follow the method of the proof of Lemma 45.1 and use the fact that the first cohomology group vanishes.]

(45.2) Prove the uniqueness statement in Lemma 45.6. [Hint: Follow the method of the proof of Lemma 45.6 and use the fact that the first cohomology group vanishes.]

(45.3) Prove that the homomorphism ψ defined in 45.8 is unique up to conjugation by an element of $P{\cdot}(1 + J(A_\gamma^P))$.

(45.4) Prove the uniqueness statement in Theorem 45.11. [Hint: Use the previous exercise.]

(45.5) Let $1 \to k^* \overset{\phi}{\to} \widehat{E} \to E \to 1$ be a central extension and let $\mathcal{O}_\sharp \widehat{E}$ be the quotient of the group algebra $\mathcal{O}\widehat{E}$ by the ideal generated by the elements $\phi(\lambda) - \lambda'{\cdot}1$, where $\lambda \in k^*$ and $\lambda \mapsto \lambda'$ is the unique homomorphism $k^* \to \mathcal{O}^*$ (Lemma 2.3). Consider the push-out

$$\begin{array}{ccccccccc} 1 & \longrightarrow & k^* & \longrightarrow & \widehat{E} & \longrightarrow & E & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle id} & & \\ 1 & \longrightarrow & \mathcal{O}^* & \longrightarrow & \widehat{E}' & \longrightarrow & E & \longrightarrow & 1 \end{array}$$

and let $\mathcal{O}_\sharp \widehat{E}'$ be the corresponding twisted group algebra (Example 10.4). Show that $\mathcal{O}_\sharp \widehat{E}$ and $\mathcal{O}_\sharp \widehat{E}'$ are isomorphic.

(45.6) Provide the details of the proof of Lemma 45.13.

Notes on Section 45

The two main theorems of this section are due to Puig [1988a] and extend some earlier work of Külshammer [1985] on blocks with a normal defect group. The relationship between the central extensions $\widehat{E}_G(P_\gamma)$ and $\widehat{\overline{N}}_G(P_\gamma)$ mentioned in Remark 45.10 is also proved in Puig [1988a].

§ 46 BILINEAR FORMS AND NUMBER OF BLOCKS

In this section, we study general bilinear forms on G-algebras over a field. As an application, we show that the number of blocks with a given defect group can be described as the rank of a suitable bilinear form. Throughout this section, we work over an algebraically closed field k of characteristic p. We only make use occasionally of a discrete valuation ring.

Let A be a G-algebra over k. A k-linear form $\lambda : A \to k$ is called *symmetric* if $\lambda(ab) = \lambda(ba)$ for all $a, b \in A$, and it is called *G-invariant* if $\lambda({}^g a) = \lambda(a)$ for all $g \in G$ and $a \in A$. The symmetric condition implies that $\lambda(aba^{-1}) = \lambda(b)$ if $a \in A^*$. Note that if A is an interior G-algebra, then any symmetric linear form on A is automatically G-invariant, because ${}^g a = g{\cdot}a{\cdot}g^{-1}$. Throughout this section $\lambda : A \to k$ denotes a symmetric G-invariant linear form on a G-algebra A over k. If λ is non-degenerate (that is, if the corresponding bilinear form $\phi(a,b) = \lambda(ab)$ is non-degenerate), then A is a symmetric algebra. However, we consider here symmetric G-invariant linear forms which need not be non-degenerate. Our first observation is that, for every p-subgroup P, the restriction to A^P of the form λ factorizes through the Brauer homomorphism. Recall that $\overline{N}_G(P) = N_G(P)/P$.

(46.1) LEMMA. *Let A be a G-algebra over k, let λ be a G-invariant symmetric linear form on A, and let P be a p-subgroup of G. Consider the restriction of λ to A^P.*

(a) $\mathrm{Ker}(br_P) \subseteq \mathrm{Ker}(\lambda)$.

(b) There exists a symmetric $\overline{N}_G(P)$-invariant linear form $\lambda_P : \overline{A}(P) \to k$ such that $\lambda(a) = \lambda_P(br_P(a))$ for all $a \in A^P$.

Proof. (a) If $Q < P$, then for every $a \in A^Q$, we have

$$\lambda(t_Q^P(a)) = \sum_{g \in [P/Q]} \lambda({}^g a) = \sum_{g \in [P/Q]} \lambda(a) = |P:Q|\,\lambda(a) = 0\,,$$

because p divides $|P:Q|$.

(b) By (a), there exists a linear form λ_P such that $\lambda(a) = \lambda_P(br_P(a))$ for all $a \in A^P$. It is clear that λ_P is symmetric and $\overline{N}_G(P)$-invariant. □

Given a G-algebra A over k, a symmetric G-invariant linear form $\lambda : A \to k$, and a p-subgroup P of G, we define a bilinear form

$$\text{(46.2)} \qquad \rho_{P,G}^{A,\lambda} : A_P^G \times A_P^G \longrightarrow k\,, \qquad \rho_{P,G}^{A,\lambda}(a,b) = \lambda(ab') = \lambda(a'b)\,,$$

where $a', b' \in A^P$ are such that $t_P^G(a') = a$ and $t_P^G(b') = b$. It is not obvious that this is well-defined and that the two definitions coincide. We first prove this.

(46.3) PROPOSITION. *Let A be a G-algebra over k, let λ be a G-invariant symmetric linear form on A, let P be a p-subgroup of G, and let $\rho_{P,G}^{A,\lambda}$ be the bilinear form defined in 46.2.*

(a) The form $\rho_{P,G}^{A,\lambda}$ is well-defined and symmetric.

(b) The form $\rho_{P,G}^{A,\lambda}$ is associative, that is, $\rho_{P,G}^{A,\lambda}(ab,c) = \rho_{P,G}^{A,\lambda}(a,bc)$ for all $a,b,c \in A_P^G$.

(c) For all $a,b \in A_P^G$, we have

$$\rho_{P,G}^{A,\lambda}(a,b) = \rho_{1,\overline{N}_G(P)}^{\overline{A}(P),\lambda_P}(br_P(a), br_P(b))\,,$$

where $\lambda_P : \overline{A}(P) \to k$ is induced by λ (Lemma 46.1).

Proof. If $a = t_P^G(a')$ and $b = t_P^G(b')$ with $a', b' \in A^P$, then we have $br_P(a) = t_1^{\overline{N}_G(P)}(br_P(a'))$ and $br_P(b) = t_1^{\overline{N}_G(P)}(br_P(b'))$ by Proposition 11.9. Thus by Lemma 46.1, we obtain

$$\begin{aligned}\rho_{P,G}^{A,\lambda}(a,b) &= \lambda(ab') = \lambda_P(br_P(ab')) = \lambda_P(br_P(a)br_P(b')) \\ &= \rho_{1,\overline{N}_G(P)}^{\overline{A}(P),\lambda_P}(br_P(a), br_P(b))\,.\end{aligned}$$

This shows that (c) is satisfied, and also that we can assume that $P = 1$, for we can replace (A, λ, G, P) by $(\overline{A}(P), \lambda_P, \overline{N}_G(P), 1)$.

Assume now that $P = 1$, so that $a = t_1^G(a')$ and $b = t_1^G(b')$. Since λ is G-invariant, we have $\lambda({}^g a' b') = \lambda(a' \, {}^{g^{-1}} b')$, and therefore

$$\text{(46.4)} \qquad \lambda(ab') = \lambda(\sum_{g \in G} {}^g a' b') = \lambda(\sum_{g \in G} a' \, {}^{g^{-1}} b') = \lambda(a'b) .$$

This shows that the two definitions of $\rho_{1,G}^{A,\lambda}$ coincide. Now if we write $b = t_1^G(b') = t_1^G(b'')$, we can apply 46.4 to both b' and b'' and we obtain $\lambda(ab') = \lambda(a'b) = \lambda(ab'')$. Thus the bilinear form $\rho_{1,G}^{A,\lambda}$ is well-defined. It is symmetric because λ is symmetric, so that $\lambda(ab') = \lambda(a'b) = \lambda(ba')$ using again 46.4. Since $t_1^G(a'b) = t_1^G(a')b = ab$, we have

$$\rho_{1,G}^{A,\lambda}(ab, c) = \lambda((a'b)c) = \lambda(a'(bc)) = \rho_{1,G}^{A,\lambda}(a, bc) ,$$

so that $\rho_{1,G}^{A,\lambda}$ is associative. □

Now we assume that λ vanishes on the Jacobson radical $J(A)$. This has a number of consequences which we discuss. A typical example of such a linear form λ is obtained as follows. Consider a point $\alpha \in \mathcal{P}(A)$, the canonical surjection $\pi_\alpha : A \to S(\alpha)$ onto the simple quotient $S(\alpha)$ corresponding to α, and the linear form

$$\chi_\alpha = \mathrm{tr} \cdot \pi_\alpha : A \longrightarrow k ,$$

where $\mathrm{tr} : S(\alpha) \to k$ is the trace form, as discussed in Section 32 (see Lemma 32.5). In other words χ_α is the character of A afforded by the simple A-module $V(\alpha)$. Clearly χ_α is symmetric because tr is symmetric. If $H = N_G(G_\alpha)$ denotes the stabilizer of α, then $S(\alpha)$ is an H-algebra and tr is H-invariant. Indeed the action of $h \in H$ on $S(\alpha)$ is equal to some inner automorphism $\mathrm{Inn}(\widehat{h})$ by the Skolem–Noether theorem, and so $\mathrm{tr}({}^h a) = \mathrm{tr}(\widehat{h} a \widehat{h}^{-1}) = \mathrm{tr}(a)$ for all $a \in S(\alpha)$ and $h \in H$. It follows that

$$\lambda = \sum_{g \in [G/H]} \chi_{{}^g \alpha} : A \longrightarrow k$$

is a G-invariant symmetric linear form on A. We have $J(A) \subseteq \mathrm{Ker}(\lambda)$ because $J(A) \subseteq \mathrm{Ker}(\pi_\alpha)$ for all $\alpha \in \mathcal{P}(A)$.

Any linear combination of such forms λ is again a G-invariant symmetric linear form on A vanishing on $J(A)$. We want to prove the converse. If λ is a G-invariant symmetric linear form on A and if $\alpha \in \mathcal{P}(A)$, then $\lambda(i)$ is constant when i runs over α and we write simply $\lambda(\alpha) = \lambda(i)$. Note that by G-invariance, we have $\lambda({}^g \alpha) = \lambda(\alpha)$.

(46.5) LEMMA. *Let A be a G-algebra over k, let λ be a G-invariant symmetric linear form on A, and assume that λ vanishes on $J(A)$. Then $\lambda = \sum_{\alpha \in \mathcal{P}(A)} \lambda(\alpha)\chi_\alpha$.*

Proof. Since $\lambda(J(A)) = 0$, we can replace A by $A/J(A)$ and assume that A is semi-simple. Then $A \cong \prod_{\alpha \in \mathcal{P}(A)} S(\alpha)$ and, by elementary linear algebra, the linear form λ is a sum

$$\lambda = \sum_{\alpha \in \mathcal{P}(A)} \lambda_\alpha \pi_\alpha ,$$

where $\lambda_\alpha : S(\alpha) \to k$ is a linear form. Clearly λ_α is symmetric (since it can be viewed as the restriction of λ to a direct summand). A well-known exercise of linear algebra asserts that any symmetric linear form on a matrix algebra is a scalar multiple of the trace form. Therefore $\lambda_\alpha = c_\alpha \,\mathrm{tr}$ for some $c_\alpha \in k$, and so

$$\lambda = \sum_{\alpha \in \mathcal{P}(A)} c_\alpha \;\mathrm{tr}\; \pi_\alpha = \sum_{\alpha \in \mathcal{P}(A)} c_\alpha \, \chi_\alpha .$$

By construction of χ_α, we have $\chi_\alpha(\beta) = 0$ if $\beta \neq \alpha$ because $\pi_\alpha(\beta) = 0$. Moreover $\chi_\alpha(\alpha) = 1_k$ because if $i \in \alpha$, then $\pi_\alpha(i)$ is a primitive idempotent of $S(\alpha)$, and a primitive idempotent has trace 1_k since it is a projection onto a one-dimensional subspace. It follows that

$$\lambda(\beta) = \sum_{\alpha \in \mathcal{P}(A)} c_\alpha \, \chi_\alpha(\beta) = c_\beta ,$$

proving that $\lambda = \sum_{\alpha \in \mathcal{P}(A)} \lambda(\alpha)\chi_\alpha$. □

(46.6) COROLLARY. *Let A be a G-algebra over k and let λ be a G-invariant symmetric linear form on A. Then λ vanishes on $J(A)$ if and only if $\lambda(a) = 0$ for every nilpotent element $a \in A$.*

Proof. One implication is obvious because every element of $J(A)$ is nilpotent. So assume that λ vanishes on $J(A)$. If a is nilpotent, then so is $\pi_\alpha(a)$ for every $\alpha \in \mathcal{P}(A)$. Thus $\chi_\alpha(a) = \mathrm{tr}\; \pi_\alpha(a) = 0$ since a nilpotent matrix has trace zero. The result now follows from Lemma 46.5. □

The effect of this corollary is that the assumption that $\lambda(J(A)) = 0$ is inherited by subalgebras.

(46.7) COROLLARY. *Let A be a G-algebra over k and let λ be a G-invariant symmetric linear form on A such that $\lambda(J(A)) = 0$. Then $\lambda(J(B)) = 0$ for every subalgebra B of A.*

Proof. This is an immediate consequence of Corollary 46.6 since every element of $J(B)$ is nilpotent. □

We now come to the local description of the form $\rho_{P,G}^{A,\lambda}$ under the assumption that $\lambda(J(A)) = 0$. Recall that $N_G(P)$ acts on the set $\mathcal{LP}(A^P)$ of local points of A^P. We write $[\mathcal{LP}(A^P)/N_G(P)]$ for a system of representatives of orbits.

(46.8) PROPOSITION. *Let A be a G-algebra over k, let λ be a G-invariant symmetric linear form on A vanishing on $J(A)$, and let P be a p-subgroup of G.*
(a) The corresponding bilinear form $\rho_{P,G}^{A,\lambda}$ on A_P^G satisfies

$$\rho_{P,G}^{A,\lambda}(a,b) = \sum_{\gamma \in [\mathcal{LP}(A^P)/N_G(P)]} \lambda(\gamma)\, \rho_{1,\overline{N}_G(P_\gamma)}^{S(\gamma),\mathrm{tr}}(\pi_\gamma(a), \pi_\gamma(b)) \,.$$

(b) The rank of $\rho_{P,G}^{A,\lambda}$ is equal to

$$\mathrm{rk}(\rho_{P,G}^{A,\lambda}) = \sum_{\substack{\gamma \in [\mathcal{LP}(A^P)/N_G(P)] \\ \lambda(\gamma) \neq 0}} \dim(S(\gamma)_1^{\overline{N}_G(P_\gamma)}) \,.$$

Proof. (a) Let λ' be the restriction of λ to A^P. By Corollary 46.7, $\lambda'(J(A^P)) = 0$, and so by Lemma 46.5, we have

$$\lambda' = \sum_{\gamma \in \mathcal{P}(A^P)} \lambda(\gamma)\chi_\gamma \,.$$

But $\lambda(\gamma) = 0$ if γ is not local because $\mathrm{Ker}(br_P) \subseteq \mathrm{Ker}(\lambda)$ by Lemma 46.1. Therefore

$$\lambda' = \sum_{\gamma \in \mathcal{LP}(A^P)} \lambda(\gamma)\chi_\gamma = \sum_{\gamma \in [\mathcal{LP}(A^P)/N_G(P)]} \lambda(\gamma) \sum_{g \in [N_G(P)/N_G(P_\gamma)]} \chi_{\,{}^g\gamma} \,.$$

The corresponding bilinear form $\rho_{P,G}^{A,\lambda}$ decomposes in the same way as a sum over $\gamma \in [\mathcal{LP}(A^P)/N_G(P)]$, with coefficients $\lambda(\gamma)$. Note that in fact $\rho_{P,G}^{A,\lambda}$ only depends on λ', not on λ.

Thus it suffices to consider each linear form $\sum_{g\in[N_G(P)/N_G(P_\gamma)]}\chi_{\,{}^g\gamma}$ separately, and we now assume that $\lambda' = \sum_{g\in[N_G(P)/N_G(P_\gamma)]}\chi_{\,{}^g\gamma}$ for some fixed local point $\gamma \in \mathcal{LP}(A^P)$. We then have to prove that the corresponding bilinear form $\rho^{A,\lambda}_{P,G}$ satisfies

$$\rho^{A,\lambda}_{P,G}(a,b) = \rho^{S(\gamma),\mathrm{tr}}_{1,\overline{N}_G(P_\gamma)}(\pi_\gamma(a),\pi_\gamma(b))$$

for all $a,b\in A^G_P$. By Proposition 46.3, we have

$$\rho^{A,\lambda}_{P,G}(a,b) = \rho^{\overline{A}(P),\lambda_P}_{1,\overline{N}_G(P)}(br_P(a),br_P(b))\,.$$

Let $\overline{\gamma} = br_P(\gamma)$ be the corresponding point of $\overline{A}(P)$, let $\pi_{\overline{\gamma}} : \overline{A}(P)\to S(\gamma)$ be the canonical map (so that $\pi_\gamma = \pi_{\overline{\gamma}}\,br_P$), and let $\chi_{\overline{\gamma}} = \mathrm{tr}\ \pi_{\overline{\gamma}}$ be the corresponding linear form. Then we have

$$\lambda_P \;=\; \sum_{g\in[N_G(P)/N_G(P_\gamma)]} \chi_{\,{}^g\overline{\gamma}}\,.$$

Changing notation, we let $a,b\in \overline{A}(P)_1^{\overline{N}_G(P)}$, and we choose $b'\in\overline{A}(P)$ such that $t_1^{\overline{N}_G(P)}(b') = b$. By a trivial special case of the Mackey decomposition formula, we have

$$\text{(46.9)}\qquad b \;=\; r^{\overline{N}_G(P)}_{\overline{N}_G(P_\gamma)}\, t_1^{\overline{N}_G(P)}(b') \;=\; t_1^{\overline{N}_G(P_\gamma)}\Big(\sum_{g\in[N_G(P_\gamma)\backslash N_G(P)]} {}^g b'\Big)\,.$$

Using the easy property $\mathrm{tr}\ \pi_{\,{}^g\overline{\gamma}}(c) = \mathrm{tr}\ \pi_{\overline{\gamma}}({}^{g^{-1}}c)$ (see Exercise 46.2), and then setting $h = g^{-1}$, it follows that

$$\begin{aligned}
\rho^{\overline{A}(P),\lambda_P}_{1,\overline{N}_G(P)}(a,b) \;&=\; \lambda_P(ab') \;=\; \sum_{g\in[N_G(P)/N_G(P_\gamma)]} \chi_{\,{}^g\overline{\gamma}}(ab')\\
&=\; \sum_{g\in[N_G(P)/N_G(P_\gamma)]} \mathrm{tr}\ \pi_{\,{}^g\overline{\gamma}}(ab')\\
&=\; \sum_{g\in[N_G(P)/N_G(P_\gamma)]} \mathrm{tr}\ \pi_{\overline{\gamma}}({}^{g^{-1}}(ab'))\\
&=\; \sum_{g\in[N_G(P)/N_G(P_\gamma)]} \mathrm{tr}\ \pi_{\overline{\gamma}}(a\,{}^{g^{-1}}b')\\
&=\; \mathrm{tr}\Big(\pi_{\overline{\gamma}}(a)\pi_{\overline{\gamma}}\big(\sum_{h\in[N_G(P_\gamma)\backslash N_G(P)]} {}^h b'\big)\Big)\\
&=\; \rho^{S(\gamma),\mathrm{tr}}_{1,\overline{N}_G(P_\gamma)}(\pi_{\overline{\gamma}}(a),\pi_{\overline{\gamma}}(b))\,.
\end{aligned}$$

The last equality follows from the definition of $\rho^{S(\gamma),\mathrm{tr}}_{1,\overline{N}_G(P_\gamma)}$ and the fact that, by 46.9, we have

$$\begin{aligned} t_1^{\overline{N}_G(P_\gamma)}\big(\pi_{\overline{\gamma}}\big(\sum_{h\in[N_G(P_\gamma)\backslash N_G(P)]} {}^h b'\big)\big) &= \pi_{\overline{\gamma}}\big(t_1^{\overline{N}_G(P_\gamma)}\big(\sum_{h\in[N_G(P_\gamma)\backslash N_G(P)]} {}^h b'\big)\big) \\ &= \pi_{\overline{\gamma}}(b)\,. \end{aligned}$$

This completes the proof of (a).

(b) By Proposition 14.7, we have

$$\pi_\gamma\, t_P^G(A^P\delta A^P) = \begin{cases} S(\gamma)_1^{\overline{N}_G(P_\gamma)} & \text{if } \gamma=\delta, \\ 0 & \text{if } \gamma \text{ and } \delta \text{ are not } N_G(P)\text{-conjugate.} \end{cases}$$

It follows that the map

$$\prod_{\gamma\in[\mathcal{LP}(A^P)/N_G(P)]} \pi_\gamma \;:\; A_P^G \;\longrightarrow\; \prod_{\gamma\in[\mathcal{LP}(A^P)/N_G(P)]} S(\gamma)_1^{\overline{N}_G(P_\gamma)}$$

is surjective. By (a), the form $\rho^{A,\lambda}_{P,G}$ on A_P^G is obtained by first applying this map and then the sum of the forms $\lambda(\gamma)\,\rho^{S(\gamma),\mathrm{tr}}_{1,\overline{N}_G(P_\gamma)}$. Therefore the rank of $\rho^{A,\lambda}_{P,G}$ is the sum of the ranks of the forms $\lambda(\gamma)\,\rho^{S(\gamma),\mathrm{tr}}_{1,\overline{N}_G(P_\gamma)}$. This is zero if $\lambda(\gamma)=0$ and is simply the rank of $\rho^{S(\gamma),\mathrm{tr}}_{1,\overline{N}_G(P_\gamma)}$ if the scalar $\lambda(\gamma)$ is non-zero.

Thus it suffices to show that

$$\mathrm{rk}(\rho^{S(\gamma),\mathrm{tr}}_{1,\overline{N}_G(P_\gamma)}) = \dim(S(\gamma)_1^{\overline{N}_G(P_\gamma)})\,.$$

Since the form is defined on the whole of $S(\gamma)_1^{\overline{N}_G(P_\gamma)}$, this is equivalent to the fact that the kernel of the form is zero. In order to prove this, we let $a\in \mathrm{Ker}(\rho^{S(\gamma),\mathrm{tr}}_{1,\overline{N}_G(P_\gamma)})$. Then for all $b=t_1^{\overline{N}_G(P_\gamma)}(b')\in S(\gamma)_1^{\overline{N}_G(P_\gamma)}$, we have $\mathrm{tr}(ab')=0$, which means that a lies in the kernel of the trace form since $b'\in S(\gamma)$ is arbitrary. By non-degeneracy of tr, we obtain $a=0$, as required. □

We now specialize to the case of a block algebra. In that situation the form $\rho^{A,\lambda}_{P,G}$ on A_P^G is always zero except in one case.

(46.10) PROPOSITION. *Let $A = kGb$ be a block algebra. Let λ be a G-invariant symmetric linear form on A vanishing on $J(A)$, and let P be a p-subgroup of G.*

(a) If P is not a defect group of A, then $\rho^{A,\lambda}_{P,G} = 0$.

(b) If P is a defect group of A, then $\rho^{A,\lambda}_{P,G} \neq 0$ if and only if $\lambda(\gamma) \neq 0$, where γ is a source point of A. In that case $\mathrm{rk}(\rho^{A,\lambda}_{P,G}) = 1$.

Proof. (a) If P is not contained in a defect group of A, then $\overline{A}(P) = 0$ (Corollary 18.6). Thus br_P is the zero map and $\rho^{A,\lambda}_{P,G} = 0$ by Proposition 46.3. If P is strictly contained in a defect group of A, then $A^G_P \neq A^G$ (Proposition 18.5) and therefore $A^G_P \subseteq J(A^G)$ since A^G is a local ring. Thus every element $a \in A^G_P$ is nilpotent. But a is also central (because $(kGb)^G = ZkGb$), so that ab' is nilpotent for every $b' \in A$. If now $b \in A^G_P$ is written $b = t^G_P(b')$, we obtain

$$\rho^{A,\lambda}_{P,G}(a,b) = \lambda(ab') = 0$$

because λ vanishes on nilpotent elements by Corollary 46.6.

(b) Let P be a defect group of A. Since A is primitive, there is a unique $N_G(P)$-conjugacy class of local points of A^P, namely the source points of A (Corollary 18.4). If γ is one of them, then by Proposition 46.8 we have

$$\rho^{A,\lambda}_{P,G}(a,b) = \lambda(\gamma)\, \rho^{S(\gamma),\mathrm{tr}}_{1,\overline{N}_G(P_\gamma)}(\pi_\gamma(a), \pi_\gamma(b))\,.$$

In particular $\rho^{A,\lambda}_{P,G} = 0$ if $\lambda(\gamma) = 0$. Assuming now that $\lambda(\gamma) \neq 0$, we have to prove that $\rho^{A,\lambda}_{P,G} \neq 0$ and that $\mathrm{rk}(\rho^{A,\lambda}_{P,G}) = 1$. Clearly it suffices to prove the latter equality.

We have $S(\gamma) \cong \mathrm{End}_k(V(\gamma))$ and, by Corollary 37.6, the defect multiplicity module $V(\gamma)$ is simple (and projective) over $k_\sharp\widehat{\overline{N}}_G(P_\gamma)$. Therefore, by Schur's lemma,

$$S(\gamma)_1^{\overline{N}_G(P_\gamma)} = S(\gamma)^{\overline{N}_G(P_\gamma)} \cong k\,.$$

By Proposition 46.8 and the assumption that $\lambda(\gamma) \neq 0$, we have

$$\mathrm{rk}(\rho^{A,\lambda}_{P,G}) = \dim(S(\gamma)_1^{\overline{N}_G(P_\gamma)}) = 1\,,$$

and the proof is complete. □

We apply this result to the group algebra kG, which is the direct sum of its block algebras kGb.

(46.11) COROLLARY. *Let λ be a G-invariant symmetric linear form on kG vanishing on $J(kG)$, and let P be a p-subgroup of G. The rank of the form $\rho_{P,G}^{kG,\lambda}$ is equal to the number of blocks b of kG such that P is a defect group of b and $\lambda(\gamma)\neq 0$, where γ is a source point of b.*

Proof. If b and b' are distinct blocks of kG, then $bb'=0$ and

$$\rho_{P,G}^{kG,\lambda}(ab,a'b') = \rho_{P,G}^{kG,\lambda}(ab,b'a') = \rho_{P,G}^{kG,\lambda}(abb',a') = 0$$

for all $a,a'\in (kG)_P^G$. Therefore the decomposition $(kG)_P^G = \bigoplus_b (kGb)_P^G$, where b runs over the blocks of kG, is orthogonal with respect to the form $\rho_{P,G}^{kG,\lambda}$. It follows that

$$\mathrm{rk}(\rho_{P,G}^{kG,\lambda}) = \sum_b \mathrm{rk}(\rho_{P,G}^{kGb,\lambda}).$$

By Proposition 46.10, $\mathrm{rk}(\rho_{P,G}^{kGb,\lambda})\neq 0$ only when P is a defect group of b and $\lambda(\gamma)\neq 0$, where γ is a source point of b, and in that case $\mathrm{rk}(\rho_{P,G}^{kGb,\lambda})=1$. The result follows immediately from this. □

In order to describe the number of blocks with defect group P as the rank of a bilinear form, we want to find a linear form λ such that the second property of the corollary (namely $\lambda(\gamma)\neq 0$) is always satisfied. To this end, we make a short digression and prove that the multiplication by a block leaves invariant the linear combinations of elements of G_{reg}. For any commutative ring R, we let ZRG_{reg} be the R-submodule of ZRG spanned by the class sums of p-regular elements of G.

(46.12) PROPOSITION. *Let b be a block of $\mathcal{O}G$.*
(a) Assume that $\mathcal{O}$ is a complete discrete valuation ring of characteristic zero (satisfying Assumption 42.1). Then $b\cdot Z\mathcal{O}G_{\mathrm{reg}} \subseteq Z\mathcal{O}G_{\mathrm{reg}}$.
(b) Assume that $\mathcal{O}=k$. Then $b\cdot ZkG_{\mathrm{reg}}\subseteq ZkG_{\mathrm{reg}}$.

Proof. (a) Let K be the field of fractions of $\mathcal{O}$. It suffices to show that $b\cdot ZKG_{\mathrm{reg}}\subseteq ZKG_{\mathrm{reg}}$, because $ZKG_{\mathrm{reg}}\cap Z\mathcal{O}G = Z\mathcal{O}G_{\mathrm{reg}}$. Let $a=\sum_{g\in G} f(g^{-1})g \in ZKG_{\mathrm{reg}}$, with $f(g^{-1})\in K$. It is here more convenient to view the coefficient of g as a function of g^{-1}. Since a is central, $f(hgh^{-1})=f(g)$ for all $g,h\in G$. Thus f is a central function on G vanishing outside G_{reg}. By Proposition 42.10, f is a K-linear combination of characters of projective $\mathcal{O}G$-lattices, that is,

$$f=\sum_i c_i\,\chi_{P_i}\,, \qquad c_i\in K\,,$$

where P_i is a projective $\mathcal{O}G$-lattice. Clearly the direct summand bP_i belonging to b is again projective. By Lemma 43.1, the character of bP_i satisfies $\chi_{bP_i}(g) = \chi_{P_i}(gb)$ for all $g \in G$. Therefore

$$f(gb) = \sum_i c_i \, \chi_{P_i}(gb) = \sum_i c_i \, \chi_{bP_i}(g) \, ,$$

and this is zero if $g \notin G_{\mathrm{reg}}$ since bP_i is projective (Proposition 42.10). Thus the function $g \mapsto f(gb)$ is a central function on G vanishing outside G_{reg}.

For every $x \in G$, we have $xa = \sum_{g \in G} f(g^{-1})xg = \sum_{h \in G} f(h^{-1}x)h$ because $h = xg$ runs again over G when g does. By K-linearity, the same equation holds for every $x \in KG$. We now take $x = b$ and use the above fact that $f(h^{-1}b) = 0$ if $h^{-1} \notin G_{\mathrm{reg}}$ (that is, $h \notin G_{\mathrm{reg}}$). Thus ba is a linear combination of G_{reg} and is still central (because b is central). In other words $ba \in ZKG_{\mathrm{reg}}$, as was to be shown.

(b) For every algebraically closed field k of characteristic p, there exists a complete discrete valuation ring $\mathcal{O}$ of characteristic zero satisfying Assumption 42.1 and such that $\mathcal{O}/\mathfrak{p}\mathcal{O} = k$ (Example 2.2). The block b of ZkG lifts to a block $\widetilde{b}$ of $Z\mathcal{O}G$ and we have $\widetilde{b}\cdot Z\mathcal{O}G_{\mathrm{reg}} \subseteq Z\mathcal{O}G_{\mathrm{reg}}$ by (a). It follows immediately that $b\cdot ZkG_{\mathrm{reg}} \subseteq ZkG_{\mathrm{reg}}$. □

(46.13) COROLLARY. *Suppose that $\mathcal{O}$ satisfies the assumption of either (a) or (b) in the above proposition. Then for every block b of $\mathcal{O}G$, we have $b \in Z\mathcal{O}G_{\mathrm{reg}}$.*

Proof. It suffices to multiply by b the element $1_{\mathcal{O}G} \in Z\mathcal{O}G_{\mathrm{reg}}$. □

It can be shown that the proposition and its corollary hold more generally for any ring $\mathcal{O}$ satisfying our usual Assumption 2.1.

Returning to our bilinear forms, we want to find a linear form on kG which never vanishes on source points of blocks. We define $\overline{\chi} : kG \to k$ to be the k-valued character of the permutation kG-module $k[G/Q]$, where Q is a Sylow p-subgroup of G. In other words $\overline{\chi}(a)$ is the trace of the action of a on $k[G/Q]$, for every $a \in kG$. Since the trace of a nilpotent element is zero, it is clear that $\overline{\chi}$ vanishes on $J(kG)$. In fact $\overline{\chi}$ is obtained by reduction modulo $\mathfrak{p}$ from an $\mathcal{O}$-valued ordinary character χ, as follows. Assume that $\mathcal{O}$ is a complete discrete valuation ring of characteristic zero (satisfying Assumption 42.1). Then the permutation module $k[G/Q]$ lifts to the permutation $\mathcal{O}G$-lattice $\mathcal{O}[G/Q]$, and we let χ be the ordinary character of $\mathcal{O}[G/Q]$. Clearly $\overline{\chi}(g)$ is the reduction modulo $\mathfrak{p}$ of $\chi(g)$. We first give an explicit description of the values of χ and $\overline{\chi}$.

(46.14) LEMMA. *Let* χ *be the ordinary character defined above, let* G_p *be the set of all elements of* G *of order a power of* p, *and let* $g \in G$.
(a) *If* $g \notin G_p$, *then* $\chi(g) = 0$.
(b) *If* $g \in G_p$, *then* $\overline{\chi}(g) = |G : Q|{\cdot}1_k$. *In other words, the function* $|G : Q|^{-1}\overline{\chi}$ *on* G *is the characteristic function of* G_p.

Proof. Let $X = G/Q$, endowed with the left action of G. With respect to the basis X, the action of g on $\mathcal{O}X$ is given by a permutation matrix. The diagonal entry indexed by x is zero if $g{\cdot}x \neq x$ and is one if $g{\cdot}x = x$. Therefore

$$\chi(g) = \mathrm{tr}(g; \mathcal{O}X) = |X^g|{\cdot}1_{\mathcal{O}},$$

where X^g is the set of g-fixed elements in X. Now X^g is the set of all cosets hQ such that $ghQ = hQ$, that is, ${}^{h^{-1}}g \in Q$. If $g \notin G_p$, then no conjugate of g lies in Q, so that X^g is empty and $\chi(g) = 0$. If $g \in G_p$, then write $X = X^g \cup Y$, where Y is the union of all non-trivial orbits of g. Every such non-trivial orbit has cardinality divisible by p, because g has order a power of p (so that any subgroup of the cyclic group $<g>$ has index a power of p). It follows that $|X| \equiv |X^g| \pmod{p}$ and, since k has characteristic p,

$$\overline{\chi}(g) = |X^g|{\cdot}1_k = |X|{\cdot}1_k = |G : Q|{\cdot}1_k,$$

as was to be shown. □

The desired property of the character $\overline{\chi}$ is the following.

(46.15) PROPOSITION. *Let* $\overline{\chi}$ *be the character of the permutation* kG*-module* $k[G/Q]$, *where* Q *is a Sylow* p*-subgroup of* G. *Let* b *be any block of* kG *and let* γ *be a source point of* b. *Then* $\overline{\chi}(\gamma) \neq 0$.

Proof. By Proposition 46.12, $\overline{\chi}(\gamma) \neq 0$ if and only if $\rho_{P,G}^{kGb,\overline{\chi}} \neq 0$, where P is a defect group of b. Thus it suffices to show that this form is non-zero. Write $b = \sum_{g \in G} \overline{f}(g^{-1})g$ with $\overline{f}(g) \in k$. We know that $br_P(b) \neq 0$ (Proposition 18.5) and that $br_P(b) = \sum_{g \in C_G(P)} \overline{f}(g^{-1})g$ (Proposition 37.5). By Corollary 46.13 and since $br_P(b)$ is a sum of blocks of $kC_G(P)$, there exists $g_0 \in C_G(P)_{\mathrm{reg}}$ such that $\overline{f}(g_0) \neq 0$. We have $g_0 \in (kG)^P$, so that $t_P^G(g_0 b) = t_P^G(g_0)b \in (kGb)_P^G$. Moreover $b \in (kGb)_P^G$ because P is a defect group of b. By definition of the form $\rho_{P,G}^{kGb,\overline{\chi}}$, we have

$$\rho_{P,G}^{kGb,\overline{\chi}}(t_P^G(g_0 b), b) = \overline{\chi}(g_0 bb) = \overline{\chi}(g_0 b).$$

We claim that $\overline{\chi}(g_0 b) = |G:Q|{\cdot}\overline{f}(g_0)$. This will complete the proof since $|G:Q|{\cdot}\overline{f}(g_0) \neq 0$.

In order to be able to use denominators, we work with the complete discrete valuation ring $\mathcal{O}$ of characteristic zero (satisfying Assumption 42.1) and with the ordinary character χ . Let $\widetilde{b} \in \mathcal{O}G$ be the (unique) block of $\mathcal{O}G$ lifting $b \in kG$ and write $\widetilde{b} = \sum_{g\in G} f(g^{-1})g$, so that $f(g)$ maps to $\overline{f}(g)$ by reduction modulo $\mathfrak{p}$. The sum of all conjugates of g_0 is the central element $t_C^G(g_0)$ where $C = C_G(g_0)$. Since χ is a central function, we have

$$\chi(g_0\widetilde{b}) = |G:C|^{-1}\chi(t_C^G(g_0)\widetilde{b})$$

in the field of fractions K of $\mathcal{O}$. Now $t_C^G(g_0) \in Z\mathcal{O}G_{\mathrm{reg}}$ and by Proposition 46.12, $t_C^G(g_0)\widetilde{b} \in Z\mathcal{O}G_{\mathrm{reg}}$. Since $G_{\mathrm{reg}} \cap G_p = \{1\}$ and since χ vanishes outside G_p (Lemma 46.14), we obtain

$$\chi(t_C^G(g_0)\widetilde{b}) = a\,\chi(1) = |G:Q|a\,,$$

where a is the coefficient of 1 in the expression of $t_C^G(g_0)\widetilde{b} = t_C^G(g_0\widetilde{b})$. Since the coefficient of 1 in $g_0\widetilde{b}$ is equal to $f(g_0)$, we have $a = |G:C|f(g_0)$. Summarizing this computation, we deduce that

$$\chi(g_0\widetilde{b}) = |G:C|^{-1}|G:Q|a = |G:Q|f(g_0)\,.$$

This implies in particular that $\overline{\chi}(g_0 b) = |G:Q|\overline{f}(g_0)$, as required. □

Proposition 46.15 can be used to give a new proof of Proposition 44.9, as follows.

(46.16) COROLLARY. *Let the interior P-algebra $(\mathcal{O}Gb)_\gamma$ be a source algebra of a block b of $\mathcal{O}G$. Then there exists a simple $(\mathcal{O}Gb)_\gamma$-module of dimension prime to p .*

Proof. Since we are considering simple modules, we can assume that $\mathcal{O} = k$. Let $\overline{\chi}_M$ be the k-valued character of the permutation kG-module $M = k[G/Q]$, where Q is a Sylow p-subgroup of G . We can assume that $(kGb)_\gamma = ikGi$, where $i \in \gamma$. Consider the $ikGi$-module iM and its k-valued character $\overline{\chi}_{iM}$. By Lemma 43.1 and Proposition 46.15, we have

$$\dim(iM){\cdot}1_k = \overline{\chi}_{iM}(1) = \overline{\chi}_M(i) \neq 0\,,$$

so that p does not divide $\dim(iM)$. It follows that some simple $ikGi$-module has dimension prime to p , otherwise p would divide the dimension of every $ikGi$-module. □

We have used in the proof of Proposition 46.15 the ordinary character χ and the lifted block $\widetilde{b}$ of $\mathcal{O}G$. The property that $\overline{\chi}(\gamma) \neq 0$ (or equivalently that $\rho_{P,G}^{kGb,\overline{\chi}} \neq 0$) can in fact be stated in a third way using χ and $\widetilde{b}$: the element $|G : P|^{-1}\chi(\widetilde{b})$ is an invertible element of $\mathcal{O}$ (Exercise 46.3). This means that the character χ has *height zero* (with respect to $\widetilde{b}$). If χ is an arbitrary character, $\chi(\widetilde{b})$ is always an integral multiple of $|G : P|$, and the exponent of the highest power of p dividing $|G : P|^{-1}\chi(\widetilde{b})$ is called the *height* of χ (with respect to $\widetilde{b}$). In a way similar to the proof of Corollary 46.16, one can prove that there always exists an irreducible ordinary character χ associated with a block $\widetilde{b}$ such that χ has height zero (Exercise 46.3).

We now come to the main result of this section.

(46.17) THEOREM (Robinson's theorem). *Let Q be a Sylow p-subgroup of G, let $\overline{\chi}$ be the character of the permutation kG-module $k[G/Q]$, and let P be any p-subgroup of G. Then the rank of the form $\rho_{P,G}^{kG,\overline{\chi}}$ on $(kG)_P^G$ is equal to the number of blocks of kG with defect group P.*

Proof. This is an immediate application of Corollary 46.11 in view of the fact that $\overline{\chi}(\gamma) \neq 0$ for every source point γ of a block (Proposition 46.15). $\square$

(46.18) REMARK. The form $\rho_{P,G}^{kG,\overline{\chi}}$ is defined on the space $(kG)_P^G$, which has a basis consisting of all class sums of elements $g \in G$ such that a Sylow p-subgroup of $C_G(g)$ is contained in a conjugate of P (Exercise 37.2). This gives an explicit description of the rank of $\rho_{P,G}^{kG,\overline{\chi}}$ as the rank of a suitable matrix. A further study of this matrix shows that only a small subset of the basis actually plays a role, for many basis elements lie in the kernel of the form. For instance one only needs to consider the conjugacy class of g when P is exactly a Sylow p-subgroup of $C_G(g)$. This yields a much smaller matrix, whose rank is the number of blocks with defect group P.

Exercises

(46.1) Prove that Proposition 46.10 holds more generally for any primitive G-algebra A such that A^G is central in A. [Hint: If P_γ is a defect of A, use Theorem 19.2 to show that $S(\gamma)^{\overline{N}_G(P_\gamma)}$ is central in $S(\gamma)$, hence isomorphic to k.]

(46.2) Let P_γ be a pointed group on a G-algebra A and let $g \in N_G(P)$. For every $c \in A^P$, prove that $\mathrm{tr}\, \pi_{{}^g\gamma}(c) = \mathrm{tr}\, \pi_\gamma({}^{g^{-1}}c)$. [Hint: Show that the isomorphism $S(\gamma) \xrightarrow{\sim} S({}^g\gamma)$ induced by conjugation by g necessarily preserves traces.]

(46.3) Assume that $\mathcal{O}$ is a complete discrete valuation ring of characteristic zero (satisfying Assumption 42.1), let b be a block of $\mathcal{O}G$ with defect P_γ, and let $\bar{b}$ and $\bar{\gamma}$ be the images of b and γ in kG. Let χ be the character of an $\mathcal{O}G$-lattice M and let $\overline{\chi}$ be its reduction modulo $\mathfrak{p}$ (so that $\overline{\chi}$ is the k-valued character of $M/\mathfrak{p}M$).

(a) Prove that $\chi(b) = \dim(bM)$ and that it is a multiple of $|G:P|$. [Hint: Show that $\chi(b) = |G:P|\,\chi(c)$ where $b = t_P^G(c)$ and $c \in (\mathcal{O}Gb)^P$.]

(b) Prove that the following conditions are equivalent.

(i) p does not divide $|G:P|^{-1}\chi(b)$ (that is, χ has height zero with respect to b).

(ii) $|G:P|^{-1}\chi(b)$ is invertible in $\mathcal{O}$.

(iii) p does not divide $\chi(i)$, for any $i \in \gamma$.

(iv) $\overline{\chi}(\overline{\gamma}) \neq 0$.

(v) The bilinear form $\rho_{P,G}^{kG\bar{b},\overline{\chi}}$ is non-zero.

[Hint: The equivalence of (iii), (iv), and (v) follows from Proposition 46.10. Let c be as in (a) and let $\bar{c}$ be its image in kG. Prove that $\rho_{P,G}^{kG\bar{b},\overline{\chi}}(\bar{b},\bar{b}) = \overline{\chi}(\bar{c})$ and that (ii) is equivalent to $\overline{\chi}(\bar{c}) \neq 0$. Deduce that (ii) and (v) are equivalent, using the fact that $\rho_{P,G}^{kG\bar{b},\overline{\chi}}$ always vanishes on the codimension-one subspace $J(ZkG\bar{b})$ of $ZkG\bar{b} = (kG\bar{b})_P^G$.]

(c) Prove that there always exists an irreducible ordinary character χ associated with b such that χ has height zero. [Hint: Proceed as in the proof of Corollary 46.16, by applying (b) to the permutation KG-module $K[G/Q]$.]

Notes on Section 46

The main result giving the number of blocks with defect group P as the rank of a suitable matrix is due to Robinson [1983], who proved the strong version of the theorem hinted at in Remark 46.18. The approach using bilinear forms is due to Broué and Robinson [1986] and all the results of this section are taken from their paper. A detailed discussion of the facts mentioned in Remark 46.18, as well as some interesting applications of bilinear forms to the theory of Scott modules can also be found in the Broué–Robinson paper. Another approach of Robinson's result appears in Külshammer [1984].

CHAPTER 7

Local categories and nilpotent blocks

In this chapter the poset of local pointed groups on a block algebra is made into a category, and the notion of control of fusion is developed. We prove Alperin's fusion theorem, which describes arbitrary fusions in terms of automorphisms of essential local pointed groups. The first case of control occurs when a defect group controls fusion, leading to the concept of nilpotent block. We prove one of the main results of this book: the determination of a source algebra of a nilpotent block. This allows us to compute the generalized decomposition numbers of such a block and describe the values of the ordinary characters of the block.

§ 47 LOCAL CATEGORIES

In order to deal with the problems of fusion, it is convenient to organize the local pointed groups associated with a block b into a category: the Puig category of b. This is analogous to the Frobenius category and the Brauer category, made of p-subgroups and Brauer pairs respectively. We show that the Puig category can be determined (up to equivalence) by a source algebra of the block.

The *Frobenius category* $\mathcal{F}(G)$ of G is the category whose objects are the p-subgroups of G and whose set of morphisms from Q to P is the set of all group homomorphisms $Q \to P$ induced by conjugation by some element $g \in G$ (which must therefore satisfy ${}^gQ \leq P$). Note that any such morphism is an injective map. We write $\mathrm{Hom}_G(Q,P)$ for this set of morphisms. Since any element of $C_G(Q)$ induces the trivial automorphism of Q (and similarly with P), we have

$$\begin{aligned} &\mathrm{Hom}_G(Q,P) = C_G(P)\backslash T_G(Q,P)/C_G(Q) \\ &\text{where} \quad T_G(Q,P) = \{\, g \in G \mid {}^gQ \leq P \,\}\,. \end{aligned}$$

In fact $\mathrm{Hom}_G(Q,P) = T_G(Q,P)/C_G(Q)$ because $C_G(P)$ acts trivially on $T_G(Q,P)/C_G(Q)$. Indeed if $c \in C_G(P)$ and $g \in T_G(Q,P)$, then we have ${}^{g^{-1}}c \in C_G({}^{g^{-1}}P) \leq C_G(Q)$ (because $Q \leq {}^{g^{-1}}P$) and therefore $cgC_G(Q) = g({}^{g^{-1}}c)C_G(Q) = gC_G(Q)$. In particular any endomorphism of the object Q is an automorphism and $\mathrm{Aut}_G(Q) = N_G(Q)/C_G(Q)$.

The Frobenius category is a convenient tool for the p-local analysis in finite group theory. In analogy we define the *Puig category* $\mathcal{L}_G(A)$ of an interior G-algebra A to be the category whose objects are the local pointed groups on A and whose set of morphisms from Q_δ to P_γ is the set of all group homomorphisms $\phi : Q \to P$ such that there exists $g \in G$ satisfying ${}^g(Q_\delta) \leq P_\gamma$ and $\phi(u) = {}^gu$ for all $u \in Q$. Again ϕ is necessarily injective. We write $\mathrm{Hom}_G(Q_\delta, P_\gamma)$ for this set of morphisms. Moreover any element of $C_G(Q)$ induces the trivial automorphism of Q and fixes the point δ (because A is interior so that $C_G(Q)$ maps to A^Q). Thus we have

$$\begin{aligned} &\mathrm{Hom}_G(Q_\delta,P_\gamma) = C_G(P)\backslash T_G(Q_\delta,P_\gamma)/C_G(Q) \\ &\text{where} \quad T_G(Q_\delta,P_\gamma) = \{\, g \in G \mid {}^g(Q_\delta) \leq P_\gamma \,\}\,. \end{aligned}$$

Again $\mathrm{Hom}_G(Q_\delta,P_\gamma) = T_G(Q_\delta,P_\gamma)/C_G(Q)$ because $C_G(P)$ acts trivially on $T_G(Q_\delta,P_\gamma)/C_G(Q)$. In particular

$$\mathrm{End}_G(Q_\delta) = \mathrm{Aut}_G(Q_\delta) = N_G(Q_\delta)/C_G(Q)\,.$$

We shall be particularly interested in the Puig category of a block b, which we denote by $\mathcal{L}_G(b)$ instead of $\mathcal{L}_G(\mathcal{O}Gb)$ for simplicity. By Proposition 37.2, the Puig category of $\mathcal{O}G$ is the disjoint union of the Puig categories $\mathcal{L}_G(b)$, where b runs over the blocks of $\mathcal{O}G$.

Finally there is the *Brauer category* $\mathcal{B}_G(b)$ of a block b of $\mathcal{O}G$, whose objects are the Brauer pairs associated with b and whose set of morphisms from (Q,f) to (P,e) is the set of all group homomorphisms $\phi : Q \to P$ such that there exists $g \in G$ satisfying ${}^g(Q,f) \leq (P,e)$ and $\phi(u) = {}^g u$ for all $u \in Q$. Again ϕ is necessarily injective. We write $\mathrm{Hom}_G((Q,f),(P,e))$ for this set of morphisms and we have

$$\begin{aligned}\mathrm{Hom}_G\big((Q,f),(P,e)\big) &= C_G(P)\backslash T_G\big((Q,f),(P,e)\big)/C_G(Q) \\ &= T_G\big((Q,f),(P,e)\big)/C_G(Q)\,,\end{aligned}$$

where $T_G\big((Q,f),(P,e)\big) = \{\, g \in G \mid {}^g(Q,f) \leq (P,e)\,\}$. In particular we have $\mathrm{End}_G(Q,f) = \mathrm{Aut}_G(Q,f) = N_G(Q,f)/C_G(Q)$. The Brauer category is a generalization of the Frobenius category, because by Brauer's third main Theorem 40.17, the Brauer category of the principal block of $\mathcal{O}G$ is isomorphic to the Frobenius category of G. For this reason, we shall only work with the Puig category and the Brauer category.

Our first observation is that a naturally defined subcategory is in fact equivalent to the whole category. Let A be an interior G-algebra and assume that A is primitive, so that all maximal local pointed groups on A are conjugate (they are the defects of A). If P_γ denotes a defect of A, we define $\mathcal{L}_G(A)_{\leq P_\gamma}$ to be the full subcategory of $\mathcal{L}_G(A)$ whose objects Q_δ satisfy $Q_\delta \leq P_\gamma$. Recall that the word "full" means by definition that, if $Q_\delta, R_\varepsilon \leq P_\gamma$, the whole set $\mathrm{Hom}_G(Q_\delta, R_\varepsilon)$ is the set of morphisms in $\mathcal{L}_G(A)_{\leq P_\gamma}$.

(47.1) LEMMA. *Let A be a primitive interior G-algebra and let P_γ be a defect of A. Then the inclusion functor $\mathcal{L}_G(A)_{\leq P_\gamma} \to \mathcal{L}_G(A)$ is an equivalence of categories.*

Proof. By a standard result of category theory (see Mac Lane [1971, § IV.4]), it suffices to prove that the inclusion functor is full and faithful, and that any object of $\mathcal{L}_G(A)$ is isomorphic to an object of the subcategory. Any inclusion functor from a full subcategory is always full and faithful. Now if Q_δ is an object of $\mathcal{L}_G(A)$, then Q_δ is contained in a conjugate of P_γ, because all maximal local pointed groups on A are conjugate. Therefore a conjugate of Q_δ is contained in P_γ, hence lies in $\mathcal{L}_G(A)_{\leq P_\gamma}$. Clearly a conjugate of Q_δ is isomorphic to Q_δ in the Puig category. □

If b is a block of $\mathcal{O}G$, the subcategory $\mathcal{B}_G(b)_{\leq(P,e)}$ is defined similarly when (P,e) is a maximal Brauer pair and one can prove in the same way that the inclusion functor $\mathcal{B}_G(b)_{\leq(P,e)} \to \mathcal{B}_G(b)$ is an equivalence of categories.

The relevance of the various categories we have defined will become clear in the next two sections. In the rest of this section, we are going to prove that the Puig category of a block b deserves to be called "local", in the sense that it can be determined (up to equivalence) from a source algebra of b. This is not at all clear since the morphisms of $\mathcal{L}_G(b)$ are induced by elements of G, while G is not present in the source algebra. To this end, we need to introduce another category which behaves well with respect to source algebras. Then the crucial result will be that both categories coincide for a block algebra $\mathcal{O}Gb$, and consequently we shall be able to deduce the main result.

This new category can be defined for any interior G-algebra A. An element $g \in G$ induces an inner automorphism $\mathrm{Inn}(g{\cdot}1_A)$ and, in the definition of the Puig category $\mathcal{L}_G(A)$, we have $g \in T_G(Q_\delta, P_\gamma)$ if and only if $\mathrm{Inn}(g{\cdot}1_A)$ maps δ to a point of $A^{{}^gQ}$ contained in P_γ. We can consider more generally inner automorphisms defined by arbitrary elements of A^*, and this yields a larger category $\mathcal{L}_{A^*}(A)$ defined as follows. The objects are again the local pointed groups on A and the set of morphisms from Q_δ to P_γ is the set of all injective group homomorphisms $\phi : Q \to P$ such that, choosing $i \in \gamma$ and $j \in \delta$, there exists $a \in A^*$ (depending on i and j) satisfying the following three conditions.

(a) $\phi(u)\cdot {}^aj = {}^aj\cdot\phi(u)$ for all $u \in Q$.
(b) ${}^a(u\cdot j) = \phi(u)\cdot {}^aj$ for all $u \in Q$.
(c) ${}^aj = i\,{}^aji$.

We write $\mathrm{Hom}_{A^*}(Q_\delta, P_\gamma)$ for the set of morphisms from Q_δ to P_γ in the category $\mathcal{L}_{A^*}(A)$. We shall see later that $\mathcal{L}_G(A)$ is indeed a subcategory of $\mathcal{L}_{A^*}(A)$.

We first mention that this definition is independent of the choice of i and j. If i is replaced by $i' = {}^bi$ for some $b \in (A^P)^*$ and j is replaced by $j' = {}^cj$ for some $c \in (A^Q)^*$, then we replace a by $a' = bac^{-1}$. It is easy to see that the three conditions are satisfied by i', j', and a' (Exercise 47.1).

We comment the conditions of the definition. Note first that we have ${}^aj \in A^{\phi(Q)}$ by (a) and that ${}^ajA\,{}^aj$ can be given an interior Q-algebra structure by restriction along ϕ (written $\mathrm{Res}_\phi({}^ajA\,{}^aj)$): for this structure, $u \in Q$ is mapped to $\phi(u)\cdot {}^aj \in {}^ajA\,{}^aj$. Now conjugation by a yields an isomorphism between jAj and ${}^ajA\,{}^aj$, and condition (b) means that $\mathrm{Conj}(a) : jAj \to \mathrm{Res}_\phi({}^ajA\,{}^aj)$ is an isomorphism of interior Q-algebras. In particular ${}^aj$ is a primitive idempotent of $A^{\phi(Q)}$ so that ${}^a\delta$ is a point of $A^{\phi(Q)}$. Finally the third condition means that ${}^a j$ appears in a decomposition of i in $A^{\phi(Q)}$, or in other words that $\phi(Q)_{{}^a\delta} \leq P_\gamma$. As a last comment, we note that condition (b) implies the injectivity of the map $Q{\cdot}j \to P{\cdot}i$ induced by ϕ (given explicitly by $u{\cdot}j \mapsto \phi(u){\cdot}\,{}^a j$), but not the injectivity of ϕ itself (unless Q maps injectively into jAj). This is why the injectivity of ϕ is required in the definition.

It is easy to check that $\mathcal{L}_{A^*}(A)$ is a category. For instance let Q_δ, P_γ, and R_ε be local pointed groups on A and choose $j \in \delta$ and $i \in \gamma$. Let ϕ be a morphism from Q_δ to P_γ and let $a \in A^*$ satisfying the conditions of the definition (with respect to j and i); similarly let ψ be a morphism from P_γ to R_ε and let $b \in A^*$ satisfying the conditions of the definition (with respect to i and some idempotent in ε). Then the element ba satisfies the conditions for the morphism $\psi\phi$. Indeed, for all $u \in Q$, we have

$$\begin{aligned}\psi\phi(u){\cdot}\,{}^{ba}j &= \psi\phi(u){\cdot}\,{}^{b}(i\,{}^{a}j) = (\psi\phi(u){\cdot}\,{}^{b}i)\,{}^{ba}j = {}^{b}(\phi(u){\cdot}i)\,{}^{ba}j \\ &= {}^{b}(\phi(u){\cdot}\,{}^{a}j) = {}^{ba}(u{\cdot}j)\,,\end{aligned}$$

and the other conditions are verified in a similar fashion (Exercise 47.1).

As in the case of the Puig category or the Brauer category, every morphism ϕ is in fact the composition of an isomorphism followed by an inclusion. Indeed we have noticed above that ${}^a\delta$ is a point of $A^{\phi(Q)}$ and it is clear that $\phi : Q_\delta \to \phi(Q)_{{}^a\delta}$ is an isomorphism in the category $\mathcal{L}_{A^*}(A)$, because the same element a satisfies the conditions of the definition (with respect to $j \in \delta$ and ${}^a j \in {}^a\delta$). Then the inclusion map $\phi(Q) \to P$ is a morphism $\phi(Q)_{{}^a\delta} \to P_\gamma$ in the category $\mathcal{L}_{A^*}(A)$, because ${}^a j$ appears in a decomposition of $\mathrm{Res}^P_{\phi(Q)}(i)$ so that the element 1_A satisfies the conditions of the definition (with respect to ${}^a j \in {}^a\delta$ and $i \in \gamma$). Note that when ϕ is an isomorphism, condition (c) in the definition says that ${}^a j = i$, and then condition (b) asserts that ${}^a(u{\cdot}j) = \phi(u){\cdot}i$ for all $u \in Q$.

(47.2) REMARK. Any endomorphism ϕ of Q_δ is an automorphism, and in that case ${}^a j = j$ so that a commutes with j. Thus we have $a = jaj + (1_A - j)a(1_A - j)$ and the element $b = jaj = aj = ja$ is invertible in the localization $A_\delta = jAj$. Moreover condition (b) implies that ${}^b(u{\cdot}j) = \phi(u){\cdot}j$ for all $u \in Q$. Thus ϕ is also an automorphism of Q_δ, viewed as a pointed group on A_δ, hence as an object of $\mathcal{L}_{A_\delta^*}(A_\delta)$. Conversely if ϕ is an automorphism of Q_δ in $\mathcal{L}_{A_\delta^*}(A_\delta)$, then there exists $b \in (jAj)^*$ satisfying the above property. Then $a = b + (1_A - j)$ is invertible in A, commutes with j, and satisfies ${}^a(u{\cdot}j) = \phi(u){\cdot}j$ for all $u \in Q$. Thus we have proved that

$$\mathrm{Aut}_{A^*}(Q_\delta) = \mathrm{Aut}_{A_\delta^*}(Q_\delta)\,.$$

Moreover any ϕ in the right hand side determines $b \in N_{A_\delta}(Q)$ satisfying the above property, and b is unique up to multiplication by $(A_\delta^Q)^*$. Here $N_{A_\delta}(Q)$ denotes the normalizer of $Q{\cdot}1_{A_\delta}$ in A_δ^*, that is, the set of all $c \in A_\delta^*$ such that $c{\cdot}Q{\cdot}c^{-1} \subseteq Q{\cdot}1_{A_\delta}$. Thus there is a canonical group homomorphism

$$\tau : \mathrm{Aut}_{A^*}(Q_\delta) = \mathrm{Aut}_{A_\delta^*}(Q_\delta) \longrightarrow N_{A_\delta}(Q)/(A_\delta^Q)^* .$$

Clearly $N_{A_\delta}(Q)/(A_\delta^Q)^*$ is isomorphic to a group of automorphisms of the group $Q{\cdot}1_{A_\delta}$. In case Q maps injectively into A_δ^* (for instance for a block algebra, by Proposition 38.7), it is easy to see that τ is an isomorphism (Exercise 47.4).

It may be surprising to generalize the condition $\phi(u) = {}^g u$ in the definition of $\mathcal{L}_G(A)$ by condition (b) in the definition of $\mathcal{L}_{A^*}(A)$, since one might expect the stronger requirement $\phi(u){\cdot}1_A = {}^a(u{\cdot}1_A)$. The point is that this definition is well adapted to localization, as in Remark 47.2 above. This is also crucial in the following equivalent characterization of morphisms.

(47.3) PROPOSITION. *Let Q_δ and P_γ be two local pointed groups on an interior G-algebra A, with associated embeddings $\mathcal{F}_\delta : A_\delta \to \mathrm{Res}_Q^G(A)$ and $\mathcal{F}_\gamma : A_\gamma \to \mathrm{Res}_P^G(A)$. Let $\phi : Q \to P$ be an injective group homomorphism. The following conditions are equivalent.*
(a) $\phi \in \mathrm{Hom}_{A^*}(Q_\delta, P_\gamma)$.
(b) There exists an exomorphism $\mathcal{H}_\phi : A_\delta \to \mathrm{Res}_\phi(A_\gamma)$ of interior Q-algebras such that $\mathrm{Res}_1^Q(\mathcal{F}_\delta) = \mathrm{Res}_1^P(\mathcal{F}_\gamma)\,\mathrm{Res}_1^Q(\mathcal{H}_\phi)$.
Moreover if these conditions are satisfied, then the exomorphism $\mathcal{H}_\phi$ is an embedding and is unique.

Proof. Let $i \in \gamma$ and $j \in \delta$. Since $\mathcal{F}_\gamma : A_\gamma \to \mathrm{Res}_P^G(A)$ is unique up to a unique exo-isomorphism (Lemma 13.1), we can assume that $A_\gamma = iAi$ and that $\mathcal{F}_\gamma$ is the exomorphism containing the inclusion $f_i : iAi \to \mathrm{Res}_P^G(A)$. Similarly we assume that $A_\delta = jAj$ and that $\mathcal{F}_\delta$ is the exomorphism containing the inclusion $f_j : jAj \to \mathrm{Res}_Q^G(A)$.

Suppose that (a) holds. Then there exists $a \in A^*$ satisfying the three conditions in the definition of morphisms. The third condition says that ${}^a j$ belongs to iAi, so that ${}^a jA\,{}^a j \subseteq iAi$. Let $h : jAj \to iAi$ be the homomorphism of $\mathcal{O}$-algebras defined to be the composite

$$jAj \xrightarrow{\mathrm{Conj}(a)} {}^a jA\,{}^a j \longrightarrow iAi ,$$

where the second map is the inclusion. The first two conditions then assert that h is a homomorphism of interior Q-algebras, provided iAi is endowed with the interior Q-algebra structure obtained by restriction along ϕ. If $\mathcal{H}_\phi$ denotes the exomorphism containing h, we note for later use that $\mathcal{H}_\phi$ is an embedding, because the image of h is the whole of ${}^a jA\,{}^a j$ by construction. Finally as homomorphism of $\mathcal{O}$-algebras (that is, on restriction to the trivial subgroup), the composite

$$jAj \xrightarrow{h} iAi \xrightarrow{f_i} A$$

is equal to the inclusion $f_j : jAj \to A$ followed by the inner automorphism $\mathrm{Inn}(a)$, so that $f_i h$ and f_j belong to the same exomorphism. Therefore $\mathrm{Res}_1^Q(\mathcal{F}_\delta) = \mathrm{Res}_1^P(\mathcal{F}_\gamma)\,\mathrm{Res}_1^Q(\mathcal{H}_\phi)$.

Assume conversely that $\mathcal{H}_\phi$ exists and let $h \in \mathcal{H}_\phi$. The property of $\mathcal{H}_\phi$ implies the existence of $a \in A^*$ such that $f_i h = \mathrm{Inn}(a) f_j$. This means that $h(b) = {}^a b$ for all $b \in jAj$. We prove that a, i, and j satisfy the three conditions in the definition of morphisms. Since h is a homomorphism of interior Q-algebras, we have for all $u \in Q$

$${}^a(u{\cdot}j) = h(u{\cdot}j) = \phi(u){\cdot}h(j) = \phi(u){\cdot}\,{}^a j\,,$$

proving the first condition. Similary $h(j{\cdot}u) = {}^a j{\cdot}\phi(u)$, and so ${}^a j$ commutes with $\phi(u)$ because j commutes with u, proving the second condition. Finally $h(j) = {}^a j$ belongs to iAi, so that $i\,{}^a j i = {}^a j$. This completes the proof that ϕ is a morphism in the category $\mathcal{L}_{A^*}(A)$.

To prove the additional statement, we first note that the exomorphism $\mathcal{H}_\phi$ constructed above is an embedding, so that it suffices to prove uniqueness. Let $\mathcal{H}'_\phi : A_\delta \to \mathrm{Res}_\phi(A_\gamma)$ be another exomorphism of interior Q-algebras such that

$$\mathrm{Res}_1^Q(\mathcal{F}_\delta) = \mathrm{Res}_1^P(\mathcal{F}_\gamma)\,\mathrm{Res}_1^Q(\mathcal{H}'_\phi)\,.$$

Then we have $\mathrm{Res}_1^P(\mathcal{F}_\gamma)\,\mathrm{Res}_1^Q(\mathcal{H}_\phi) = \mathrm{Res}_1^P(\mathcal{F}_\gamma)\,\mathrm{Res}_1^Q(\mathcal{H}'_\phi)$ and therefore $\mathrm{Res}_1^Q(\mathcal{H}_\phi) = \mathrm{Res}_1^Q(\mathcal{H}'_\phi)$ by Proposition 12.2, because $\mathcal{F}_\gamma$ is an embedding. Finally Proposition 12.1 implies that $\mathcal{H}_\phi = \mathcal{H}'_\phi$. □

Note that if the embedding $\mathcal{H}_\phi$ corresponds to the morphism ϕ, the image $\mathcal{H}_\phi(\delta)$ is the point of $A^{\phi(Q)}$ previously written ${}^a\delta$ (where $a \in A^*$ satisfies the conditions of the definition of morphisms). This is because $\mathcal{H}_\phi$ is by construction the exomorphism containing conjugation by a. Note also that the non-uniqueness of a in the definition is now incorporated in the exomorphism $\mathcal{H}_\phi$ and we have the much better condition that $\mathcal{H}_\phi$ is unique. Finally we remark that, for interior G-algebras, Proposition 12.1 allows us to replace an equality of restricted exomorphisms by the equality of the exomorphisms themselves (and this has been used at the end of the proof above), but this cannot be used in the statement of Proposition 47.3 because $\mathrm{Res}_Q^G(A)$ and $\mathrm{Res}_\phi \mathrm{Res}_P^G(A)$ are in general two *distinct* interior Q-algebras structures. However, Proposition 12.1 can be used when ϕ is trivial, as in the following result.

(47.4) COROLLARY. *Let Q_δ and $Q_{\delta'}$ be two local points on an interior G-algebra A. If the identity group homomorphism $id_Q : Q \to Q$ is a morphism from Q_δ to $Q_{\delta'}$ in the category $\mathcal{L}_{A^*}(A)$, then $\delta = \delta'$ and the morphism is the identity in the category $\mathcal{L}_{A^*}(A)$.*

Proof. By the proposition, there exists an exomorphism of Q-algebras $\mathcal{H} : A_\delta \to A_{\delta'}$ such that $\mathrm{Res}^Q_1(\mathcal{F}_\delta) = \mathrm{Res}^Q_1(\mathcal{F}_{\delta'})\,\mathrm{Res}^Q_1(\mathcal{H})$. Since $\mathrm{Res}^G_Q(A)$ coincides with $\mathrm{Res}_{id_Q}\mathrm{Res}^G_P(A)$, we can apply Proposition 12.1 and it follows that $\mathcal{F}_\delta = \mathcal{F}_{\delta'}\mathcal{H}$ (because A is interior). Now by Proposition 13.6, this property is equivalent to the containment relation $Q_\delta \leq Q_{\delta'}$, which is only possible if $\delta = \delta'$. □

We now show that the previous category $\mathcal{L}_G(A)$ is indeed contained in the new one $\mathcal{L}_{A^*}(A)$. Moreover we give a condition for a morphism in the larger category to lie in the small one.

(47.5) LEMMA. *Let P_γ and Q_δ be local pointed groups on an interior G-algebra A.*

(a) $\mathrm{Hom}_G(Q_\delta, P_\gamma) \subseteq \mathrm{Hom}_{A^*}(Q_\delta, P_\gamma)$.

(b) Let $\phi : Q \to P$ be a homomorphism such that $\phi \in \mathrm{Hom}_{A^*}(Q_\delta, P_\gamma)$. If there exists $g \in G$ such that $\phi(u) = {}^g u$ for all $u \in Q$ (that is, ϕ is a morphism in the Frobenius category, without any reference to points), then $\phi \in \mathrm{Hom}_G(Q_\delta, P_\gamma)$.

Proof. (a) We use the direct definition rather than the characterization of the previous proposition. Let $\phi \in \mathrm{Hom}_G(Q_\delta, P_\gamma)$ be represented by $g \in T_G(Q_\delta, P_\gamma)$. We can choose $i \in \gamma$ and $j \in \delta$ such that ${}^g j = i\,{}^g j i$ (because ${}^g(Q_\delta) \leq P_\gamma$) and the condition $\phi(u) = {}^g u$ certainly implies that ${}^g(u{\cdot}j) = \phi(u){\cdot}{}^g j = {}^g j{\cdot}\phi(u)$ for all $u \in Q$. Therefore the element $a = g{\cdot}1_A$ satisfies the conditions of the definition of morphisms in the category $\mathcal{L}_{A^*}(A)$, and so $\phi \in \mathrm{Hom}_{A^*}(Q_\delta, P_\gamma)$.

(b) Let $\mathcal{H}_\phi$ be the embedding corresponding to the morphism ϕ (Proposition 47.3). We have already noted that ϕ is the composition of an isomorphism $Q_\delta \to \phi(Q)_{\mathcal{H}_\phi(\delta)}$ followed by the inclusion $\phi(Q)_{\mathcal{H}_\phi(\delta)} \to P_\gamma$. Since the inclusion is a morphism in the category $\mathcal{L}_G(A)$, it suffices to show that the isomorphism lies in $\mathcal{L}_G(A)$. Thus we assume from now on that ϕ is an isomorphism, so that $P = \phi(Q)$.

By assumption ϕ is induced by $g \in T_G(Q, P)$, and this implies that $P = {}^g Q$. Let $\delta' = {}^{g^{-1}}\gamma$, a point of A^Q. Then conjugation by g^{-1} is an isomorphism $\psi : P_\gamma \to Q_{\delta'}$ in the category $\mathcal{L}_G(A)$. Thus $\psi \in \mathcal{L}_{A^*}(A)$ by part (a), and so $\psi\phi : Q_\delta \to Q_{\delta'}$ is a morphism in $\mathcal{L}_{A^*}(A)$. Since ϕ is conjugation by g and ψ is conjugation by g^{-1}, the composite is the identity as a group homomorphism. By Corollary 47.4, $\delta = \delta'$ and $\psi\phi$ is the identity morphism in $\mathcal{L}_{A^*}(A)$. Therefore $\phi = \psi^{-1}$ is a morphism in $\mathcal{L}_G(A)$. □

For the group of automorphisms of Q_δ, there is the canonical group homomorphism τ mentioned in Remark 47.2. Since $\mathcal{L}_G(A)$ is a subcategory of $\mathcal{L}_{A^*}(A)$, we can restrict τ to $\mathrm{Aut}_G(Q_\delta) \cong N_G(Q_\delta)/C_G(Q)$ and obtain a group homomorphism

$$N_G(Q_\delta)/C_G(Q) \longrightarrow N_{A_\delta}(Q)/(A_\delta^Q)^* .$$

It is easy to see that this coincides with the homomorphism defined in 45.3 (Exercise 47.4).

We now prove that the category $\mathcal{L}_{A^*}(A)$ behaves well with respect to embeddings. This was already indicated in a special case in Remark 47.2.

(47.6) PROPOSITION. *Let $\mathcal{F} : A \to B$ be an embedding of interior G-algebras, let Q_δ and P_γ be two local pointed groups on A, and let $Q_{\delta'}$ and $P_{\gamma'}$ be their images under $\mathcal{F}$. Then*

$$\mathrm{Hom}_{A^*}(Q_\delta, P_\gamma) = \mathrm{Hom}_{B^*}(Q_{\delta'}, P_{\gamma'}) .$$

Proof. Let $\mathcal{F}_\delta : A_\delta \to \mathrm{Res}_Q^G(A)$ and $\mathcal{F}_\gamma : A_\gamma \to \mathrm{Res}_P^G(A)$ be embeddings associated with δ and γ respectively. Since $\mathcal{F}$ is an embedding, the composite

$$\mathrm{Res}_Q^G(\mathcal{F})\mathcal{F}_\delta : A_\delta \longrightarrow \mathrm{Res}_P^G(B)$$

is an embedding associated with $Q_{\delta'}$, so that we can choose $B_{\delta'} = A_\delta$ and $\mathcal{F}_{\delta'} = \mathrm{Res}_Q^G(\mathcal{F})\mathcal{F}_\delta$. Similarly $B_{\gamma'} = A_\gamma$ and $\mathcal{F}_{\gamma'} = \mathrm{Res}_P^G(\mathcal{F})\mathcal{F}_\gamma$ is an embedding associated with $P_{\gamma'}$.

Let $\phi : Q \to P$ be an injective group homomorphism. Suppose that $\phi \in \mathrm{Hom}_{A^*}(Q_\delta, P_\gamma)$. Then by Proposition 47.3, there exists an exomorphism of interior Q-algebras $\mathcal{H}_\phi : A_\delta \to \mathrm{Res}_\phi(A_\gamma)$ such that

$$\mathrm{Res}_1^Q(\mathcal{F}_\delta) = \mathrm{Res}_1^P(\mathcal{F}_\gamma)\,\mathrm{Res}_1^Q(\mathcal{H}_\phi) . \tag{47.7}$$

Composing with $\mathrm{Res}_1^G(\mathcal{F})$, we obtain

$$\begin{aligned}\mathrm{Res}_1^Q(\mathcal{F}_{\delta'}) &= \mathrm{Res}_1^G(\mathcal{F})\,\mathrm{Res}_1^Q(\mathcal{F}_\delta) = \mathrm{Res}_1^G(\mathcal{F})\,\mathrm{Res}_1^P(\mathcal{F}_\gamma)\,\mathrm{Res}_1^Q(\mathcal{H}_\phi) \\ &= \mathrm{Res}_1^P(\mathcal{F}_{\gamma'})\,\mathrm{Res}_1^Q(\mathcal{H}_\phi) .\end{aligned} \tag{47.8}$$

Thus it follows from Proposition 47.3 that $\phi \in \mathrm{Hom}_{B^*}(Q_{\delta'}, P_{\gamma'})$.

Conversely assume that $\phi \in \mathrm{Hom}_{B^*}(Q_{\delta'}, P_{\gamma'})$. Then there exists an exomorphism of interior Q-algebras $\mathcal{H}_\phi : A_\delta \to \mathrm{Res}_\phi(A_\gamma)$ satisfying 47.8. Since $\mathcal{F}$ is an embedding, we can cancel $\mathrm{Res}_1^G(\mathcal{F})$ (Proposition 12.2) and deduce that 47.7 holds. Thus $\phi \in \mathrm{Hom}_{A^*}(Q_\delta, P_\gamma)$. □

We have seen in Proposition 44.2 that an element of $N_G(P)$ belongs to $N_G(P_\gamma)$ if and only if there exists $a \in A_\gamma^*$ such that $a{\cdot}u{\cdot}a^{-1} = {}^g u{\cdot}1_{A_\gamma}$ for all $u \in P$. This is in fact a special case of Proposition 47.6, applied to the embedding $\mathcal{F}_\gamma : A_\gamma \to \mathrm{Res}_P^G(A)$, the point $\{1_{A_\gamma}\}$, and its image γ. The verification is left as an exercise for the reader (Exercise 47.2).

(47.9) COROLLARY. *Let A be a primitive interior G-algebra with defect P_γ. The associated embedding $\mathcal{F}_\gamma : A_\gamma \to \mathrm{Res}_P^G(A)$ induces an equivalence of categories $\mathcal{L}_{A_\gamma^*}(A_\gamma) \to \mathcal{L}_{A^*}(A)$.*

Proof. We know that $\mathcal{F}_\gamma$ induces an isomorphism between the poset of local pointed groups on A_γ and the poset of local pointed groups on A contained in P_γ (Propositions 15.1 and 15.2). If Q_δ and R_ε are local pointed groups on A_γ, and if we denote their images in A by the same letters, we have

$$\mathrm{Hom}_{A_\gamma^*}(Q_\delta, R_\varepsilon) = \mathrm{Hom}_{A^*}(Q_\delta, R_\varepsilon)$$

by Proposition 47.6. This means that $\mathcal{F}_\gamma$ induces a full and faithful functor $\mathcal{L}_{A_\gamma^*}(A_\gamma) \to \mathcal{L}_{A^*}(A)$, with image $\mathcal{L}_{A^*}(A)_{\leq P_\gamma}$ (consisting of all objects Q_δ satisfying $Q_\delta \leq P_\gamma$). In order to prove that this functor is an equivalence, it suffices to show that any object of $\mathcal{L}_{A^*}(A)$ is isomorphic to an object of $\mathcal{L}_{A^*}(A)_{\leq P_\gamma}$ (see Mac Lane [1971, § IV.4]). But since A is primitive, the G-conjugates of P_γ are the only maximal local pointed groups on A (Corollary 18.4), and therefore any local pointed group Q_δ on A has a conjugate contained in P_γ. Clearly a G-conjugate of Q_δ is isomorphic to Q_δ in the category $\mathcal{L}_{A^*}(A)$ (in fact already in $\mathcal{L}_G(A)$). □

Now we come to the main result, which asserts that the Puig category of a block b can be determined up to equivalence from a source algebra of b. For simplicity, we write $\mathcal{L}_{(\mathcal{O}Gb)^*}(b)$ instead of $\mathcal{L}_{(\mathcal{O}Gb)^*}(\mathcal{O}Gb)$.

(47.10) THEOREM. *Let b be a block of $\mathcal{O}G$.*
(a) The categories $\mathcal{L}_G(b)$ and $\mathcal{L}_{(\mathcal{O}Gb)^*}(b)$ are equal.
(b) If the interior P-algebra $(\mathcal{O}Gb)_\gamma$ is a source algebra of b, the associated embedding $\mathcal{F}_\gamma : (\mathcal{O}Gb)_\gamma \to \mathrm{Res}_P^G(\mathcal{O}Gb)$ induces an equivalence of categories

$$\mathcal{L}_{(\mathcal{O}Gb)_\gamma^*}((\mathcal{O}Gb)_\gamma) \xrightarrow{\sim} \mathcal{L}_{(\mathcal{O}Gb)^*}(b) = \mathcal{L}_G(b)\,.$$

Proof. (b) is an immediate consequence of (a) and Corollary 47.9. In order to prove (a), we recall that any morphism in the category $\mathcal{L}_G(b)$ belongs to $\mathcal{L}_{(\mathcal{O}Gb)^*}(b)$, and we have to see that the converse holds. Since both categories are subcategories of the corresponding categories for the whole group algebra $\mathcal{O}G$, it suffices to prove the result for $\mathcal{O}G$, using also the fact that $\mathcal{L}_G(b)$ is a full subcategory of $\mathcal{L}_G(\mathcal{O}G)$. Moreover since any morphism is the composite of an isomorphism followed by an inclusion and since an inclusion belongs to $\mathcal{L}_G(\mathcal{O}G)$, it suffices to prove the result for an isomorphism.

Write $A = \mathcal{O}G$ for simplicity, let $\phi : Q_\delta \to R_\varepsilon$ be an isomorphism in $\mathcal{L}_{A^*}(A)$, and let $j \in \delta$ and $i \in \varepsilon$. By definition there exists $a \in A^*$ such that ${}^a j = i$ and ${}^a(j{\cdot}u) = {}^a(u{\cdot}j) = \phi(u){\cdot}i$ for all $u \in Q$. Since $u{\cdot}1_A$ can be identified with the element u of A, we can forget all the dots and write

$$(47.11) \qquad aj = ia \qquad \text{and} \qquad aju = \phi(u)ia \quad \text{for all } u \in Q\,.$$

In particular $iAia = iAj$.

Recall that the group algebra A has an $\mathcal{O}(G \times G)$-module structure defined by $(g,h){\cdot}b = gbh^{-1}$ (for $g,h \in G$ and $b \in A$). Since ε is a local point, we know by Proposition 38.7 that iAi is a direct summand of A as an $\mathcal{O}(R \times R)$-module and that iAi has an $(R \times R)$-invariant basis X containing i. Moreover every left R-orbit of X has cardinality $|R|$.

Multiplying on the right by a and using 47.11, we deduce that iAj is a direct summand of A as an $\mathcal{O}(R \times Q)$-module and that iAj has a basis $Y = Xa$ which is invariant under $(R \times Q)$ and contains $ia = aj$. Moreover the $(R \times Q)$-orbit of ia coincides with its left R-orbit (or with its right Q-orbit) because of 47.11 and the fact that every element of R can be written $\phi(u)$ with $u \in Q$. Thus the orbit of ia is equal to Ria ($= ajQ$) and has cardinality $|R| = |Q|$. Moreover $\mathcal{O}Ria$ is a direct summand of iAj as an $\mathcal{O}(R \times Q)$-module. We are going to describe in two different ways the $\mathcal{O}(R \times Q)$-module structure of $\mathcal{O}Ria$.

By 47.11, the subgroup $Q_\phi = \{\,(\phi(u),u) \in R \times Q \mid u \in Q\,\}$ fixes ia and has index $|Q|$ (because it has order $|Q|$). Since $|Q|$ is the cardinality of the orbit of ia, the stabilizer of ia is exactly Q_ϕ, and therefore the permutation $\mathcal{O}(R \times Q)$-module $\mathcal{O}Ria$ is isomorphic to

$$\mathcal{O}Ria \cong \mathrm{Ind}_{Q_\phi}^{R\times Q}(\mathcal{O})\,.$$

By Lemma 27.1, $\mathcal{O}Ria$ is an indecomposable $\mathcal{O}(R \times Q)$-module and has vertex Q_ϕ, because $R \times Q$ is a p-group (since Q_δ and R_ε are local pointed groups).

Now $\mathcal{O}Ria$ is a direct summand of iAj, which in turn is a direct summand of A (as $\mathcal{O}(R \times Q)$-modules). Using the basis G of A, we see that the $(R \times Q)$-orbits are the double cosets RgQ and that A decomposes as

$$A = \bigoplus_{g \in [R\backslash G/Q]} \mathcal{O}RgQ \;\cong \bigoplus_{g \in [R\backslash G/Q]} \mathrm{Ind}_{Q_g}^{R\times Q}(\mathcal{O})\,,$$

where $Q_g = \{ ({}^g u, u) \in R \times Q \mid u \in Q \cap {}^{g^{-1}}R \}$. Here g runs over representatives of double cosets, and clearly Q_g is the stabilizer of g in $R \times Q$. By Lemma 27.1 again, the summand indexed by g is an indecomposable $\mathcal{O}(R \times Q)$-module with vertex Q_g .

By the Krull–Schmidt theorem, the indecomposable summand $\mathcal{O}Ria$ must be isomorphic to one of the summands $\mathrm{Ind}_{Q_g}^{R \times Q}(\mathcal{O})$. Since all the vertices of an indecomposable module are conjugate, Q_ϕ and Q_g are conjugate in $R \times Q$. But a conjugate of Q_g has the form Q_h for some $h \in G$, because a direct computation shows that $(r,s)Q_g(r,s)^{-1} = Q_h$ where $h = rgs^{-1}$. Thus $Q_\phi = Q_h$, and in particular $Q \cap {}^{h^{-1}}R = Q$, so that ${}^{h^{-1}}R = Q$, that is, ${}^h Q = R$. Looking at the first components in the subgroup $Q_\phi = Q_h$, we have $\phi(u) = {}^h u$ for all $u \in Q$. Therefore the assumptions of Lemma 47.5 are satisfied and it follows that ϕ is a morphism in the category $\mathcal{L}_G(A)$. □

We deduce as a special case a result already hinted at twice (after Corollary 38.4 and after Proposition 44.2).

(47.12) COROLLARY. *Let b be a block of $\mathcal{O}G$ and let Q_δ be a local pointed group on $A = \mathcal{O}Gb$.*
(a) $N_G(Q_\delta)/C_G(Q) \cong N_{A_\delta}(Q)/(A_\delta^Q)^*$.
(b) $N_G(Q_\delta)/C_G(Q)$ *can be computed from a source algebra of* b .

Proof. (a) The left hand side is isomorphic to the group of automorphisms of Q_δ in the Puig category $\mathcal{L}_G(b)$, while the right hand side is isomorphic to the group of automorphisms of Q_δ in the category $\mathcal{L}_{A^*}(b)$, by Remark 47.2 and Exercise 47.4. Thus the theorem implies that these groups are isomorphic.

(b) We can assume after conjugation that $Q_\delta \leq P_\gamma$, where P_γ is a fixed defect of b , so that Q_δ is the image of a local pointed group (still written Q_δ) on the source algebra A_γ . Then A_δ is a localization of A_γ , so that the right hand side of part (a) is described within A_γ . □

Note that, by the remark following Lemma 47.5, the isomorphism of part (a) is given by the map constructed in 45.3.

Another consequence of the theorem is that, for the computation of generalized decomposition numbers from a source algebra, the ad hoc equivalence relation used in Proposition 43.10 can be replaced by the isomorphism relation in the category $\mathcal{L}_{(\mathcal{O}Gb)_\gamma^*}((\mathcal{O}Gb)_\gamma)$, in other words by suitable conjugations within $(\mathcal{O}Gb)_\gamma$. Details are left to the reader (Exercise 47.5).

(47.13) REMARK. By passing to the quotient by inner automorphisms, one can define quotient categories of $\mathcal{L}_G(A)$ and $\mathcal{L}_{A^*}(A)$. Thus the morphisms in the quotient categories are group exomorphisms rather than group homomorphisms. In particular, for the quotient of $\mathcal{L}_G(A)$, the automorphism group of an object Q_δ is the group $E_G(Q_\delta) = N_G(Q_\delta)/QC_G(Q)$ already encountered. Of course Theorem 47.10 also holds for the quotient categories. In particular this shows that, if Q_δ is a local pointed group on a block algebra $\mathcal{O}Gb$, the group $E_G(Q_\delta)$ can be computed from a source algebra of b (a result which can also be deduced from Corollary 47.12 above).

Exercises

(47.1) Let A be an interior G-algebra.

(b) Prove that the definition of morphisms $Q_\delta \to P_\gamma$ in $\mathcal{L}_{A^*}(A)$ is independent of the choice of $i \in \gamma$ and $j \in \delta$.

(b) Prove that $\mathcal{L}_{A^*}(A)$ is a category.

(47.2) Show that Proposition 44.2 is a special case of Proposition 47.6. [Hint: Apply Proposition 47.6 to the embedding $\mathcal{F}_\gamma : A_\gamma \to \mathrm{Res}^G_P(A)$, the point $\{1_{A_\gamma}\}$, and its image γ. Use also both statements of Lemma 47.5.]

(47.3) Let H be a subgroup of G, let B be an interior H-algebra, and let $A = \mathrm{Ind}^G_H(B)$. Prove that the canonical embedding $\mathcal{D}^G_H : B \to \mathrm{Res}^G_H(A)$ induces an equivalence of categories $\mathcal{L}_{B^*}(B) \to \mathcal{L}_{A^*}(A)$.

(47.4) Let Q_δ be a local pointed group on an interior G-algebra A and let $N_{A_\delta}(Q)$ be the normalizer of $Q{\cdot}1_{A_\delta}$ in A^*_δ.

(a) Prove that there is a canonical group homomorphism

$$\tau : \mathrm{Aut}_{A^*}(Q_\delta) = \mathrm{Aut}_{A^*_\delta}(Q_\delta) \longrightarrow N_{A_\delta}(Q)/(A^Q_\delta)^*$$

and that it is an isomorphism if Q maps injectively into A^*_δ. [Hint: See Remark 47.2.]

(b) Prove that the restriction of τ to $\mathrm{Aut}_G(Q_\delta) = N_G(Q_\delta)/C_G(Q)$ coincides with the canonical group homomorphism defined in 45.3.

(47.5) Let $\mathcal{O}$ be a complete discrete valuation ring of characteristic zero (satisfying Assumption 42.1) and let K be the field of fractions of $\mathcal{O}$. Let b be a block of $\mathcal{O}G$ and let $(\mathcal{O}Gb)_\gamma$ be a source algebra of b. Consider the matrix $D = (\chi(u_\delta))$, where χ runs over the set of irreducible characters of $K \otimes_{\mathcal{O}} (\mathcal{O}Gb)_\gamma$ and u_δ runs over representatives of isomorphism classes of pointed elements on $(\mathcal{O}Gb)_\gamma$. Here, an isomorphism is understood to be an isomorphism in the category $\mathcal{L}_{(\mathcal{O}Gb)_\gamma^*}((\mathcal{O}Gb)_\gamma)$. Prove that D is the generalized decomposition matrix of b. [Hint: Follow the method of Proposition 43.10, replacing the ad hoc equivalence relation used there by the isomorphism relation in the category $\mathcal{L}_{(\mathcal{O}Gb)_\gamma^*}((\mathcal{O}Gb)_\gamma)$.]

Notes on Section 47

The definition of the Frobenius category goes back to Puig's thesis [1976], and that of the Brauer category is due to Alperin and Broué [1979]. The Puig category $\mathcal{L}_G(A)$ and the category $\mathcal{L}_{A^*}(A)$ are defined in Puig [1986] (in the slightly different version using exomorphisms, as mentioned in Remark 47.13). Theorem 47.10 is due to Puig [1986].

§ 48 ALPERIN'S FUSION THEOREM

Alperin's fusion theorem asserts that all the morphisms of the Puig category of a block are in fact determined by the automorphisms of a rather small subset of objects (called essential). A similar result holds for the Brauer category (hence for the Frobenius category).

Let P_γ be a defect of a block b of $\mathcal{O}G$. Two local pointed groups $Q_\delta, R_\varepsilon \leq P_\gamma$ may be G-conjugate without being conjugate in P. In that case Q_δ and R_ε are said to "fuse" under G, and this type of phenomenon is known in general by the name of "fusion". All the information about fusion is contained in the morphisms of the category $\mathcal{L}_G(b)_{\leq P_\gamma}$. Thus an important problem of the local theory is to understand these morphisms, and Alperin's fusion theorem gives an answer to this problem.

In the case of the Frobenius category, the proof of Alperin's fusion theorem is based on the following two properties. Let Q and P be p-subgroups of G.

(a) If $Q < P$, there exists $R \leq N_G(Q)$ with $Q < R \leq P$.
(b) All maximal p-subgroups normalizing Q are conjugate in $N_G(Q)$.

It is well-known that every subgroup of a p-group is subnormal, so that (a) holds, and (b) holds because the Sylow p-subgroups of $N_G(Q)$ are conjugate. The analogous properties (a) and (b) also hold for Brauer pairs (Corollary 40.11 and Proposition 40.15). Turning now to the case of local pointed groups, we know that property (a) holds for local pointed groups on any G-algebra (Corollary 20.5). Finally property (b) holds for local pointed groups in the special case of the group algebra (or a block algebra), as we now show. We say that a pointed group P_γ *normalizes* Q_δ if $Q_\delta \leq P_\gamma$ and $P \leq N_G(Q_\delta)$.

(48.1) LEMMA. *Let Q_δ be a local pointed group on $\mathcal{O}G$.*
(a) If $Q_\delta < P_\gamma$ with P_γ local, then there exists a local pointed group R_ε normalizing Q_δ such that $Q_\delta < R_\varepsilon \leq P_\gamma$.
(b) All local pointed groups on $\mathcal{O}G$ which are maximal with respect to the property of normalizing Q_δ are conjugate under $N_G(Q_\delta)$.

Proof. (a) This is exactly Corollary 20.5.
(b) Let $N = N_G(Q_\delta)$ and let P_γ be a local pointed group normalizing Q_δ . There exists a point α of $(\mathcal{O}G)^N$ such that $P_\gamma \leq N_\alpha$ (Exercise 13.5), and so $Q_\delta \leq P_\gamma \leq N_\alpha$. But α is the unique point of $(\mathcal{O}G)^N$ such that $Q_\delta \leq N_\alpha$ because $QC_G(Q) \leq N$ (Proposition 37.7). Therefore all local pointed groups P_γ normalizing Q_δ are contained in the same pointed group N_α . Thus the maximal ones are the defects of N_α , hence are conjugate under N (Theorem 18.3). □

It will be clear in the proof of Alperin's fusion theorem that the result holds in general when the above two properties hold. For this reason we only prove the result for the Puig category of a block b of $\mathcal{O}G$. The case of the Brauer category (and therefore also the Frobenius category) is left as an exercise for the reader (Exercise 48.1).

We need some terminology and notation. If X is a finite poset, we define an equivalence relation on X as follows. Two elements $x, y \in X$ are linked by the relation if there exists a sequence $\{x_0, \ldots, x_n\}$ of elements of X such that $x_0 = x$, $x_n = y$, and, for $0 \leq i \leq n-1$, either $x_i \leq x_{i+1}$ or $x_i \geq x_{i+1}$. This clearly defines an equivalence relation on X and the equivalence classes are called the *connected components* of X . Moreover X is called *connected* if there is a single connected component, and *disconnected* otherwise. If a group G acts on X by order-preserving maps, then G permutes the connected components of X . We shall be in a situation where all maximal elements of X are in a single G-orbit, in which case the connected components of X are necessarily permuted transitively by G .

Let Q_δ be a local pointed group on $\mathcal{O}G$ and write $\mathcal{N}_{>Q_\delta}$ for the poset of local pointed groups P_γ normalizing Q_δ and such that $Q_\delta \neq P_\gamma$. We say that Q_δ is *weakly essential* if $\mathcal{N}_{>Q_\delta}$ is disconnected. In that case

$N_G(Q_\delta)$ acts transitively on the set of connected components of $\mathcal{N}_{>Q_\delta}$, because it acts transitively on the set of maximal elements (Lemma 48.1). Note that a weakly essential local pointed group Q_δ cannot be maximal, because $\mathcal{N}_{>Q_\delta}$ is empty when Q_δ is maximal.

It may happen that the normal subgroup $C_G(Q)$ already acts transitively on the set of connected components of $\mathcal{N}_{>Q_\delta}$, but we want to be able to leave that case aside because, in the Puig category, the group $C_G(Q)$ induces trivial morphisms starting from Q_δ. Thus we say that Q_δ is *essential* if $C_G(Q)$ does not act transitively on the set of connected components of $\mathcal{N}_{>Q_\delta}$ (so that in particular Q_δ is weakly essential). Note that the group $N_G(Q_\delta)/C_G(Q)$ permutes transitively the $C_G(Q)$-orbits of connected components.

If M is the stabilizer of a connected component Y, then $C_G(Q)M$ is the stabilizer of the $C_G(Q)$-orbit of connected components containing Y. Thus Q_δ is weakly essential if and only if M is a proper subgroup of $N_G(Q_\delta)$, and Q_δ is essential if and only if $C_G(Q)M$ is a proper subgroup of $N_G(Q_\delta)$. Note also that any G-conjugate of an essential local pointed group is again essential.

Similarly, if (Q,f) is a Brauer pair of G, then (Q,f) is called *weakly essential* if the poset $\mathcal{N}_{>(Q,f)}$ of Brauer pairs normalizing (Q,f) is disconnected, and (Q,f) is called *essential* if $C_G(Q)$ does not act transitively on the set of connected components of $\mathcal{N}_{>(Q,f)}$.

(48.2) REMARK. The notion of *(weakly) essential* p-subgroup Q is defined similarly using the poset of p-subgroups. In that case the stabilizer M of a connected component of $\mathcal{N}_{>Q}$ is a proper subgroup of $N_G(Q)$, and M has the property that M/Q contains a Sylow p-subgroup of $N_G(Q)/Q$ and that $(M/Q) \cap {}^g(M/Q)$ is a group of order prime to p for every $g \in N_G(Q) - M$. This is the definition of a *strongly p-embedded* subgroup of $N_G(Q)/Q$. Thus Q is weakly essential if and only if there exists a strongly p-embedded proper subgroup of $N_G(Q)/Q$. Similarly one can show that Q is essential if and only if Q is self-centralizing and there exists a strongly p-embedded proper subgroup of $N_G(Q)/QC_G(Q)$ (Exercise 48.5). The existence of strongly p-embedded proper subgroups is a rather rare phenomenon and there is a complete classification of groups which have a strongly p-embedded proper subgroup (using the classification of all finite simple groups).

Recall that our purpose is to describe the morphisms in the Puig category of a block b of $\mathcal{O}G$, or more precisely (thanks to Lemma 47.1) in the category $\mathcal{L}_G(b)_{\leq P_\gamma}$, where P_γ is a defect of b. An isomorphism $\phi : Q_\delta \to R_\varepsilon$ in the category $\mathcal{L}_G(b)_{\leq P_\gamma}$ is called *essential* if there exists an essential local pointed group L_λ with $Q_\delta \leq L_\lambda \leq P_\gamma$ and an element

$g \in N_G(L_\lambda)$ such that ϕ is induced by conjugation by g. In that case $R_\varepsilon = {}^g(Q_\delta)$ and since g normalizes L_λ, we also have ${}^g(Q_\delta) \leq L_\lambda$. We shall say that L_λ is the essential local pointed group *corresponding* to the essential isomorphism ϕ. We shall not only need essential objects, but also maximal ones. So we say similarly that an isomorphism $\phi : Q_\delta \to R_\varepsilon$ in the category $\mathcal{L}_G(b)_{\leq P_\gamma}$ is *maximal* if there exists an element $g \in N_G(P_\gamma)$ such that ϕ is induced by conjugation by g.

The last notion we need is the following. If $Q_\delta \leq P_\gamma$, we say that Q_δ is *fully normalized* in P_γ if there exists a local pointed group R_ε, maximal with respect to the property of normalizing Q_δ, such that $Q_\delta \leq R_\varepsilon \leq P_\gamma$. Clearly Q_δ is always fully normalized in some maximal local pointed group P_γ, because when R_ε is maximal with respect to the property of normalizing Q_δ, it suffices to choose P_γ containing R_ε. However, when P_γ is given in advance, the property may not hold.

Now we can state Alperin's fusion theorem, which asserts in essence that the automorphisms of essential and maximal objects suffice to determine the whole category.

(48.3) THEOREM (Alperin's fusion theorem). *Let b be a block of $\mathcal{O}G$ with defect P_γ. Any morphism in the category $\mathcal{L}_G(b)_{\leq P_\gamma}$ is a composite of an isomorphism followed by an inclusion, and the isomorphism is the composite of a sequence of isomorphisms of the following two types:*

(a) a maximal isomorphism,

(b) an essential isomorphism whose corresponding essential local pointed group is fully normalized in P_γ.

Proof. Throughout this proof, we denote all local pointed groups by capital letters P, Q, R, L, M without indices, and P denotes our fixed maximal element in the poset $\mathcal{L}_G(b)_{\leq P}$. Also $\mathcal{N}_{>Q}$ denotes the poset of local pointed groups normalizing Q and containing Q properly. Apart from the advantage of simplicity, this notation emphasizes that the proof is a formal argument which works for other posets for which $\mathcal{N}_{>Q}$ has a meaning and which satisfy properties analogous to those of Lemma 48.1.

Let $\phi : Q \to R$ be a morphism in $\mathcal{L}_G(b)_{\leq P}$ induced by conjugation by some $g \in G$. Then ϕ is the composite of $\mathrm{Conj}(g) : Q \to {}^gQ$ followed by the inclusion ${}^gQ \to R$. Thus it suffices to show that $\mathrm{Conj}(g)$ is a composite of isomorphisms of the prescribed types, when both Q and ${}^gQ$ are contained in P.

Conjugating by g^{-1}, we see that Q is contained in both P and ${}^{g^{-1}}P$. This operation allows us to work with a fixed Q and various conjugates of P containing Q. We first prove in this situation a result analogous to the statement, and we shall later use conjugation to transform it into the required result. We let $h = g^{-1}$ for simplicity of notation and we want to prove the following assertion.

(48.4) If Q is contained in both P and ${}^hP$, then $h = h_n \dots h_1$ with $h_i \in N_G(M_i)$, where M_i satisfies $Q \leq M_i \leq {}^{h_{i-1}\dots h_1}P$ (and therefore also $M_i \leq {}^{h_i \dots h_1}P$), and one of the following three conditions holds.
(a) M_i is essential and fully normalized in ${}^{h_{i-1}\dots h_1}P$.
(b) M_i is maximal (hence $M_i = {}^{h_{i-1}\dots h_1}P$).
(c) $h_i \in C_G(M_i)$ (where $C_G(M_i)$ denotes the centralizer of the p-subgroup underlying the local pointed group M_i).

In (c), we could in fact also add that M_i is weakly essential, but this will not play any role. We prove 48.4 by induction on the index $|P : Q|$ of Q (which is defined for the p-subgroups underlying the local pointed groups). We shall say that h_i is of type (a), (b), or (c) to indicate that (a), (b), or (c) is satisfied.

If $|P : Q| = 1$, then $Q = P$ and since ${}^hQ \leq P$, we have ${}^hQ = Q$. Thus $h \in N_G(Q)$ and since Q is maximal, h is of type (b), completing the proof in that case.

Assume now that $|P : Q| > 1$. By the first property of Lemma 48.1, there exist R and R' normalizing Q such that $Q < R \leq P$ and $Q < R' \leq {}^hP$. Let T be maximal in $\mathcal{N}_{>Q}$ with $R \leq T$. By the second property of Lemma 48.1, all maximal elements of $\mathcal{N}_{>Q}$ are conjugate under $N_G(Q)$. Thus R' is contained in some conjugate ${}^yT$ with $y \in N_G(Q)$.

Now T in turn is contained in some maximal local pointed group on $\mathcal{O}Gb$, which must be conjugate to P, say $T \leq {}^xP$ with $x \in G$. Since $R \leq P$ and $R \leq T \leq {}^xP$, we can apply induction (because $|P : R| < |P : Q|$ since $Q < R$). Therefore x is a product of elements $x_i \in N_G(M_i)$ as in 48.4 (each M_i containing R, hence Q).

A similar argument applies with R' instead of R as follows. Writing $h = x'yx$ (where $x' = hx^{-1}y^{-1}$ by definition), we have $R' \leq {}^yT \leq {}^{yx}P$ and $R' \leq {}^{x'yx}P$. Thus by induction x' is a product of elements of the prescribed types. Therefore we only have to find a product decomposition of y.

If Q is essential, then we are done because $y \in N_G(Q)$ is of type (a). Indeed Q is fully normalized in ${}^xP$ by construction, since $Q \leq T \leq {}^xP$ and T is maximal in $\mathcal{N}_{>Q}$.

If Q is not essential, there is a single orbit of connected components of $\mathcal{N}_{>Q}$ under the action of $C_G(Q)$, and therefore there exists $c \in C_G(Q)$ such that ${}^{cy}T$ lies in the same connected component as T. Writing $z = cy$, we have $y = c^{-1}z$, the element c^{-1} is of type (c), and z now has the property that T and ${}^zT$ lie in the same connected component. By definition of connected components, there exist local pointed groups $S_1, \dots, S_r$ and $T_0, \dots, T_r$ in $\mathcal{N}_{>Q}$ such that

$$T = T_0 \geq S_1 \leq T_1 \geq S_2 \leq \dots \leq T_{r-1} \geq S_r \leq T_r = {}^zT .$$

Recall that $T \leq {}^xP$. For $1 \leq i \leq r-1$, each T_i is contained in some maximal local pointed group on $\mathcal{O}Gb$, hence conjugate to ${}^xP$. We can choose $z_i \in G$ such that

$$T_i \leq {}^{z_i \ldots z_1 x}P \quad (1 \leq i \leq r-1).$$

Then we define $z_r = z z_1^{-1} \ldots z_{r-1}^{-1}$, so that $z = z_r \ldots z_1$. For $1 \leq i \leq r$, we have $S_i \leq T_{i-1} \leq {}^{z_{i-1} \ldots z_1 x}P$ and $S_i \leq T_i \leq {}^{z_i \ldots z_1 x}P$. Since $Q < S_i$ (because $S_i \in \mathcal{N}_{>Q}$), we can apply induction and deduce that z_i is a product of elements of the prescribed types. Therefore so is $z = z_r \ldots z_1$, completing the proof of 48.4.

Now we use conjugation to transform the decomposition of $h = g^{-1}$ described in 48.4 into a decomposition of g involving objects of $\mathcal{L}_G(b)_{\leq P}$ only. We define $L_1 = M_1$, $g_1 = h_1^{-1}$, and then

$$L_i = {}^{h_1^{-1} \ldots h_{i-1}^{-1}}(M_i), \quad g_i = (h_1^{-1} \ldots h_{i-1}^{-1}) h_i^{-1} (h_{i-1} \ldots h_1) \in N_G(L_i).$$

It is easy to see by induction that $g_i \ldots g_1 = h_1^{-1} \ldots h_i^{-1}$, so in particular $g_n \ldots g_1 = h_1^{-1} \ldots h_n^{-1} = h^{-1} = g$. The relation $Q \leq M_i \leq {}^{h_{i-1} \ldots h_1}P$ is transformed by conjugation by $g_{i-1} \ldots g_1$ into

$${}^{g_{i-1} \ldots g_1}Q \leq L_i \leq P,$$

and since $g_i \in N_G(L_i)$, we also have ${}^{g_i \ldots g_1}Q \leq L_i$.

We have decomposed the isomorphism $\mathrm{Conj}(g) : Q \to {}^gQ$ into a product of isomorphisms

$$\mathrm{Conj}(g_i) : {}^{g_{i-1} \ldots g_1}Q \longrightarrow {}^{g_i \ldots g_1}Q.$$

Both the origin and the target of this morphism are contained in L_i and g_i normalizes L_i. If h_i is of type (a), then M_i is essential, and therefore so is its conjugate L_i. Thus $\mathrm{Conj}(g_i)$ is an essential isomorphism. Moreover L_i is fully normalized in P, because M_i is fully normalized in ${}^{h_{i-1} \ldots h_1}P$. If h_i is of type (b), then M_i is maximal, and therefore so is its conjugate L_i (that is, $L_i = P$). Thus $\mathrm{Conj}(g_i)$ is a maximal isomorphism. Finally if h_i is of type (c), then $h_i \in C_G(M_i)$, and therefore $g_i \in C_G(L_i)$. In particular $g_i \in C_G({}^{g_{i-1} \ldots g_1}Q)$, and so ${}^{g_{i-1} \ldots g_1}Q = {}^{g_i \ldots g_1}Q$. In that case the automorphism $\mathrm{Conj}(g_i)$ of ${}^{g_{i-1} \ldots g_1}Q$ is the identity, by definition of the category, and therefore it can be ignored in the sequence of isomorphisms. This completes the proof. Note for completeness that in the last case just discussed, the isomorphism $\mathrm{Conj}(h_i) : {}^{h_{i-1} \ldots h_1}P \to {}^{h_i \ldots h_1}P$ may not be the identity; it is only its composition with the inclusion $M_i \to {}^{h_{i-1} \ldots h_1}P$ which yields a morphism $\mathrm{Conj}(h_i) : M_i \to {}^{h_i \ldots h_1}P$ which is equal to the inclusion. □

(48.5) REMARK. A careful analysis of the method used in the proof of Alperin's fusion theorem yields a more precise result. For each essential local pointed group $L_\lambda \geq Q_\delta$, let us choose a connected component Y of $\mathcal{N}_{>L_\lambda}$, with stabilizer $M < N_G(L_\lambda)$. The stabilizer of the $C_G(L)$-orbit of Y is the proper subgroup $C_G(L)M$ and we choose a system of representatives $\{g_i\}$ of $N_G(L_\lambda)/C_G(L)M$. This choice can be made in a G-equivariant way, by choosing for a conjugate ${}^g(L_\lambda)$ of L_λ the conjugate representatives $\{{}^g(g_i)\}$. Then the only essential isomorphisms actually needed in the decomposition of an arbitrary isomorphism are the conjugations by elements in the chosen systems of representatives. Similarly the only maximal isomorphisms actually needed are the conjugations by some fixed representatives of $N_G(P_\gamma)/C_G(P_\gamma)$. Another improvement consists in using a single maximal isomorphism in the decomposition of an arbitrary isomorphism. This can be achieved by conjugating a maximal isomorphism in order to put it in front of the sequence of isomorphisms.

Alperin's fusion theorem shows that an essential role is played by essential objects, and we now give more information about them.

(48.6) PROPOSITION. *Let b be a block of $\mathcal{O}G$, let Q_δ be a local pointed group on $\mathcal{O}Gb$, and let (Q,f) be a Brauer pair associated with b.*
(a) If Q_δ is essential, then Q_δ is self-centralizing.
(b) If (Q,f) is essential, then (Q,f) is self-centralizing.

Proof. (a) Let $H = QC_G(Q)$ and let H_β be the unique pointed group such that $Q_\delta \leq H_\beta$ (Proposition 37.7). Let $N = N_G(Q_\delta)$ and let N_α be the unique pointed group such that $Q_\delta \leq N_\alpha$. There exists $H_{\beta'}$ such that $Q_\delta \leq H_{\beta'} \leq N_\alpha$ (Exercise 13.5), and the uniqueness of β implies that $\beta' = \beta$.

Let R_ε be a maximal local pointed group such that $Q_\delta \leq R_\varepsilon \leq H_\beta$ (so that R_ε is a defect of H_β), and let P_γ be a maximal local pointed group such that $R_\varepsilon \leq P_\gamma \leq N_\alpha$ (so that P_γ is a defect of N_α). The maximal objects of $\mathcal{N}_{>Q_\delta}$ are the N-conjugates of P_γ (see Lemma 48.1). Let ${}^g(P_\gamma)$ be one of them, where $g \in N$. Since H is a normal subgroup of N, we have

$$Q_\delta = {}^g(Q_\delta) \leq {}^g(R_\varepsilon) \leq {}^g(H_\beta) = H_{{}^g\beta},$$

and therefore ${}^g\beta = \beta$ by uniqueness of β. Since all maximal local pointed groups contained in H_β are the H-conjugates of R_ε, it follows that ${}^g(R_\varepsilon) = {}^h(R_\varepsilon)$ for some $h \in H = QC_G(Q)$. But Q acts trivially on R_ε (because $Q \leq R$) and so we can choose $h \in C_G(Q)$.

Assume that Q_δ is not self-centralizing, so that $Q_\delta < R_\varepsilon$ by definition. We have to prove that Q_δ is not essential. Since ${}^g(R_\varepsilon) \in \mathcal{N}_{>Q_\delta}$, the relations

$$ {}^g(P_\gamma) \geq {}^g(R_\varepsilon) = {}^h(R_\varepsilon) \leq {}^h(P_\gamma) $$

show that ${}^g(P_\gamma)$ and ${}^h(P_\gamma)$ lie in the same connected component of $\mathcal{N}_{>Q_\delta}$. But as ${}^g(P_\gamma)$ is an arbitrary maximal element of $\mathcal{N}_{>Q_\delta}$ and $h \in C_G(Q)$, this proves that $C_G(Q)$ acts transitively on the set of connected components of $\mathcal{N}_{>Q_\delta}$, showing that Q_δ is not essential.

(b) The proof is similar. It is based on the fact that all maximal Brauer pairs centralizing (Q,f) are conjugate under $QC_G(Q)$ (Exercise 40.3), and all maximal Brauer pairs normalizing (Q,f) are conjugate under $N_G(Q,f)$ (Proposition 40.15). Details are left as an exercise for the reader. □

(48.7) COROLLARY. *Let (Q,f) be a Brauer pair of G and let Q_δ be a local pointed group on $\mathcal{O}G$ associated with (Q,f). Then Q_δ is essential if and only if (Q,f) is essential. Moreover in that case, Q_δ is the unique local pointed group associated with (Q,f), and the posets $\mathcal{N}_{>Q_\delta}$ and $\mathcal{N}_{>(Q,f)}$ are isomorphic.*

Proof. If Q_δ is essential, then it is self-centralizing. Therefore (Q,f) is self-centralizing and Q_δ is the unique local pointed group associated with (Q,f) (Proposition 41.1). Since any local pointed group $P_\gamma \geq Q_\delta$ is again self-centralizing by Corollary 41.4, it is the unique local pointed group associated with some self-centralizing Brauer pair (P,e). Clearly P_γ normalizes Q_δ if and only if (P,e) normalizes (Q,f). Therefore the posets $\mathcal{N}_{>Q_\delta}$ and $\mathcal{N}_{>(Q,f)}$ are isomorphic. Since $C_G(Q)$ does not act transitively on the connected components of $\mathcal{N}_{>Q_\delta}$, it does not act transitively on the connected components of $\mathcal{N}_{>(Q,f)}$, showing that (Q,f) is essential.

Conversely if (Q,f) is essential, then it is self-centralizing. Therefore Q_δ is self-centralizing and is the unique local pointed group associated with (Q,f). Again the posets $\mathcal{N}_{>Q_\delta}$ and $\mathcal{N}_{>(Q,f)}$ are isomorphic, showing that Q_δ is essential. □

The corollary implies that the notions of essential local pointed group and essential Brauer pair are actually the same (as for the self-centralizing property). But we have an even much better grasp of this concept, as the next result shows. The self-centralizing property of a local pointed group Q_δ is a condition of projectivity of the multiplicity module of δ (Lemma 37.8). In contrast, we show that the additional property needed for Q_δ to be essential is purely group theoretic.

(48.8) THEOREM. *Let Q_δ be a local pointed group on $\mathcal{O}G$. Then Q_δ is essential if and only if the following two conditions are satisfied:*
(a) Q_δ is self-centralizing.
(b) $N_G(Q_\delta)/QC_G(Q)$ has a strongly p-embedded proper subgroup.

Proof. Since an essential local pointed group is self-centralizing, we can assume that Q_δ is self-centralizing. We must then show that Q_δ is essential if and only if condition (b) holds.

We are interested in the left action of $C_G(Q)$ on $\mathcal{N}_{>Q_\delta}$ and we let $[R_\varepsilon]$ be the orbit of $R_\varepsilon \in \mathcal{N}_{>Q_\delta}$. The set of orbits $C_G(Q)\backslash\mathcal{N}_{>Q_\delta}$ is again a poset: the relation $[R_\varepsilon] \leq [P_\gamma]$ holds by definition if some element of the orbit $[R_\varepsilon]$ is contained in some element of the orbit $[P_\gamma]$, or equivalently if $R_\varepsilon \leq {}^cP_\gamma$ for some $c \in C_G(Q)$. It is clear that Q_δ is essential if and only if the poset $C_G(Q)\backslash\mathcal{N}_{>Q_\delta}$ is disconnected.

On the other hand we let $H = N_G(Q_\delta)$ and we consider the set

$$\mathcal{S} = \{\, S \mid QC_G(Q) < S \leq H \text{ and } S/QC_G(Q) \text{ is a } p\text{-group}\,\}.$$

Clearly $\mathcal{S}$ is a poset and is isomorphic to the poset of all non-trivial p-subgroups of $H/QC_G(Q)$. By definition, $H/QC_G(Q)$ has a strongly p-embedded proper subgroup if and only if $\mathcal{S}$ is disconnected (the strongly p-embedded subgroup being the stabilizer of a connected component, see Remark 48.2).

We are going to prove that the posets $C_G(Q)\backslash\mathcal{N}_{>Q_\delta}$ and $\mathcal{S}$ are isomorphic. Thus one poset is disconnected if and only if the other one is and the result follows immediately. We define a map

$$C_G(Q)\backslash\mathcal{N}_{>Q_\delta} \longrightarrow \mathcal{S}, \qquad [R_\varepsilon] \mapsto \widetilde{R} = RC_G(Q).$$

Since R is a p-group, it is clear that $\widetilde{R}/QC_G(Q)$ is a p-group, and $\widetilde{R} \leq H$ because R normalizes Q_δ by definition of $\mathcal{N}_{>Q_\delta}$. Morerover $\widetilde{R}$ only depends on the $C_G(Q)$-orbit of R_ε, because if $c \in C_G(Q)$, we have ${}^cR\,C_G(Q) = {}^c(RC_G(Q)) = RC_G(Q)$. In order to have a well-defined map, we must show that $\widetilde{R}/QC_G(Q)$ is non-trivial. But this is a consequence of the following property:

(48.9) If $R_\varepsilon \in \mathcal{N}_{>Q_\delta}$, then $R \cap QC_G(Q) = Q$.

This implies that $\widetilde{R}/QC_G(Q)$ is non-trivial because

$$\widetilde{R}/QC_G(Q) = RQC_G(Q)/QC_G(Q) \cong R/(R \cap QC_G(Q)) = R/Q \neq 1.$$

To prove 48.9, we note that R_ε is local and contains Q_δ which is self-centralizing. Therefore we have $R \cap C_G(Q) = C_R(Q) = Z(Q)$ by Proposition 41.3. Since R contains Q, it follows that

$$R \cap QC_G(Q) = Q(R \cap C_G(Q)) = QZ(Q) = Q\,.$$

Our next step is to show that one can recover $[R_\varepsilon]$ from $\widetilde{R}$. Recall that, by Proposition 37.7, there is a unique point $\tilde{\varepsilon}$ such that $R_\varepsilon \leq \widetilde{R}_{\tilde{\varepsilon}}$ (because $C_G(R) \leq C_G(Q)$, so that $RC_G(R) \leq \widetilde{R}$).

(48.10) If $R_\varepsilon \in \mathcal{N}_{>Q_\delta}$, then R_ε is a defect of $\widetilde{R}_{\tilde{\varepsilon}}$. Moreover every defect of $\widetilde{R}_{\tilde{\varepsilon}}$ is conjugate to R_ε under $C_G(Q)$ (and so contains Q_δ). Finally $N_H(\widetilde{R}) = N_H(R_\varepsilon)C_G(Q)$.

Indeed let P_γ be a local pointed group such that $R_\varepsilon \leq P_\gamma \leq \widetilde{R}_{\tilde{\varepsilon}}$. Then we have $P = R(P \cap QC_G(Q))$ (because $\widetilde{R} = R{\cdot}QC_G(Q)$) and therefore $P = RQ = R$ by 48.9. Thus $P_\gamma = R_\varepsilon$, showing that R_ε is maximal local in $\widetilde{R}_{\tilde{\varepsilon}}$. Now all defects of $\widetilde{R}_{\tilde{\varepsilon}}$ are conjugate under $\widetilde{R} = RC_G(Q)$, hence under $C_G(Q)$ since R normalizes R_ε. For the last assertion in 48.10, let $g \in N_H(\widetilde{R})$. We have $g \in N_H(\widetilde{R}_{\tilde{\varepsilon}})$ because $\tilde{\varepsilon}$ is the unique point such that $Q_\delta \leq \widetilde{R}_{\tilde{\varepsilon}}$ (Proposition 37.7) and g normalizes Q_δ since $g \in H$. Thus ${}^g(R_\varepsilon)$ is also maximal local in $\widetilde{R}_{\tilde{\varepsilon}}$, hence conjugate to R_ε under some $c \in C_G(Q)$. Then ${}^{c^{-1}g}(R_\varepsilon) = R_\varepsilon$, so that $g = c(c^{-1}g) \in C_G(Q)N_H(R_\varepsilon)$, as required. This completes the proof of 48.10. The last property we need is the following.

(48.11) If P_γ is maximal in $\mathcal{N}_{>Q_\delta}$, then $\widetilde{P} = PC_G(Q)$ is maximal in $\mathcal{S}$ (that is, $\widetilde{P}/QC_G(Q)$ is a Sylow p-subgroup of $H/QC_G(Q)$). Moreover every maximal element of $\mathcal{S}$ has the form $\widetilde{P}$ for some maximal element $[P_\gamma]$ of $C_G(Q)\backslash\mathcal{N}_{>Q_\delta}$.

By Proposition 37.10, p does not divide $|N_H(P_\gamma) : PC_G(P)|$. Now by 48.10, we have

$$N_H(\widetilde{P})/\widetilde{P} = N_H(P_\gamma)C_G(Q)/\widetilde{P} = N_H(P_\gamma)\widetilde{P}/\widetilde{P} \cong N_H(P_\gamma)/(\widetilde{P} \cap N_H(P_\gamma))\,.$$

This is a quotient of $N_H(P_\gamma)/PC_G(P)$ (because $PC_G(P) \leq \widetilde{P} \cap N_H(P_\gamma)$). Therefore p does not divide $|N_H(\widetilde{P})/\widetilde{P}|$, so that $\widetilde{P}/QC_G(Q)$ is a Sylow p-subgroup of its normalizer $N_H(\widetilde{P})/QC_G(Q)$. This implies that $\widetilde{P}/QC_G(Q)$ is a Sylow p-subgroup of $H/QC_G(Q)$ (because if $\widetilde{P}/QC_G(Q)$ is a proper subgroup of a p-subgroup $S/QC_G(Q)$, it is a proper subgroup of its normalizer $N_S(\widetilde{P})/QC_G(Q)$). The second statement in 48.11 follows from the fact that the maximal elements of $\mathcal{S}$, as well as the maximal elements of $C_G(Q)\backslash\mathcal{N}_{>Q_\delta}$, are conjugate under H (see Lemma 48.1).

Now we can prove that the map

$$C_G(Q)\backslash\mathcal{N}_{>Q_\delta} \longrightarrow \mathcal{S}\,, \qquad [R_\varepsilon] \mapsto \widetilde{R}$$

is an isomorphism of posets. For the injectivity, let $[R_\varepsilon]$ and $[R'_{\varepsilon'}]$ be such that $\widetilde{R} = \widetilde{R}'$. There are unique points $\tilde{\varepsilon}$ and $\tilde{\varepsilon}'$ such that $R_\varepsilon \leq \widetilde{R}_{\tilde{\varepsilon}}$ and $R'_{\varepsilon'} \leq \widetilde{R}_{\tilde{\varepsilon}'}$. We have $Q_\delta \leq \widetilde{R}_{\tilde{\varepsilon}}$ and $Q_\delta \leq \widetilde{R}_{\tilde{\varepsilon}'}$, forcing $\tilde{\varepsilon} = \tilde{\varepsilon}'$ (Proposition 37.7). Now by 48.10, R_ε and $R'_{\varepsilon'}$ are defects of $\widetilde{R}_{\tilde{\varepsilon}}$ and are $C_G(Q)$ conjugate. This proves that $[R_\varepsilon] = [R'_{\varepsilon'}]$.

To prove the surjectivity, let $S \in \mathcal{S}$. Then $S/QC_G(Q)$ is contained in a Sylow p-subgroup $\widetilde{P}/QC_G(Q)$ of $H/QC_G(Q)$. By 48.11, $\widetilde{P}$ is the image of a maximal element $[P_\gamma]$ of $C_G(Q)\backslash\mathcal{N}_{>Q_\delta}$. Let $R = S \cap P$. We have $Q < R \leq P$ and by Corollary 40.9, there is a unique Brauer pair (R,e) such that $(R,e) \leq (P,g)$, where (P,g) is the Brauer pair associated with P_γ. If (Q,f) is the Brauer pair associated with Q_δ (so that $(Q,f) < (P,g)$), then we necessarily have $(Q,f) < (R,e) \leq (P,g)$ (Exercise 40.5). Now since Q_δ is self-centralizing, so is every local pointed group containing Q_δ (Corollary 41.4), and therefore there is a unique local pointed group associated with each of the above Brauer pairs (Corollary 41.2). It follows that if R_ε is the unique local pointed group associated with (R,e), then $Q_\delta < R_\varepsilon \leq P_\gamma$. Since $S \leq \widetilde{P} = PC_G(Q)$ and $C_G(Q) \leq S$, we obtain $S = (S \cap P)C_G(Q) = RC_G(Q) = \widetilde{R}$. This proves the surjectivity.

Finally we have to prove that the bijection is an isomorphism of posets. Let $R_\varepsilon, S_\gamma \in \mathcal{N}_{>Q_\delta}$. We first note that if $R_\varepsilon \leq S_\gamma$, then obviously $\widetilde{R} \leq \widetilde{S}$. If conversely R_ε and S_γ are such that $\widetilde{R} \leq \widetilde{S}$, then the argument used in the proof of the surjectivity shows that $\widetilde{R}$ is the image of some $R'_{\varepsilon'}$ with $R'_{\varepsilon'} \leq S_\gamma$. By injectivity, we have $[R'_{\varepsilon'}] = [R_\varepsilon]$, and so $[R'_{\varepsilon'}] \leq [S_\gamma]$. This completes the proof that we have an isomorphism of posets, and the theorem follows. □

The theorem gives a very efficient characterization of essential local pointed groups in group theoretic terms, in view of the classification of groups having a strongly p-embedded subgroup (see Remark 48.2).

Exercises

(48.1) Prove Alperin's fusion theorem for the Brauer category of a block and for the Frobenius category.

(48.2) Prove the statements made in Remark 48.5.

(48.3) Prove statement (b) of Proposition 48.6.

(48.4) Let Q_δ be an essential local pointed group on $\mathcal{O}G$. Prove that if Q_δ is maximal with respect to the property of being essential, then Q_δ is fully normalized in every maximal local pointed group P_γ containing Q_δ. [Hint: Use statement 48.4.]

(48.5) Let Q be a p-subgroup of G. Prove that Q is essential if and only if Q is self-centralizing and $N_G(Q)/QC_G(Q)$ has a strongly p-embedded proper subgroup. [Hint: For a direct proof, follow the method of Theorem 48.8, using p-subgroups instead of pointed groups. Otherwise one can simply apply Theorem 48.8 to a local pointed group associated with the principal block, using the fact that the poset of self-centralizing local pointed groups is isomorphic to the corresponding poset of self-centralizing Brauer pairs, which in turn is isomorphic to the poset of self-centralizing p-subgroups by Brauer's third main theorem.]

Notes on Section 48

In the case of the Frobenius category, Alperin's fusion theorem goes back to Alperin [1967], who proved a slightly weaker version of the result. The improved version using essential objects is due to Goldschmidt [1970] and Puig [1976]. The generalization of Alperin's fusion theorem to the case of Brauer pairs is mentioned in Alperin and Broué [1979]. The case of local pointed groups is due to Puig but does not appear in print. Theorem 48.8 can be found in Puig [1976] in the case of p-subgroups. The classification of groups having a strongly p-embedded proper subgroup appears in Gorenstein and Lyons [1983] in the case of simple groups; the general case can be deduced from it and is explicitly stated in Aschbacher [1993].

§ 49 CONTROL OF FUSION AND NILPOTENT BLOCKS

In this section we define the notion of control of fusion and that of nilpotent block, obtained by requiring that a defect group controls fusion. Various properties of nilpotent blocks are discussed.

A subgroup H of a G is said to *control fusion* in G (or more precisely, to control p-fusion in G) if the inclusion $H \to G$ induces an equivalence of Frobenius categories $\mathcal{F}(H) \to \mathcal{F}(G)$.

(49.1) LEMMA. *Let H be a subgroup of G. Then H controls fusion in G if and only if the following two conditions are satisfied:*

(a) H contains a Sylow p-subgroup of G (that is, $|G:H|$ is prime to p).

(b) If Q is a p-subgroup of H and if $g \in G$ is such that ${}^gQ \leq H$, then $g = hc$ with $h \in H$ and $c \in C_G(Q)$.

Proof. Recall that $\mathcal{F}(H) \to \mathcal{F}(G)$ is an equivalence if and only if the functor is full and faithful and any object of $\mathcal{F}(G)$ is isomorphic to an object of $\mathcal{F}(H)$. The functor is always faithful because it is clear that two morphisms in $\mathcal{F}(H)$ which become equal in $\mathcal{F}(G)$ are already equal in $\mathcal{F}(H)$. The fact that any object of $\mathcal{F}(G)$ is isomorphic to an object of $\mathcal{F}(H)$ translates into condition (a), because any p-subgroup is contained in a Sylow p-subgroup P of G, so that some conjugate of every p-subgroup is contained in H if and only if some conjugate of P is contained in H. Finally the condition that $\mathcal{F}(H) \to \mathcal{F}(G)$ be full is equivalent to condition (b). Indeed let Q, R be p-subgroups of H and let $\mathrm{Conj}(g) : Q \to R$ be a morphism in $\mathcal{F}(G)$, so that ${}^gQ \leq R \leq H$. This is already a morphism in $\mathcal{F}(H)$ if and only if there exists $h \in H$ such that ${}^hQ = {}^gQ$ and $\mathrm{Conj}(g) = \mathrm{Conj}(h) : Q \to R$. This is equivalent to (b). □

We now define the analogous notion for the Puig category $\mathcal{L}_G(A)$, replacing p-subgroups by local pointed groups. In analogy with the fact that all Sylow p-subgroups are conjugate, it is natural to work only with a *primitive* G-algebra A, so that all maximal local pointed groups on A are conjugate. So let A be a primitive interior G-algebra and let H_β be a pointed group on A. By Proposition 15.1, an associated embedding $\mathcal{F}_\beta : A_\beta \to \mathrm{Res}^G_H(A)$ induces an isomorphism between the poset of local pointed groups on A_β and the poset of local pointed groups on A contained in H_β. This isomorphism commutes with the action of H and therefore $\mathcal{F}_\beta$ induces a faithful functor

$$\mathcal{L}_H(A_\beta) \longrightarrow \mathcal{L}_G(A),$$

mapping a local pointed group Q_δ on A_β to its image in A (still written Q_δ), and mapping a morphism $\mathrm{Conj}(h) : Q_\delta \to R_\varepsilon$ to the same morphism, viewed as a morphism in $\mathcal{L}_G(A)$. The image of this functor is the set of local pointed groups on A contained in H_β. A morphism is in the image of this functor if it is a conjugation by some element of H.

We now come to a first version of the definition of control of fusion. A pointed group H_β on A is said to *control fusion* in the Puig category $\mathcal{L}_G(A)$ if the functor $\mathcal{L}_H(A_\beta) \to \mathcal{L}_G(A)$ is an equivalence of categories. Again there is a description analogous to that of Lemma 49.1.

(49.2) LEMMA. *Let A be a primitive interior G-algebra, let $\alpha = \{1_A\}$ be the unique point of A^G, and let H_β be a pointed group on A. Then H_β controls fusion in $\mathcal{L}_G(A)$ if and only if the following two conditions are satisfied:*

(a) H_β contains a defect of G_α.

(b) If Q_δ is a local pointed group on A contained in H_β and if $g \in G$ is such that ${}^g(Q_\delta) \leq H_\beta$, then $g = hc$ with $h \in H$ and $c \in C_G(Q)$.

Proof. Since A is primitive, all maximal local pointed groups on A are G-conjugate (they are the defects of G_α). Therefore every object of $\mathcal{L}_G(A)$ is isomorphic to an object contained in H_β if and only if the maximal ones are conjugate to an object contained in H_β, which is condition (a). The functor $\mathcal{L}_H(A_\beta) \to \mathcal{L}_G(A)$ is always faithful and it is full precisely when condition (b) holds. This is proved in the same way as in Lemma 49.1. □

(49.3) REMARK. One obtains a slightly different definition if one replaces condition (a) by the condition $G_\alpha \, pr \, H_\beta$ (which is analogous to the requirement that $|G : H|$ is prime to p in the case of the Frobenius category). If $G_\alpha \, pr \, H_\beta$, then H_β contains a defect of G_α by Theorem 18.3. However, it is not clear whether the converse implication holds. But in all cases to be discussed here, the stronger condition $G_\alpha \, pr \, H_\beta$ will always be verified.

We have seen in Lemma 47.1 that the Puig category of a primitive interior G-algebra A can be replaced by the equivalent subcategory $\mathcal{L}_G(A)_{\leq P_\gamma}$, where P_γ is a defect of A. We now explain how control of fusion can be interpreted using this subcategory. We define another notion of control of fusion which turns out to be equivalent to the previous one.

Let H be a subgroup of G containing P. Define $\mathcal{L}_H(A)_{\leq P_\gamma}$ to be the subcategory of $\mathcal{L}_G(A)_{\leq P_\gamma}$ having the same objects (that is, all local pointed groups $Q_\delta \leq P_\gamma$), but morphisms induced by conjugations by elements of H only. We write $\mathrm{Hom}_H(Q_\delta, R_\varepsilon)$ for the set of morphisms from Q_δ to R_ε in the subcategory $\mathcal{L}_H(A)_{\leq P_\gamma}$. We say that the subgroup H *controls fusion* in $\mathcal{L}_G(A)_{\leq P_\gamma}$ if the subcategory $\mathcal{L}_H(A)_{\leq P_\gamma}$ is equal to the whole of $\mathcal{L}_G(A)_{\leq P_\gamma}$, or in other words if $\mathrm{Hom}_H(Q_\delta, R_\varepsilon) = \mathrm{Hom}_G(Q_\delta, R_\varepsilon)$ for all $Q_\delta, R_\varepsilon \leq P_\gamma$.

(49.4) LEMMA. *Let A be a primitive interior G-algebra with defect P_γ , let H be a subgroup of G containing P , and let β be any point of A^H such that $P_\gamma \leq H_\beta$.*
(a) The categories $\mathcal{L}_H(A_\beta)$ and $\mathcal{L}_H(A)_{\leq P_\gamma}$ are equivalent.
(b) H controls fusion in $\mathcal{L}_G(A)_{\leq P_\gamma}$ if and only if H_β controls fusion in $\mathcal{L}_G(A)$.

Proof. (a) By Lemma 47.1, the inclusion $\mathcal{L}_H(A_\beta)_{\leq P_\gamma} \to \mathcal{L}_H(A_\beta)$ is an equivalence. Moreover it is clear that the image of $\mathcal{L}_H(A_\beta)_{\leq P_\gamma}$ under the faithful functor $\mathcal{L}_H(A_\beta) \to \mathcal{L}_G(A)$ is equal to $\mathcal{L}_H(A)_{\leq P_\gamma}$, so that $\mathcal{L}_H(A_\beta)_{\leq P_\gamma}$ and $\mathcal{L}_H(A)_{\leq P_\gamma}$ are isomorphic.

(b) In the following commutative diagram of functors

$$\begin{array}{ccc} \mathcal{L}_H(A_\beta)_{\leq P_\gamma} & \longrightarrow & \mathcal{L}_G(A)_{\leq P_\gamma} \\ \downarrow{\simeq} & & \downarrow{\simeq} \\ \mathcal{L}_H(A_\beta) & \longrightarrow & \mathcal{L}_G(A) \end{array}$$

both vertical functors are equivalences by Lemma 47.1. Therefore the first row is an equivalence if and only if the second row is an equivalence (that is, H_β controls fusion in $\mathcal{L}_G(A)$). But we have just seen that the first row induces an isomorphism between $\mathcal{L}_H(A_\beta)_{\leq P_\gamma}$ and its image $\mathcal{L}_H(A)_{\leq P_\gamma}$. The inclusion $\mathcal{L}_H(A)_{\leq P_\gamma} \to \mathcal{L}_G(A)_{\leq P_\gamma}$ is an equivalence if and only if it is an equality (because the objects of both categories are the same), and equality means that H controls fusion in $\mathcal{L}_G(A)_{\leq P_\gamma}$. □

As a consequence of the lemma, we see that, in the first definition of control of fusion, the point β does not actually play an important role. Any point β such that $H_\beta \geq P_\gamma$ has the property of the definition if one of them does. For this reason we shall from now on use the second definition, in which only the subgroup H is involved.

Another advantage of the second definition is that it also applies to Brauer pairs. Let b be a block of $\mathcal{O}G$ and let (P,e) be a maximal Brauer pair associated with b . We define $\mathcal{B}_H(b)_{\leq (P,e)}$ to be the subcategory of $\mathcal{B}_G(b)_{\leq (P,e)}$ having the same objects, but having morphisms induced by elements of H only. If H is a subgroup containing the defect group P, then H is said to *control fusion* in $\mathcal{B}_G(b)_{\leq(P,e)}$ if the subcategory $\mathcal{B}_H(b)_{\leq(P,e)}$ is equal to the whole of $\mathcal{B}_G(b)_{\leq(P,e)}$. We now prove that this notion coincides in fact with the one defined with the Puig category of b. This is possible because, whereas the definition of control of fusion involves arbitrary morphisms of the category $\mathcal{L}_G(A)_{\leq P_\gamma}$, one can use Alperin's fusion theorem to restrict the conditions, as follows.

(49.5) PROPOSITION. *Let b be a block of $\mathcal{O}G$, let P_γ be a defect of b, and let (P,e) be the maximal Brauer pair associated with P_γ. Let H be a subgroup of G containing the defect group P. The following conditions are equivalent.*

(a) *H controls fusion in $\mathcal{L}_G(b)_{\leq P_\gamma}$.*
(b) *We have $N_G(Q_\delta) = N_H(Q_\delta)C_G(Q)$ for every local pointed group Q_δ contained in P_γ.*
(c) *We have $N_G(Q_\delta) = N_H(Q_\delta)C_G(Q)$ for every local pointed group Q_δ contained in P_γ, fully normalized in P_γ, and such that Q_δ is either essential or maximal.*
(a′) *H controls fusion in $\mathcal{B}_G(b)_{\leq(P,e)}$.*
(b′) *We have $N_G(Q,f) = N_H(Q,f)C_G(Q)$ for every Brauer pair (Q,f) contained in (P,e).*
(c′) *We have $N_G(Q,f) = N_H(Q,f)C_G(Q)$ for every Brauer pair (Q,f) contained in (P,e), fully normalized in (P,e), and such that (Q,f) is either essential or maximal.*

Proof. If H controls fusion in $\mathcal{L}_G(b)_{\leq P_\gamma}$, then

$$N_G(Q_\delta)/C_G(Q) = \mathrm{End}_G(Q_\delta) = \mathrm{End}_H(Q_\delta) = N_H(Q_\delta)/C_H(Q)\,,$$

so that $N_G(Q_\delta) = N_H(Q_\delta)C_G(Q)$. Thus (a) implies (b). It is plain that (b) implies (c).

In order to prove that (c) implies (a), we have to show that any morphism in $\mathcal{L}_G(b)_{\leq P_\gamma}$ is a conjugation by some element of H. By Alperin's fusion Theorem 48.3, any morphism in $\mathcal{L}_G(b)_{\leq P_\gamma}$ is a composite of essential isomorphisms (corresponding to essential local pointed groups which are fully normalized in P_γ), maximal isomorphisms and an inclusion. Clearly the inclusion is in $\mathcal{L}_H(b)_{\leq P_\gamma}$. Consider now an isomorphism $R_\varepsilon \to R'_{\varepsilon'}$ induced by conjugation by $g \in N_G(Q_\delta)$, where Q_δ is either essential or maximal, contains R_ε, and is fully normalized in P_γ. By assumption (c), $g = hc$ with $h \in N_H(Q_\delta)$ and $c \in C_G(Q)$. Since the origin R_ε of the isomorphism is contained in Q_δ, the element c induces the identity automorphism of R_ε. Thus the isomorphism is induced by conjugation by $h \in H$, and therefore it belongs to $\mathcal{L}_H(b)_{\leq P_\gamma}$, as required.

The proof of the equivalence of (a′), (b′) and (c′) is the same, replacing local pointed groups by Brauer pairs. Thus it suffices to prove that (c) and (c′) are equivalent. We apply Corollary 48.7. Thus Q_δ is essential if and only if it is associated with an essential Brauer pair (Q,f). In that case Q_δ is the only local pointed group associated with (Q,f), and therefore $N_G(Q,f) = N_G(Q_\delta)$. Moreover Q_δ is fully normalized in P_γ if and only if (Q,f) is fully normalized in (P,e), because the posets $\mathcal{N}_{>Q_\delta}$ and $\mathcal{N}_{>(Q,f)}$ are isomorphic. Similarly, in the maximal case, $N_G(P,e) = N_G(P_\gamma)$, because P_γ is the only local pointed group associated with (P,e). The equivalence of (c) and (c′) follows. □

It may happen in practice that one does not know what are the essential local pointed groups. But statement (b) can be verified instead, and this is why we have included it for completeness.

Having seen that there is in fact only one notion of control of fusion for blocks, we turn to an example.

(49.6) PROPOSITION. *Let b be a block of $\mathcal{O}G$ and let P_γ be a defect of b. If P is abelian, then $N_G(P_\gamma)$ controls fusion in $\mathcal{L}_G(b)_{\leq P_\gamma}$.*

Proof. Let $N = N_G(P_\gamma)$ and let β be the unique point of $(\mathcal{O}Gb)^N$ such that $P_\gamma \leq N_\beta$ (Proposition 37.7). Let Q_δ be a local pointed group on $\mathcal{O}Gb$ such that $Q_\delta \leq P_\gamma$, and let $g \in G$ be such that ${}^g(Q_\delta) \leq P_\gamma$. Thus we have $Q_\delta \leq {}^{g^{-1}}(P_\gamma)$ and in particular $Q \leq P$ and $Q \leq {}^{g^{-1}}P$.

Since P is abelian, $P \leq C_G(Q)$ and ${}^{g^{-1}}P \leq C_G(Q)$. Let α be the unique point of $(\mathcal{O}Gb)^{C_G(Q)}$ such that $Q_\delta \leq C_G(Q)_\alpha$ (which exists by Proposition 37.7 because $C_G(Q) = QC_G(Q)$). If $\alpha' \in \mathcal{P}((\mathcal{O}Gb)^{C_G(Q)})$ denotes a point such that $P_\gamma \leq C_G(Q)_{\alpha'}$ (which always exists by Exercise 13.5), then $Q_\delta \leq P_\gamma \leq C_G(Q)_{\alpha'}$, forcing $\alpha = \alpha'$. The same argument applies with ${}^{g^{-1}}(P_\gamma)$, and therefore both P_γ and ${}^{g^{-1}}(P_\gamma)$ are contained in the same pointed group $C_G(Q)_\alpha$. Since they are maximal local, they are defects of $C_G(Q)_\alpha$ and so they are conjugate under $C_G(Q)$. Thus there exists $c \in C_G(Q)$ such that ${}^{g^{-1}}(P_\gamma) = {}^c(P_\gamma)$, from which it follows that $gc \in N_G(P_\gamma) = N$. Thus $g = (gc)c^{-1} \in NC_G(Q)$, as was to be shown. □

In fact, for a block b with abelian defect group, there are no essential local pointed groups (Exercise 49.1), so that, by Alperin's fusion theorem, only the automorphisms of a maximal local pointed group P_γ are necessary to determine all morphisms of the Puig category. This provides another approach to Proposition 49.6.

Since a subgroup H controlling fusion must contain a defect group P, the first case of control occurs when $H = P$. Let us first mention the situation in the case of the Frobenius category $\mathcal{F}(G)$.

(49.7) THEOREM (Frobenius). *Let P be a Sylow p-subgroup of G. Then P controls fusion in $\mathcal{F}(G)$ if and only if G is p-nilpotent.*

Proof. If G is p-nilpotent, then it is not difficult to see that the quotient $N_G(Q)/C_G(Q)$ is a p-group for every p-subgroup Q of G (see the proof of Proposition 49.13 below). Moreover, if Q is fully normalized in some fixed Sylow p-subgroup P of G, this implies that we have $N_G(Q) = N_P(Q)C_G(Q)$. Therefore P controls fusion in $\mathcal{F}(G)$, by the analogue of Proposition 49.5 for the Frobenius category (which is in fact the special case of Proposition 49.5 for the principal block b_0 since we have $\mathcal{F}(G) \cong \mathcal{B}_G(b_0)$). If conversely P controls fusion, then $N_G(Q)/C_G(Q)$ is a p-group for every p-subgroup Q of G, and in that case a classical theorem of Frobenius asserts that G is p-nilpotent (see Exercise 50.4). □

This work of Frobenius is the motivation for giving his name to the category of p-subgroups. If G is p-nilpotent, then we shall see in Proposition 49.13 below that, for every block of $\mathcal{O}G$, we also have a similar property of control of fusion.

In analogy with the above case, a block b of $\mathcal{O}G$ with defect P_γ is said to be *nilpotent* if P controls fusion in $\mathcal{L}_G(b)_{\leq P_\gamma}$. Using the first definition of control of fusion, this is equivalent to requiring that P_γ controls fusion in $\mathcal{L}_G(b)$. This definition does not depend on the choice of the defect P_γ, because by conjugating the whole situation by g, we see that P controls fusion in $\mathcal{L}_G(b)_{\leq P_\gamma}$ if and only if ${}^gP$ controls fusion in $\mathcal{L}_G(b)_{\leq {}^g(P_\gamma)}$. We first give equivalent characterizations of nilpotent blocks.

(49.8) PROPOSITION. *Let b be a block of $\mathcal{O}G$. The following conditions are equivalent.*
(a) b is a nilpotent block.
(b) $N_G(Q_\delta)/C_G(Q)$ is a p-group for every local pointed group Q_δ associated with b.
(c) $N_G(Q,f)/C_G(Q)$ is a p-group for every Brauer pair (Q,f) associated with b.

Proof. (a) ⇒ (c). Let (P,e) be a maximal Brauer pair associated with b. Since b is nilpotent, we have $N_G(Q,f) = N_P(Q,f)C_G(Q)$ for every Brauer pair $(Q,f) \leq (P,e)$, by Proposition 49.5. This implies (c), because

$$N_G(Q,f)/C_G(Q) = N_P(Q,f)C_G(Q)/C_G(Q)$$
$$\cong N_P(Q,f)/(N_P(Q,f) \cap C_G(Q)),$$

and this is a p-group since $N_P(Q,f) \leq P$. This works if $(Q,f) \leq (P,e)$, but then (c) holds because an arbitrary (Q,f) is conjugate to a Brauer pair contained in (P,e).

(c) $\Rightarrow$ (b). Let Q_δ be a local pointed group on $\mathcal{O}Gb$ associated with the Brauer pair (Q,f). We have $N_G(Q_\delta) \leq N_G(Q,f)$, because if $g \in N_G(Q_\delta)$, then ${}^g(Q_\delta) = Q_\delta$ is associated with ${}^g(Q,f) = (Q, {}^gf)$, forcing ${}^gf = f$ since Q_δ is associated with a single block. Thus if $N_G(Q,f)/C_G(Q)$ is a p-group, so is its subgroup $N_G(Q_\delta)/C_G(Q)$.

(b) $\Rightarrow$ (a). Let P_γ be a defect of b. By Proposition 49.5, it suffices to prove that, for every local pointed group $Q_\delta \leq P_\gamma$ which is fully normalized in P_γ, we have $N_G(Q_\delta) = N_P(Q_\delta)C_G(Q)$. Let $H = N_G(Q_\delta)$ and let H_α be the unique pointed group such that $Q_\delta \leq H_\alpha$ (Proposition 37.7). Let R_ε be maximal local such that $Q_\delta \leq R_\varepsilon \leq H_\alpha$ (so that R_ε is a defect of H_α). Since Q_δ is fully normalized in P_γ, we can choose R_ε such that $R_\varepsilon \leq P_\gamma$.

Let $L = RC_G(Q)$ and $M = N_H(L)$, and let L_λ and M_μ be the unique pointed groups such that $R_\varepsilon \leq L_\lambda$ and $R_\varepsilon \leq M_\mu$ (which are unique by Proposition 37.7 because $RC_G(R) \leq RC_G(Q) = L \leq M$). By uniqueness of λ, we have $R_\varepsilon \leq L_\lambda \leq M_\mu$ (because there must be some $L_{\lambda'}$ with this property by Exercise 13.5 and so $\lambda = \lambda'$). Therefore we have

$$Q_\delta \leq R_\varepsilon \leq L_\lambda \leq M_\mu \leq H_\alpha ,$$

and R_ε is also a defect of L_λ and M_μ.

Let $g \in M$. Since M normalizes L as well as Q_δ (because M is contained in $H = N_G(Q_\delta)$), we have

$$Q_\delta = {}^g(Q_\delta) \leq {}^g(R_\varepsilon) \leq {}^g(L_\lambda) = L_{{}^g\lambda} ,$$

so that ${}^g\lambda = \lambda$ by uniqueness of λ. Since all maximal local pointed groups contained in L_λ are L-conjugate, ${}^g(R_\varepsilon) = {}^x(R_\varepsilon)$ for some $x \in L$, and therefore $x^{-1}g \in N_M(R_\varepsilon)$. This shows that $M = LN_M(R_\varepsilon)$. Therefore $M = N_M(R_\varepsilon)C_G(Q)$ (because $L = RC_G(Q) \leq N_M(R_\varepsilon)C_G(Q)$ and $C_G(Q)$ is a normal subgroup of H).

Now since R_ε is a defect of M_μ and since $RC_G(R) \leq M$, the group $N_M(R_\varepsilon)/RC_G(R)$ has order prime to p by Proposition 37.10. The image of this group in the quotient $H/C_G(Q)$ is isomorphic to M/L because $N_M(R_\varepsilon)C_G(Q) = M$ and $RC_G(R)C_G(Q) = RC_G(Q) = L$. Therefore M/L has order prime to p. But since $H/C_G(Q)$ is a p-group by assumption, we must have $M = L$. In other words the subgroup $L/C_G(Q)$ of the p-group $H/C_G(Q)$ is equal to its normalizer $M/C_G(Q)$. This forces L to be equal to H (because a proper subgroup of a p-group is a proper subgroup of its normalizer). Thus $H = RC_G(Q)$. But $R \leq P$ by the choice of R_ε, and so $H = (H \cap P)C_G(Q)$, that is, $N_G(Q_\delta) = N_P(Q_\delta)C_G(Q)$. This completes the proof that (b) implies (a). □

Since $QC_G(Q)/C_G(Q)$ is always a p-group, condition (b) in Proposition 49.8 is equivalent to the requirement that $E_G(Q_\delta) = N_G(Q_\delta)/QC_G(Q)$ be a p-group for every local pointed group Q_δ on $\mathcal{O}Gb$ (and similarly for Brauer pairs instead of local pointed groups). This implies in particular the following result.

(49.9) COROLLARY. *If P_γ is a defect of a nilpotent block b of $\mathcal{O}G$, then $N_G(P_\gamma) = PC_G(P)$. In other words $E_G(P_\gamma) = 1$.*

Proof. Let $E_G(P_\gamma) = N_G(P_\gamma)/PC_G(P)$. By assumption and Proposition 49.8, $E_G(P_\gamma)$ is a p-group. On the other hand $|E_G(P_\gamma)|$ is prime to p by Theorem 37.9. Therefore $E_G(P_\gamma) = 1$. □

We now show that nilpotent blocks appear in some of the situations already encountered.

(49.10) PROPOSITION. *Let b be a block of $\mathcal{O}G$ and suppose that $G = PC_G(P)$, where P is a defect group of b. Then b is nilpotent.*

Proof. Since $C_G(P)$ acts trivially on local pointed groups $Q_\delta \leq P_\gamma$ (where P_γ is a defect of b), the conjugation by an element of G is equal to the conjugation by an element of P. Thus P controls fusion. □

More generally, if $G = N_G(P_\gamma)$ (where P_γ is a defect of b), then b is nilpotent if and only if $E_G(P_\gamma) = 1$ (Exercise 49.2). Here we set $E_G(P_\gamma) = N_G(P_\gamma)/PC_G(P)$ as usual. In the same vein, if b is a block of $\mathcal{O}G$ with an abelian defect group P, then b is nilpotent if and only if $E_G(P_\gamma) = 1$ (Exercise 49.3).

(49.11) COROLLARY. *Any block with a central defect group is nilpotent.*

Proof. This is the special case $G = C_G(P)$ in Proposition 49.10. □

(49.12) COROLLARY. *Let b be a block of $\mathcal{O}G$ and let (Q,f) be a Brauer pair associated with b. If (Q,f) is self-centralizing, then f is a nilpotent block of $\mathcal{O}C_G(Q)$.*

Proof. By definition, f is a block of $C_G(Q)$ with defect group $Z(Q)$, which is a central subgroup of $C_G(Q)$. Thus Corollary 49.11 applies. □

Another situation where nilpotent blocks arise is the case of p-nilpotent groups.

(49.13) PROPOSITION. *Let G be a p-nilpotent group. Then every block of $\mathcal{O}G$ is nilpotent.*

Proof. By definition, G has a normal subgroup H of order prime to p and index a power of p. Let Q be a p-subgroup of G and consider $N_H(Q) = N_G(Q) \cap H$. Since Q normalizes H and $N_G(Q)$, it normalizes $N_H(Q)$. Therefore $N_H(Q)$ and Q normalize each other. Since they intersect trivially (because they have coprime orders), it follows that they centralize each other (because for $h \in N_H(Q)$ and $u \in Q$, the commutator $huh^{-1}u^{-1}$ belongs to both $N_H(Q)$ and Q, hence is trivial). Thus we have shown that $N_H(Q) \leq C_G(Q)$. Finally since G/H is a p-group, so is $N_G(Q)/N_H(Q)$, and therefore $N_G(Q)/C_G(Q)$ is a p-group. Now for any local pointed group Q_δ on $\mathcal{O}G$, the group $N_G(Q_\delta)/C_G(Q)$ is a subgroup of $N_G(Q)/C_G(Q)$, hence is a p-group. By Proposition 49.8, this implies that any block of $\mathcal{O}G$ is nilpotent. □

Note that the converse of Proposition 49.13 holds. In fact if just the principal block of G is nilpotent, then G is p-nilpotent (see Exercise 50.4). This is essentially the theorem of Frobenius mentioned earlier.

An easy but important fact is that the property of being nilpotent is inherited by Brauer pairs.

(49.14) PROPOSITION. *Let b be a block of $\mathcal{O}G$ and let (P,e) be a Brauer pair associated with b. If b is nilpotent, then e is a nilpotent block of $kC_G(P)$.*

Proof. Let (Q,f) be a Brauer pair of $C_G(P)$ associated with the block e of $C_G(P)$. Thus Q is a p-subgroup of $C_G(P)$ and f is a block of the group

$$C_{C_G(P)}(Q) = C_G(P) \cap C_G(Q) = C_G(PQ)\,.$$

It follows that (PQ,f) is a Brauer pair of G. Moreover $br_Q(e)f = f$ since (Q,f) is associated with e, and this can be rewritten as $br_{PQ/P}(e)f = f$, because the two Brauer homomorphisms

$$br_Q : (kC_G(P))^Q \longrightarrow kC_{C_G(P)}(Q) \qquad \text{and}$$
$$br_{PQ/P} : (kC_G(P))^{PQ/P} \longrightarrow kC_G(PQ)$$

coincide. Therefore we have $(P,e) \leq (PQ,f)$ by Theorem 40.4. It follows that (PQ,f) is associated with the same block of G as (P,e), namely b. Since b is nilpotent, $N_G(PQ,f)/C_G(PQ)$ is a p-group, and therefore so is its subgroup

$$N_{C_G(P)}(PQ,f)/C_G(PQ) = N_{C_G(P)}(Q,f)/C_{C_G(P)}(Q)\,.$$

Since (Q,f) is an arbitrary Brauer pair associated with e, it follows from Proposition 49.8 that e is a nilpotent block of $kC_G(P)$. □

One of the main properties of nilpotent blocks is the following result, which will be proved in the next section.

(49.15) THEOREM. *Let b be a nilpotent block of $\mathcal{O}G$. Then $\mathcal{O}Gb$ has a unique simple module (up to isomorphism). In other words $\mathcal{O}Gb/J(\mathcal{O}Gb)$ is a simple k-algebra.*

Equivalently, for the trivial subgroup 1, there is a single local pointed group 1_δ associated with b. More generally, we have the following result.

(49.16) COROLLARY. *Let b be a nilpotent block of $\mathcal{O}G$ with defect P_γ.*

(a) For every Brauer pair (Q,f) associated with b, there is a unique local pointed group Q_δ associated with (Q,f).

(b) The poset of local pointed groups on $\mathcal{O}Gb$ is isomorphic to the poset of Brauer pairs associated with b.

(c) For every subgroup Q of P, there is a unique local pointed group Q_δ such that $Q_\delta \le P_\gamma$.

Proof. (a) Since f is nilpotent by Proposition 49.14 above, we can apply Theorem 49.15 to f. Thus there is a unique simple $kC_G(Q)f$-module, hence a unique local pointed group Q_δ associated with (Q,f).

(b) This is an immediate consequence of (a).

(c) This follows from (b) and the fact that the analogous property always holds for Brauer pairs (Corollary 40.9). □

(49.17) REMARK. The converse of Theorem 49.15 does not hold: there exist non-nilpotent blocks with a unique simple module (Exercise 49.4). However, it seems likely that the converse of Corollary 49.16 holds: if b is a block such that, for every Brauer pair (P,e) associated with b, there is a unique local pointed group P_γ associated with (P,e), then b should be nilpotent. It can be shown that this is indeed the case when a defect group of b is abelian.

Exercises

(49.1) Let b be a block of $\mathcal{O}G$ with an abelian defect group.

(a) Let Q_δ be a local pointed group on $\mathcal{O}Gb$ and let $C_G(Q)_\alpha$ be the unique pointed group such that $Q_\delta \leq C_G(Q)_\alpha$. Prove that any maximal local pointed group P_γ containing Q_δ satisfies $P_\gamma \leq C_G(Q)_\alpha$. [Hint: See the proof of Proposition 49.6.]

(b) Prove that there are no essential local pointed group on $\mathcal{O}Gb$. [Hint: Show that, for any local pointed group Q_δ on $\mathcal{O}Gb$, the group $C_G(Q)$ acts transitively on the maximal local pointed groups normalizing Q_δ.]

(c) Use Alperin's fusion theorem to give another proof of Proposition 49.6.

(49.2) Let b be a block of $\mathcal{O}G$, let P_γ be a defect of b, and suppose that $G = N_G(P_\gamma)$. Prove that b is nilpotent if and only if $E_G(P_\gamma) = 1$ (where $E_G(P_\gamma) = N_G(P_\gamma)/PC_G(P)$).

(49.3) Let b be a block of $\mathcal{O}G$ with defect P_γ and suppose that P is abelian. Let $E_G(P_\gamma) = N_G(P_\gamma)/PC_G(P)$ as usual.

(a) Prove that b is nilpotent if and only if $E_G(P_\gamma) = 1$.

(b) Suppose that P is cyclic, let Z be the unique subgroup of P of order p, and suppose that Z is central in G. Prove that b is nilpotent. [Hint: The automorphism group of P is the direct product of a p-group and a cyclic group C of order $(p-1)$, and C acts faithfully on Z.]

(49.4) The purpose of this exercise is to show the existence of a non-nilpotent block with a unique simple module. Let H be the quaternion group of order 8, let Z be the centre of H (of order 2), let z be a generator of Z, and assume that H/Z acts faithfully on a p-group P, where p is odd. (For instance P can be an $\mathbb{F}_p$-vector space endowed with a faithful representation of H/Z, in which case P is elementary abelian.) Then H acts on P, with Z acting trivially, and we let $G = P \rtimes H$ be the semi-direct product.

(a) Prove that $C_G(P) = Z(P) \times Z$ and that $b = \frac{1}{2}(1 - z)$ is a block of $C_G(P)$.

(b) Deduce that b is a block of G with defect group P. [Hint: Use Exercise 37.8.]

(c) Prove that the one-dimensional sign representation V of Z is the unique simple module of the algebra $\mathcal{O}C_G(P)b$. Show that V is the multiplicity module of a point γ of $(\mathcal{O}G)^P$ such that P_γ is a defect of $\mathcal{O}Gb$. In other words show that (P, b) is a maximal Brauer pair associated with b.

(d) Prove that $E_G(P_\gamma) = N_G(P_\gamma)/PC_G(P)$ has order 4, so that b is not nilpotent.
(e) Prove that if W is a simple $\mathcal{O}Gb$-module, then P acts trivially on W and z acts by multiplication by -1 on W.
(f) Prove that there is a unique simple module W associated with b. [Hint: Show that, since k has odd characteristic, H has four one-dimensional representations on which z acts trivially, and exactly one two-dimensional irreducible representation W on which z acts by multiplication by -1.]
(g) Noticing that b has a normal defect group, prove that the twisted group algebra $\mathcal{O}_\sharp \widehat{E}_G(P_\gamma)$ appearing in Theorem 45.12 is $\mathcal{O}$-simple.

Notes on Section 49

The notion of control of fusion is classical for p-subgroups. It appears in Alperin and Broué [1979] for Brauer pairs (see also Broué and Olsson [1986]), and in Puig [1988b] for local pointed groups. The definition of nilpotent blocks is due to Broué and Puig [1980b], who also proved most of their properties, in particular Theorem 49.15. A proof of the Frobenius theorem appears in Huppert [1967], or in Broué and Puig [1980b] using nilpotent blocks (see also Exercise 50.4). The conjecture that the converse of Corollary 49.16 holds (see Remark 49.17) is due to Puig [1988b] and is also discussed in Watanabe [1994]. The proof of this conjecture when a defect group is abelian appears in Puig and Watanabe [1994].

§ 50 THE STRUCTURE OF A SOURCE ALGEBRA OF A NILPOTENT BLOCK

In this section we prove Puig's theorem, which describes explicitly the structure of a source algebra of a nilpotent block. For simplicity, throughout this section, $\mathcal{O}$ is equal either to k or to a complete discrete valuation ring of characteristic zero (satisfying Assumption 42.1). The main result will be completely proved over k, but in characteristic zero, it is based on a crucial property which will be proved in the next section.

Let b be a nilpotent block of $\mathcal{O}G$ and let the interior P-algebra $B = (\mathcal{O}Gb)_\gamma$ be a source algebra of b. Our aim is to show that B is isomorphic to $S \otimes_{\mathcal{O}} \mathcal{O}P$, where $S = \mathrm{End}_{\mathcal{O}}(L)$ is the endomorphism algebra of an endo-permutation $\mathcal{O}P$-lattice L. The way to get hold of S is provided by the following property.

(50.1) PROPOSITION. *Let b be a nilpotent block of $\mathcal{O}G$ and let the interior P-algebra $B = (\mathcal{O}Gb)_\gamma$ be a source algebra of b. Then there exists an $\mathcal{O}$-simple quotient S of B of dimension prime to p.*

It can be proved that this property holds for any base ring $\mathcal{O}$ satisfying our usual Assumption 2.1, but the proof involves lengthy discussions concerning only the structure of $\mathcal{O}$. For this reason we only consider the following two cases (which are actually the two main cases of interest): either $\mathcal{O} = k$ or $\mathcal{O}$ is a discrete valuation ring of characteristic zero (satisfying Assumption 42.1). The proposition is easy to prove over k (as we shall see below), but it is not at all trivial when $\mathcal{O}$ is a discrete valuation ring of characteristic zero. The proof will be given in the next section and will follow a rather complicated route: we shall use the main result of this section, which will be already proved over k, and this will allow us to lift the information to $\mathcal{O}$.

Proof of Proposition 50.1 over k. Assume that $\mathcal{O} = k$. We have already proved in two different ways that there exists a simple B-module V of dimension prime to p (Proposition 44.9 or Corollary 46.16). Thus $S = \mathrm{End}_k(V)$ is isomorphic to a simple quotient of B. Clearly $\dim_k(S)$ is prime to p since $\dim_k(S) = \dim_k(V)^2$. □

The notation above will be in force throughout this section. Thus b is a block of $\mathcal{O}G$ with defect P_γ and the interior P-algebra $B = (\mathcal{O}Gb)_\gamma$ is a source algebra of b. Moreover let $\varepsilon : \mathcal{O}P \to \mathcal{O}$ be the augmentation homomorphism, defined by $\varepsilon(u) = 1$ for every $u \in P$, and for every P-algebra C, let $h_C : C \otimes_\mathcal{O} \mathcal{O}P \to C$ be the composite

$$C \otimes_\mathcal{O} \mathcal{O}P \xrightarrow{id_C \otimes \varepsilon} C \otimes_\mathcal{O} \mathcal{O} \cong C\,.$$

Thus $h_C(c \otimes u) = c$ for $c \in C$ and $u \in P$. We shall also call h_C the *augmentation homomorphism*. We are going to work particularly with the map h_B, for B as above.

We prepare the proof of the main theorem of this section with a series of lemmas. The first one is quite general and has nothing to do with source algebras.

(50.2) LEMMA. *Let C be a P-algebra. Then the augmentation map $h_C : C \otimes_\mathcal{O} \mathcal{O}P \to C$ is a strict covering homomorphism of P-algebras. In particular $C \otimes_\mathcal{O} \mathcal{O}P$ is a primitive P-algebra if C is primitive.*

Proof. The map $s : C \to C \otimes_{\mathcal{O}} \mathcal{O}P$ defined by $s(c) = c \otimes 1_{\mathcal{O}P}$ satisfies $h_C s = id_C$. Moreover s is a homomorphism of P-algebras, because

$$s({}^u c) = {}^u c \otimes 1_{\mathcal{O}P} = {}^u c \otimes {}^u 1_{\mathcal{O}P} = {}^u(c \otimes 1_{\mathcal{O}P}) = {}^u(s(c))$$

(but we note that s is not a homomorphism of interior P-algebras in case C is interior). It follows that, for every subgroup Q of P, the restriction to Q-fixed elements $h_C^Q : (C \otimes_{\mathcal{O}} \mathcal{O}P)^Q \to C^Q$ is surjective. Indeed if $c \in C^Q$, then $s(c) \in (C \otimes_{\mathcal{O}} \mathcal{O}P)^Q$. This proves that h_C is a covering homomorphism.

To prove that h_C is strict, we note that $\mathrm{Ker}(h_C) = C \otimes_{\mathcal{O}} I(\mathcal{O}P)$, where $I(\mathcal{O}P) = \mathrm{Ker}(\varepsilon)$ is the augmentation ideal. But since P is a p-group, $I(\mathcal{O}P) \subseteq J(\mathcal{O}P)$ (Proposition 21.1), and it follows that

$$\mathrm{Ker}(h_C) \subseteq C \otimes_{\mathcal{O}} J(\mathcal{O}P) \subseteq J(C \otimes_{\mathcal{O}} \mathcal{O}P) .$$

The second inclusion is a consequence of the fact that $C \otimes_{\mathcal{O}} J(\mathcal{O}P)$ is an ideal which is nilpotent modulo $\mathfrak{p}$ (that is, $(C/\mathfrak{p}C) \otimes_k J(kP)$ is nilpotent, so that $(C/\mathfrak{p}C) \otimes_k J(kP) \subseteq J((C/\mathfrak{p}C) \otimes_k kP)$). Now the inclusion $\mathrm{Ker}(h_C) \subseteq J(C \otimes_{\mathcal{O}} \mathcal{O}P)$ shows that the covering homomorphism h_C is strict. □

It is in the following result that we use the assumption that b is a nilpotent block.

(50.3) LEMMA. *Let $h_B : B \otimes_{\mathcal{O}} \mathcal{O}P \to B$ be the augmentation map. If b is a nilpotent block, then*

$$\mathrm{Ind}_P^G(h_B) : \mathrm{Ind}_P^G(B \otimes_{\mathcal{O}} \mathcal{O}P) \longrightarrow \mathrm{Ind}_P^G(B)$$

is a strict covering homomorphism of G-algebras.

Proof. Write $f = \mathrm{Ind}_P^G(h_B)$ and $C = B \otimes_{\mathcal{O}} \mathcal{O}P$ for simplicity. We use the local characterization of covering homomorphisms given in Corollary 25.11. Thus, for every p-subgroup Q of G, we have to prove the following two properties.

(a) For every local point δ of $\mathrm{Ind}_P^G(C)^Q$, there exists a local point ε of $\mathrm{Ind}_P^G(B)^Q$ such that $f(\delta) \subseteq \varepsilon$.

(b) Whenever two local points δ and δ' of $\mathrm{Ind}_P^G(C)^Q$ satisfy $f(\delta) \subseteq \varepsilon$ and $f(\delta') \subseteq \varepsilon$, then $\delta = \delta'$.

Since h_B is a strict covering homomorphism, we know that the analogous properties hold for h_B instead of f and local pointed groups on C and B. The strategy is to reduce to that case by conjugation.

We first prove (a). Let $\mathcal{D}_P^G(C) : C \to \mathrm{Res}_P^G \mathrm{Ind}_P^G(C)$ be the canonical embedding. By Proposition 16.7, there exists $g \in G$ such that ${}^g(Q_\delta)$ is in the image of $\mathcal{D}_P^G(C)$. We use this embedding to identify pointed groups on C with pointed groups on $\mathrm{Ind}_P^G(C)$ and we say that the pointed groups in the image of $\mathcal{D}_P^G(C)$ come from C. Thus ${}^g(Q_\delta)$ comes from C, and since $h_B : C \to B$ is a strict covering homomorphism of P-algebras (Lemma 50.2), $h_B({}^g\delta) \subseteq \varepsilon$ for some local pointed group $({}^gQ)_\varepsilon$ on B. Now $({}^gQ)_\varepsilon$ is identified with a local pointed group on $\mathrm{Ind}_P^G(B)$. Therefore $Q_{{}^{g^{-1}}\varepsilon}$ is a local pointed group on $\mathrm{Ind}_P^G(B)$ and $\mathrm{Ind}_P^G(h_B)(\delta) \subseteq {}^{g^{-1}}\varepsilon$, proving (a). Note that this argument is quite general and has nothing to do with nilpotent blocks.

Before embarking on the proof of (b), we first note that, since B is a source algebra of $\mathcal{O}Gb$, there is an embedding $\mathcal{E} : \mathcal{O}Gb \to \mathrm{Ind}_P^G(B)$ such that $\mathrm{Res}_P^G(\mathcal{E})\,\mathcal{F}_\gamma = \mathcal{D}_P^G(B)$, where $\mathcal{F}_\gamma : B \to \mathrm{Res}_P^G(\mathcal{O}Gb)$ is an embedding associated with γ and $\mathcal{D}_P^G(B) : B \to \mathrm{Res}_P^G \mathrm{Ind}_P^G(B)$ is the canonical embedding (see Proposition 18.9). Via $\mathcal{E}$, we can identify the local pointed groups on $\mathcal{O}Gb$ with those on $\mathrm{Ind}_P^G(B)$. (Note for completeness that it is an easy consequence of Proposition 16.7 that every local pointed group on $\mathrm{Ind}_P^G(B)$ is in the image of $\mathcal{E}$.) Moreover the local pointed groups on B are identified with the local pointed groups on $\mathcal{O}Gb$ contained in P_γ. Therefore the G-conjugates of local pointed groups on B (which come in the definition of the Puig category), can be viewed as local pointed groups on $\mathrm{Ind}_P^G(B)$, without mentioning the block algebra $\mathcal{O}Gb$. In other words we identify the Puig category of $\mathcal{O}Gb$ with that of $\mathrm{Ind}_P^G(B)$. We use these remarks implicitly in the following argument.

Now we prove (b). Let δ and δ' be two local points of $\mathrm{Ind}_P^G(C)^Q$ such that $f(\delta) \subseteq \varepsilon$ and $f(\delta') \subseteq \varepsilon$, where $\varepsilon \in \mathcal{LP}(\mathrm{Ind}_P^G(B)^Q)$. We have to prove that $\delta = \delta'$. Since some conjugate of Q_δ comes from C (Proposition 16.7), we can conjugate the whole situation and assume that Q_δ comes from C. Then Q_ε necessarily comes from B, since $f(\delta) \subseteq \varepsilon$ and $f = \mathrm{Ind}_P^G(h_B)$. Explicitly δ contains an idempotent of the form $1 \otimes i \otimes 1$ and so $f(1 \otimes i \otimes 1) = 1 \otimes h_B(i) \otimes 1$ belongs to $\varepsilon \cap (1 \otimes B \otimes 1)$. Now by Proposition 16.7 again, there exists $g \in G$ such that ${}^g(Q_{\delta'})$ comes from C, and so ${}^g(Q_\varepsilon)$ comes from B because $f({}^g\delta') \subseteq {}^g\varepsilon$. But the local pointed groups on $\mathrm{Ind}_P^G(B)$ which come from B are precisely those which are contained in P_γ, because B is primitive and γ is the unique point of B^P. Therefore we have the relations

$$Q_\varepsilon \le P_\gamma \qquad \text{and} \qquad {}^g(Q_\varepsilon) \le P_\gamma\,.$$

Since b is a nilpotent block, P controls fusion in $\mathcal{L}_G(b)_{\le P_\gamma}$. Thus $g = uc$, where $u \in P$ and $c \in C_G(Q)$, so that ${}^g(Q_{\delta'}) = {}^{uc}(Q_{\delta'}) = {}^u(Q_{\delta'})$ (because $C_G(Q)$ normalizes $Q_{\delta'}$). Since this local pointed group comes from C, so does its conjugate $Q_{\delta'}$, because C is a P-algebra and $u \in P$. Therefore both Q_δ and $Q_{\delta'}$ come from C. Now the inclusions $f(\delta) \subseteq \varepsilon$ and $f(\delta') \subseteq \varepsilon$ can be rewritten as $h_B(\delta) \subseteq \varepsilon$ and $h_B(\delta') \subseteq \varepsilon$ if Q_δ and Q'_δ are viewed as pointed groups on C. Since we know that h_B is a covering homomorphism (Lemma 50.2), we must have $\delta = \delta'$, as was to be shown. □

We have noticed in the proof of Lemma 50.2 that the homomorphism $s : B \to B \otimes_{\mathcal{O}} \mathcal{O}P$ defined by $s(b) = b \otimes 1_{\mathcal{O}P}$ is a section of the augmentation map h_B and is a homomorphism of P-algebras. However, it is not a homomorphism of interior P-algebras. It turns out that the existence of a section of h_B which is a homomorphism of interior P-algebras is a special feature of nilpotent blocks. This is our next result.

(50.4) LEMMA. *Let $h_B : B \otimes_{\mathcal{O}} \mathcal{O}P \to B$ be the augmentation map. If b is a nilpotent block, there exists a homomorphism of interior P-algebras $s : B \to B \otimes_{\mathcal{O}} \mathcal{O}P$ such that $h_B s = id_B$.*

Proof. Throughout this proof, it is much more convenient to work with exomorphisms, so we let $\mathcal{H}$ be the exomorphism of interior P-algebras containing h_B. Since B is a source algebra of $\mathcal{O}Gb$, there is an embedding $\mathcal{F}_\alpha : \mathcal{O}Gb \to \mathrm{Ind}_P^G(B)$ such that $\mathrm{Res}_P^G(\mathcal{F}_\alpha)\,\mathcal{F}_\gamma = \mathcal{D}_P^G(B)$, where $\mathcal{F}_\gamma : B \to \mathrm{Res}_P^G(\mathcal{O}Gb)$ denotes an embedding associated with γ and where $\mathcal{D}_P^G(B) : B \to \mathrm{Res}_P^G \mathrm{Ind}_P^G(B)$ is the canonical embedding (Proposition 18.9). Since $\mathcal{O}Gb$ is a primitive G-algebra, it is a localization of $\mathrm{Ind}_P^G(B)$ with respect to the point $\alpha = \mathcal{F}_\alpha(b) \in \mathcal{P}(\mathrm{Ind}_P^G(B)^G)$. In other words $\mathcal{F}_\alpha$ is an embedding associated with the pointed group G_α on $\mathrm{Ind}_P^G(B)$, and this motivates the notation. The point $\delta = \mathcal{F}_\alpha(\gamma) \in \mathcal{P}(\mathrm{Ind}_P^G(B)^P)$ is equal to the point containing $1 \otimes 1_B \otimes 1$ because $\mathcal{D}_P^G(B) = \mathrm{Res}_P^G(\mathcal{F}_\alpha)\,\mathcal{F}_\gamma$, and so $\mathcal{D}_P^G(B)$ is an embedding associated with P_δ. Thus the embedding

$$\mathcal{F}_\gamma : B = \mathrm{Ind}_P^G(B)_\delta \longrightarrow \mathrm{Res}_P^G(\mathcal{O}Gb) = \mathrm{Res}_P^G(\mathrm{Ind}_P^G(B)_\alpha)$$

is equal to the unique embedding $\mathcal{F}_\delta^\alpha$ expressing the relation $P_\delta \le G_\alpha$ (Proposition 13.6).

Since $\mathrm{Ind}_P^G(\mathcal{H})$ is a covering exomorphism (Lemma 50.3), there exists a unique point $\alpha^* \in \mathcal{P}(\mathrm{Ind}_P^G(B \otimes \mathcal{O}P)^G)$ such that $\mathrm{Ind}_P^G(\mathcal{H})(\alpha^*) \subseteq \alpha$. We write $\mathcal{F}_{\alpha^*} : \mathrm{Ind}_P^G(B \otimes \mathcal{O}P)_{\alpha^*} \to \mathrm{Ind}_P^G(B \otimes \mathcal{O}P)$ for an embedding associated with G_{α^*}. Moreover by Proposition 25.7, the covering exomorphism induces an exomorphism between the localizations

$$\mathrm{Ind}_P^G(\mathcal{H})_\alpha : \mathrm{Ind}_P^G(B \otimes \mathcal{O}P)_{\alpha^*} \longrightarrow \mathcal{O}Gb = \mathrm{Ind}_P^G(B)_\alpha$$

such that $\mathcal{F}_\alpha\, \mathrm{Ind}_P^G(\mathcal{H})_\alpha = \mathrm{Ind}_P^G(\mathcal{H})\,\mathcal{F}_{\alpha^*}$.

Since B is a primitive P-algebra, so is $B \otimes \mathcal{O}P$ (because there is a strict covering exomorphism $\mathcal{H} : B \otimes \mathcal{O}P \to B$), and the canonical embedding

$$\mathcal{D}_P^G(B \otimes \mathcal{O}P) : B \otimes \mathcal{O}P \longrightarrow \mathrm{Res}_P^G \mathrm{Ind}_P^G(B \otimes \mathcal{O}P)$$

is an embedding associated with the pointed group P_{δ^*} , where δ^* contains $1 \otimes 1_{B\otimes\mathcal{O}P} \otimes 1$. Clearly δ^* maps to δ via the covering exomorphism $\mathrm{Ind}_P^G(\mathcal{H})$. The relation $P_\delta \le G_\alpha$ implies the relation $P_{\delta^*} \le G_{\alpha^*}$ (Proposition 25.6), and this implies the existence of an embedding

$$\mathcal{F}_{\delta^*}^{\alpha^*} : B \otimes \mathcal{O}P \longrightarrow \mathrm{Res}_P^G(\mathrm{Ind}_P^G(B \otimes \mathcal{O}P)_{\alpha^*})$$

such that $\mathrm{Res}_P^G(\mathcal{F}_{\alpha^*})\,\mathcal{F}_{\delta^*}^{\alpha^*} = \mathcal{D}_P^G(B \otimes \mathcal{O}P)$ (Proposition 13.6). Clearly the point $\gamma^* = \mathcal{F}_{\delta^*}^{\alpha^*}(1_{B\otimes\mathcal{O}P})$ of $(\mathrm{Ind}_P^G(B \otimes \mathcal{O}P)_{\alpha^*})^P$ maps to δ^* via $\mathcal{F}_{\alpha^*}$. The embedding $\mathcal{F}_{\delta^*}^{\alpha^*}$ can also be viewed as an embedding associated with the pointed group P_{γ^*} , and for this reason we write simply $\mathcal{F}_{\gamma^*} = \mathcal{F}_{\delta^*}^{\alpha^*}$.

This discussion shows that there is a commutative diagram of exomorphisms

(50.5)

$$\begin{array}{ccccc}
B \otimes \mathcal{O}P & \xrightarrow{\mathcal{F}_{\gamma^*}} & \mathrm{Res}_P^G(\mathrm{Ind}_P^G(B \otimes \mathcal{O}P)_{\alpha^*}) & \xrightarrow{\mathrm{Res}_P^G(\mathcal{F}_{\alpha^*})} & \mathrm{Res}_P^G \mathrm{Ind}_P^G(B \otimes \mathcal{O}P) \\
{\scriptstyle \mathcal{H}}\big\downarrow & & {\scriptstyle \mathrm{Res}_P^G(\mathrm{Ind}_P^G(\mathcal{H})_\alpha)}\big\downarrow & & {\scriptstyle \mathrm{Res}_P^G \mathrm{Ind}_P^G(\mathcal{H})}\big\downarrow \\
B & \xrightarrow{\mathcal{F}_\gamma} & \mathrm{Res}_P^G(\mathcal{O}Gb) & \xrightarrow{\mathrm{Res}_P^G(\mathcal{F}_\alpha)} & \mathrm{Res}_P^G \mathrm{Ind}_P^G(B)
\end{array}$$

and the composite exomorphisms in both rows are the canonical embeddings $\mathcal{D}_P^G(B\otimes\mathcal{O}P)$ and $\mathcal{D}_P^G(B)$ respectively. To prove the commutativity of the first square, we have

$$\begin{aligned}
\mathrm{Res}_P^G(\mathcal{F}_\alpha)\,\mathcal{F}_\gamma\,\mathcal{H} &= \mathcal{D}_P^G(B)\,\mathcal{H} = \mathrm{Res}_P^G \mathrm{Ind}_P^G(\mathcal{H})\,\mathcal{D}_P^G(B \otimes \mathcal{O}P) \\
&= \mathrm{Res}_P^G \mathrm{Ind}_P^G(\mathcal{H})\ \mathrm{Res}_P^G(\mathcal{F}_{\alpha^*})\,\mathcal{F}_{\gamma^*} \\
&= \mathrm{Res}_P^G(\mathcal{F}_\alpha)\ \mathrm{Res}_P^G(\mathrm{Ind}_P^G(\mathcal{H})_\alpha)\,\mathcal{F}_{\gamma^*} ,
\end{aligned}$$

and we can cancel the embedding $\mathrm{Res}_P^G(\mathcal{F}_\alpha)$ (Proposition 12.2).

Now we show that the middle exomorphism $\mathrm{Ind}_P^G(\mathcal{H})_\alpha$ has a section. For simplicity we choose some homomorphism $q \in \mathrm{Ind}_P^G(\mathcal{H})_\alpha$. Since $\mathrm{Ind}_P^G(B\otimes\mathcal{O}P)_{\alpha^*}$ is an interior G-algebra, there is a unique homomorphism of interior G-algebras $\mathcal{O}G \to \mathrm{Ind}_P^G(B \otimes \mathcal{O}P)_{\alpha^*}$, and we let

$$s : \mathcal{O}Gb \to \mathrm{Ind}_P^G(B \otimes \mathcal{O}P)_{\alpha^*}$$

be its restriction to the block algebra $\mathcal{O}Gb$. Since $\mathrm{Ind}_P^G(\mathcal{H})$ is unitary (because it is a covering homomorphism), so is $\mathrm{Ind}_P^G(\mathcal{H})_\alpha$. Thus q is unitary, so $q(g{\cdot}1) = g{\cdot}1$ for all $g \in G$, and therefore the composite

$$q\,s : \mathcal{O}Gb \longrightarrow \mathcal{O}Gb$$

can only be the identity (and thus $\mathrm{Ind}_P^G(B \otimes \mathcal{O}P)_{\alpha^*}$ is in fact associated with the block b). This shows that q has a section s (which is the same for every choice of q). In fact the exomorphism $\mathcal{S}$ containing s consists of a singleton $\mathcal{S} = \{s\}$.

We want to prove that $\mathcal{S}$ induces by restriction to B a section of $\mathcal{H}$. First we want to show that $\mathcal{S}$ induces an exomorphism between the localizations

$$\mathcal{S}_\gamma : B = (\mathcal{O}Gb)_\gamma \longrightarrow B \otimes \mathcal{O}P = (\mathrm{Ind}_P^G(B \otimes \mathcal{O}P)_{\alpha^*})_{\gamma^*} .$$

This is usually not possible since in general the image of a point under an exomorphism does not consist of primitive idempotents. But we are going to show that $\mathcal{S}(\gamma) \subseteq \gamma^*$, and then an elementary argument (as in the proof of Proposition 25.7) shows that $\mathcal{S}$ induces $\mathcal{S}_\gamma$ as above, such that $\mathcal{S}\,\mathcal{F}_\gamma = \mathcal{F}_{\gamma^*}\,\mathcal{S}_\gamma$. Now we know that $\mathrm{Ind}_P^G(\mathcal{H})$ is a strict covering exomorphism, so that $\mathrm{Ind}_P^G(\mathcal{H})_\alpha$ is also a strict covering exomorphism (Proposition 25.7). Moreover $(\mathrm{Ind}_P^G(\mathcal{H})_\alpha)(\gamma^*) \subseteq \gamma$ (because $\mathrm{Ind}_P^G(\mathcal{H})(\delta^*) \subseteq \delta$). Let us choose $i \in \gamma$ and $q \in \mathrm{Ind}_P^G(\mathcal{H})_\alpha$. If we let $s(i) = \sum j$ be a primitive decomposition of $s(i)$ in $(\mathrm{Ind}_P^G(B \otimes \mathcal{O}P)_{\alpha^*})^P$, we have

$$i = qs(i) = \sum q(j) .$$

Since q is a *strict* covering homomorphism, each $q(j)$ is non-zero (and is a primitive idempotent of $(\mathcal{O}Gb)^P$). Therefore the primitivity of i implies that there is a single idempotent j in the decomposition of $s(i)$. Moreover $s(i) = j$ belongs to γ^* because γ^* is the unique point such that $q(\gamma^*) \subseteq \gamma$ (since q is a covering homomorphism). This completes the proof that $\mathcal{S}(\gamma) \subseteq \gamma^*$ and shows the existence of the induced exomorphism $\mathcal{S}_\gamma$.

Finally we show that $\mathcal{S}_\gamma$ is a section of $\mathcal{H}$. This is because, by the commutativity of the diagram 50.5, we have

$$\begin{aligned}\mathcal{F}_\gamma\,\mathcal{H}\,\mathcal{S}_\gamma &= \mathrm{Res}_P^G(\mathrm{Ind}_P^G(\mathcal{H})_\alpha)\,\mathcal{F}_{\gamma^*}\,\mathcal{S}_\gamma = \mathrm{Res}_P^G(\mathrm{Ind}_P^G(\mathcal{H})_\alpha)\,\mathcal{S}\,\mathcal{F}_\gamma \\ &= \{id_{\mathcal{O}Gb}\}\,\mathcal{F}_\gamma = \mathcal{F}_\gamma\,\{id_B\} ,\end{aligned}$$

and the result follows by cancelling the embedding $\mathcal{F}_\gamma$ (Proposition 12.2). This completes the proof that the exomorphism $\mathcal{H}$ has a section $\mathcal{S}_\gamma$. Therefore if $t \in \mathcal{S}_\gamma$, the augmentation map $h_B \in \mathcal{H}$ satisfies $h_B\,t = \mathrm{Inn}(b)$ for some $b \in (B^P)^*$. Thus $h_B\,t\,\mathrm{Inn}(b^{-1}) = id_B$ and $t\,\mathrm{Inn}(b^{-1})$ is a homomorphism of interior P-algebras. This completes the proof that h_B has a section. □

Now we come to the main result, giving the description of a source algebra of a nilpotent block.

(50.6) THEOREM (Puig's theorem). *Assume that either $\mathcal{O} = k$ or that $\mathcal{O}$ is a discrete valuation ring of characteristic zero (satisfying Assumption 42.1). Let b be a block of $\mathcal{O}G$ with defect P_γ and let the interior P-algebra $B = (\mathcal{O}Gb)_\gamma$ be a source algebra of b.*

(a) If b is nilpotent, there exists an $\mathcal{O}$-simple interior P-algebra S and an isomorphism of interior P-algebras

$$B \cong S \otimes_{\mathcal{O}} \mathcal{O}P \,.$$

(b) S is a primitive Dade P-algebra with defect group P. In other words if we write $S \cong \mathrm{End}_{\mathcal{O}}(L)$, then the $\mathcal{O}P$-lattice L is an indecomposable endo-permutation $\mathcal{O}P$-lattice with vertex P. In particular $\dim_{\mathcal{O}}(S) \equiv 1 \pmod p$.

Proof. (a) By Proposition 50.1 (which will be proved in the next section in case $\mathcal{O}$ has characteristic zero), there exists an $\mathcal{O}$-simple quotient S of B of dimension prime to p. Let $q : B \to S$ be the quotient map. Tensoring with $\mathcal{O}P$, we obtain a homomorphism of interior P-algebras

$$\widehat{q} = q \otimes id : B \otimes_{\mathcal{O}} \mathcal{O}P \longrightarrow S \otimes_{\mathcal{O}} \mathcal{O}P \,.$$

Let also $h_B : B \otimes_{\mathcal{O}} \mathcal{O}P \to B$ and $h_S : S \otimes_{\mathcal{O}} \mathcal{O}P \to S$ be the augmentation maps. We clearly have $h_S \widehat{q} = q\, h_B$.

By Lemma 50.4, h_B has a section $s : B \to B \otimes_{\mathcal{O}} \mathcal{O}P$ (a homomorphism of interior P-algebras). We consider the composite

$$B \xrightarrow{s} B \otimes_{\mathcal{O}} \mathcal{O}P \xrightarrow{\widehat{q}} S \otimes_{\mathcal{O}} \mathcal{O}P \,.$$

We want to prove that this composite is an isomorphism. Since all algebras involved are free as $\mathcal{O}$-modules (because B is a direct summand of $\mathcal{O}G$ as an $\mathcal{O}$-module), it suffices to reduce modulo $\mathfrak{p}$ and prove that the corresponding composite map over k is an isomorphism (Proposition 1.3). Note that this reduction involves the fact that $B/\mathfrak{p}B$ is a source algebra of $kG\bar{b}$ (Lemma 38.1). Thus we assume from now on that $\mathcal{O} = k$. In particular S is now a simple algebra. We simply write $\otimes$ for the tensor product over k.

By construction $S \cong \mathrm{End}_k(V)$ where V is a simple B-module. On the other hand V also has a $S \otimes kP$-module structure via the augmentation map $h_S : S \otimes kP \to S \cong \mathrm{End}_k(V)$. The restriction of this structure to B via the map $\widehat{q}\, s$ is the given B-module structure of V because

$$h_S\, \widehat{q}\, s = q\, h_B\, s = q \,,$$

using the fact that s is a section of h_B. Thus V is both a simple $S \otimes kP$-module and a simple B-module. Moreover V is the unique simple $S \otimes kP$-module up to isomorphism, because S is the unique simple quotient of $S \otimes kP$. Indeed the augmentation map $h_S : S \otimes kP \to S$ is a covering homomorphism by Lemma 50.2 (alternatively and more directly, the kernel of h_S is nilpotent by Proposition 21.1). One crucial point to be proved below is that V is also the unique simple B-module up to isomorphism.

As V is a projective S-module, $V \otimes kP$ is a projective $S \otimes kP$-module (explicitly, a direct sum of $\dim(V)$ copies of $V \otimes kP$ is isomorphic to $S \otimes kP$). We claim that $V \otimes kP$ is also projective as a B-module (by restriction along $\widehat{q}\, s$). To prove this, it suffices by Corollary 38.4 to restrict further to kP and show that $\mathrm{Res}_P(V \otimes kP)$ is a projective kP-module. Since the structural homomorphism $kP \to S \otimes kP$ maps $u \in P$ to $u{\cdot}1_S \otimes u$, the action of P on $\mathrm{Res}_P(V \otimes kP)$ is "diagonal" (that is, $u{\cdot}(v \otimes a) = u{\cdot}v \otimes ua$ for $u \in P$, $v \in V$ and $a \in kP$), and therefore $\mathrm{Res}_P(V \otimes kP) = \mathrm{Res}_P(V) \otimes kP$. Since kP is obviously projective, $\mathrm{Res}_P(V) \otimes kP$ is a projective kP-module by Exercise 17.4. This completes the proof that $V \otimes kP$ is a projective B-module.

We claim that all composition factors of $V \otimes kP$ as a B-module are isomorphic to V. Indeed since the trivial kP-module k is the only simple kP-module (Proposition 21.1), any composition series of kP has all its composition factors isomorphic to k. Tensoring with V, we obtain a composition series of $V \otimes kP$ as $S \otimes kP$-module with all composition factors isomorphic to $V \otimes k \cong V$. Since V remains simple on restriction to B, this is also a composition series of $V \otimes kP$ as a B-module, proving the claim.

We do not know yet that $V \otimes kP$ is indecomposable as a B-module, but certainly any indecomposable direct summand Q of $V \otimes kP$ has all its composition factors isomorphic to V. In particular Q is a projective cover of V. If α denotes the point of B corresponding to the simple B-module V, we have $V = V(\alpha)$ and $Q = P(\alpha)$, and for every point $\beta \neq \alpha$, the Cartan integer $c_{\beta,\alpha}$ is zero. Since the Cartan matrix of $B = (kGb)_\gamma$ is equal to the Cartan matrix of kGb (Proposition 38.2) and since the Cartan matrix of a block algebra is symmetric (Exercise 6.5 or Theorem 42.11), we deduce that $c_{\alpha,\beta} = 0$ for every point $\beta \neq \alpha$. By Proposition 5.13, it follows that B decomposes as a direct product $B \cong B_1 \times B_2$, where α is the unique point of B_1 and $\mathcal{P}(B_2) = \{\, \beta \in \mathcal{P}(B) \mid \beta \neq \alpha \,\}$. But since B is a primitive P-algebra, it cannot decompose as a direct product in a non-trivial fashion. Therefore $B_2 = 0$, $B = B_1$ and α is the unique point of B. We record this important fact:

(50.7) B has a unique point, hence a unique simple module V up to isomorphism. Moreover p does not divide $\dim_k(V)$.

The second assertion follows from the fact that we started with a simple quotient S of B of dimension prime to p and $\dim(S) = \dim(V)^2$ (because $S \cong \mathrm{End}_k(V)$).

Now we can prove that the projective B-module $V \otimes kP$ is indecomposable. Since B has a unique point, $Q = P(\alpha)$ is the unique projective indecomposable B-module up to isomorphism, and therefore $V \otimes kP$ is isomorphic to a direct sum of m copies of Q for some integer $m \geq 1$. If n is the number of composition factors of Q (all isomorphic to V), then $\dim(Q) = n \dim(V)$ and so

$$|P| \dim(V) = \dim(V \otimes kP) = m \dim(Q) = mn \dim(V) .$$

Thus $|P| = mn$. Now on restriction to kP, Q is a projective kP-module (Corollary 38.4), hence a free kP-module (Proposition 21.1). Therefore $|P|$ divides $\dim(Q) = n \dim(V)$, and since p does not divide $\dim(V)$, it follows that $|P|$ divides n. But since we also have $|P| = mn$, we conclude that $m = 1$. This proves that $V \otimes kP \cong Q$ is indecomposable.

Now we can prove that the map $\widehat{q}\, s : B \to S \otimes kP$ is an isomorphism. If $a \in \mathrm{Ker}(\widehat{q}\, s)$, then a annihilates the module $S \otimes kP$, hence also $V \otimes kP$ (because $S \otimes kP$ is isomorphic to a direct sum of copies of $V \otimes kP$). Now $V \otimes kP$ is also indecomposable projective as a B-module and B is isomorphic to a direct sum of copies of $V \otimes kP$ (because $V \otimes kP$ is the unique indecomposable projective B-module up to isomorphism). Therefore a annihilates B, and so $a = 0$ since $a \in B$ acts by left multiplication. This proves the injectivity of $\widehat{q}\, s$.

To prove the surjectivity, it suffices now to show that B and $S \otimes kP$ have the same dimension. But by Corollary 5.3, the multiplicity of the unique indecomposable projective B-module $V \otimes kP$ as a direct summand of B is equal to $\dim(V)$. Therefore

$$\dim(B) = \dim(V \otimes kP) \dim(V) = |P| \dim(V)^2 = |P| \dim(S) = \dim(S \otimes kP)$$

and this completes the proof that $B \cong S \otimes kP$. We have already seen that this implies the similar result over $\mathcal{O}$.

(b) We now prove the additional statement about S and L, where $S \cong \mathrm{End}_{\mathcal{O}}(L)$. Note for completeness that, since we have used above reduction modulo $\mathfrak{p}$, we have $L/\mathfrak{p}L \cong V$, a simple B-module. Since B is a primitive P-algebra, so is S, otherwise there would be a nontrivial idempotent in $S^P \otimes 1_{\mathcal{O}P} \subseteq (S \otimes_{\mathcal{O}} \mathcal{O}P)^P \cong B^P$. In other words L is indecomposable. Since B has defect group P, so has S (because if S is projective relative to a proper subgroup of P, so is $S \otimes_{\mathcal{O}} \mathcal{O}P$ by Lemma 14.3). In other words L has vertex P.

In order to prove that S is a Dade P-algebra (or in other words that L is an endo-permutation $\mathcal{O}P$-lattice), we have to show that S has a P-invariant basis (for the conjugation action of P). By Proposition 38.7, we know that B has a P-invariant basis (for the conjugation action of P). But since $\mathcal{O}P = \oplus_{u \in P} \mathcal{O}u$, we have a P-invariant decomposition

$$B \cong S \otimes \mathcal{O}P = (S \otimes 1) \bigoplus \Big(\bigoplus_{\substack{u \in P \\ u \neq 1}} (S \otimes u) \Big) .$$

Therefore $S \cong S \otimes 1$ has a P-invariant basis, since a direct summand of a permutation $\mathcal{O}P$-lattice is a permutation $\mathcal{O}P$-lattice (Corollary 27.2). Finally the congruence $\dim_{\mathcal{O}}(S) \equiv 1 \pmod{p}$ follows from Corollary 28.11. This completes the proof of the theorem. □

We derive an important consequence which was announced in the previous section (Theorem 49.15).

(50.8) COROLLARY. *Let b be a nilpotent block of $\mathcal{O}G$. Then $\mathcal{O}Gb$ has a unique point, hence a unique simple module up to isomorphism. In other words $\mathcal{O}Gb/J(\mathcal{O}Gb)$ is a simple k-algebra.*

Proof. By the Morita equivalence between a block algebra and its source algebra, it suffices to show the same result for the source algebra $B = (\mathcal{O}Gb)_\gamma$. Moreover it suffices clearly to prove the result for $B/\mathfrak{p}B$. But this is precisely the statement 50.7 in the proof above. Of course this can also be deduced from the main result about the structure of B. □

We can also deduce the $\mathcal{O}$-algebra structure of the block algebra itself.

(50.9) COROLLARY. *Let b be a nilpotent block of $\mathcal{O}G$. Then, as an $\mathcal{O}$-algebra, $\mathcal{O}Gb$ is isomorphic to $T \otimes_{\mathcal{O}} OP$ for some $\mathcal{O}$-simple algebra T.*

Proof. Let α be the unique point of $\mathcal{O}Gb$ (Corollary 50.8). By Theorem 7.3, there exists an $\mathcal{O}$-simple subalgebra T of $\mathcal{O}Gb$ lifting the unique simple quotient $S(\alpha)$ of $\mathcal{O}Gb$. By Proposition 7.5, there is an isomorphism $\mathcal{O}Gb \cong T \otimes_{\mathcal{O}} C_{\mathcal{O}Gb}(T)$, and moreover $C_{\mathcal{O}Gb}(T) \cong e\mathcal{O}Gbe$ where $e \in \alpha$. Therefore $\mathcal{O}Gb \cong T \otimes_{\mathcal{O}} (\mathcal{O}Gb)_\alpha$ and it suffices to prove that the localization $(\mathcal{O}Gb)_\alpha$ is isomorphic to $\mathcal{O}P$.

Let P_γ be a defect of b, let $B = (\mathcal{O}Gb)_\gamma$ be a source algebra of b, and let $\mathcal{F}_\gamma : B \to \mathrm{Res}^G_P(\mathcal{O}Gb)$ be an embedding associated with γ. By Puig's theorem, $B \cong S \otimes_{\mathcal{O}} \mathcal{O}P$ for some $\mathcal{O}$-simple interior P-algebra S.

The unique point β of B is mapped to the unique point α of $\mathcal{O}Gb$ via the embedding $\mathcal{F}_\gamma$. Therefore the localization B_β is also the localization of $\mathcal{O}Gb$ with respect to α (Proposition 15.1). Thus it suffices to show that B_β is isomorphic to $\mathcal{O}P$.

Let i be a primitive idempotent of S. We have $iSi \cong \mathcal{O}$ (see Example 8.4). Now $i \otimes 1$ is a primitive idempotent of $S \otimes_{\mathcal{O}} \mathcal{O}P$, because it is mapped to i via the augmentation map $h_S : S \otimes_{\mathcal{O}} \mathcal{O}P \to S$ and $\mathrm{Ker}(h_S) \subseteq J(S \otimes_{\mathcal{O}} \mathcal{O}P)$ (see Lemma 50.2). Thus $i \otimes 1 \in \beta$ and so

$$B_\beta \cong (i \otimes 1)(S \otimes_{\mathcal{O}} \mathcal{O}P)(i \otimes 1) = iSi \otimes_{\mathcal{O}} \mathcal{O}P \cong \mathcal{O} \otimes_{\mathcal{O}} \mathcal{O}P \cong \mathcal{O}P\,,$$

as was to be shown. □

(50.10) REMARK. One can prove that the converse of Theorem 50.6 also holds: if B is a source algebra of a block b with defect group P and if B is isomorphic to $S \otimes_{\mathcal{O}} \mathcal{O}P$ (as interior P-algebras) for some $\mathcal{O}$-simple interior P-algebra S, then b is nilpotent. Forgetting about interior structures, there is the following open question: if $B \cong S \otimes_{\mathcal{O}} \mathcal{O}P$ as $\mathcal{O}$-algebras (or equivalently if $\mathcal{O}Gb \cong T \otimes_{\mathcal{O}} \mathcal{O}P$ for some $\mathcal{O}$-simple algebra T), is the block b nilpotent? The answer is positive if P is abelian or if G is p-soluble.

(50.11) REMARK. In view of Puig's finiteness conjecture 38.5, one expects that only finitely many Dade P-algebras S can appear in the description of a source algebra of nilpotent blocks with defect group P. This would be the case if one could prove that the order of S in the Dade group $\mathcal{D}_{\mathcal{O}}(P)$ is finite. Indeed since $\mathcal{D}_{\mathcal{O}}(P)$ is finitely generated (Remark 29.7), the torsion subgroup is finite, so that only finitely many primitive Dade P-algebras S have finite order. Thus the question is the following: if a source algebra of a nilpotent block is isomorphic to $S \otimes_{\mathcal{O}} \mathcal{O}P$, does the Dade P-algebra S have finite order in the Dade group $\mathcal{D}_{\mathcal{O}}(P)$? This question is still open.

Theorem 50.6 asserts only the existence of S and of an isomorphism $B \cong S \otimes_{\mathcal{O}} \mathcal{O}P$. We end this section with a discussion of uniqueness. The interior P-algebra S appearing in the description of B is clearly unique when we work over the field k, because S is the unique simple quotient of B. In general S is a lift to $\mathcal{O}$ of the unique simple quotient of $B/\mathfrak{p}B$ and is a primitive Dade P-algebra. Therefore by Corollary 29.5, the P-algebra structure of S is uniquely determined by that of $S/\mathfrak{p}S$, and consequently it is uniquely determined by B. However, if $S \cong \mathrm{End}_{\mathcal{O}}(L)$, the module structure of L (that is, the *interior* structure of S) is not unique: by Proposition 21.5 it can be modified by any group homomorphism $\lambda : P \to \mathcal{O}^*$. Another way of seeing this is the following. Given a group homomorphism $\lambda : P \to \mathcal{O}^*$, let us write $\mathcal{O}(\lambda)$ for the corresponding one-dimensional interior P-algebra. There is an isomorphism of interior P-algebras $\mathcal{O}(\lambda) \otimes_{\mathcal{O}} \mathcal{O}P \cong \mathcal{O}P$ (Exercise 50.3), so that

$$B \cong S \otimes_{\mathcal{O}} \mathcal{O}P \cong S \otimes_{\mathcal{O}} \mathcal{O}(\lambda) \otimes_{\mathcal{O}} \mathcal{O}P \cong \mathrm{End}_{\mathcal{O}}(L \otimes_{\mathcal{O}} \mathcal{O}(\lambda)) \otimes_{\mathcal{O}} \mathcal{O}P ,$$

where $\mathcal{O}(\lambda)$ is now viewed as a one-dimensional $\mathcal{O}P$-lattice. As a P-algebra, $\mathrm{End}_{\mathcal{O}}(L \otimes_{\mathcal{O}} \mathcal{O}(\lambda))$ is isomorphic to S, but its interior structure has been modified by λ. However, if we add the condition $\det(u{\cdot}1_S) = 1$ for all $u \in P$, then the interior P-algebra structure of S is uniquely determined (see Proposition 21.5 again). Thus we have proved the following result.

(50.12) PROPOSITION. *Let the interior P-algebra $B \cong S \otimes_{\mathcal{O}} \mathcal{O}P$ be a source algebra of a nilpotent block, where $S = \mathrm{End}_{\mathcal{O}}(L)$ and L is an indecomposable endo-permutation $\mathcal{O}P$-lattice with vertex P.*

(a) The interior P-algebra S can be chosen such that $\det(u{\cdot}1_S) = 1$ for all $u \in P$.

(b) If the condition of (a) is satisfied, then S is uniquely determined by B as an interior P-algebra (up to isomorphism). In other words, L is uniquely determined (up to isomorphism) as an indecomposable endo-permutation $\mathcal{O}P$-lattice of determinant one.

Another question is the uniqueness of the isomorphism. One can prove that any automorphism of the interior P-algebra $S \otimes_{\mathcal{O}} \mathcal{O}P$ is inner. Therefore the isomorphism $B \cong S \otimes_{\mathcal{O}} \mathcal{O}P$ is unique up to inner automorphisms. In other words the exo-isomorphism is unique.

(50.13) REMARK. Without the condition on the determinant, only the P-algebra structure of S is uniquely determined by B. Thus it may be desirable to have a description of B (as interior P-algebra) which only depends on the P-algebra structure of S. This is possible with the following construction, which extends the construction of group algebras. Let SP be the free S-module on P, endowed with the product defined by

$$(su){\cdot}(tv) = s\,{}^{u}t\,uv\,, \qquad s,t \in S,\ u,v \in P\,.$$

Then SP is an interior P-algebra (for the obvious map $P \to SP$) and the construction works for any P-algebra S. But in case S is interior for a group homomorphism $\rho : P \to S^*$, then there is an isomorphism

$$S \otimes_{\mathcal{O}} OP \longrightarrow SP\,, \qquad s \otimes u \mapsto s\rho(u)^{-1}u\,.$$

The proof that this is an isomorphism of interior P-algebras is left as an exercise. With this approach, the main theorem asserts that $B \cong SP$, for a uniquely determined Dade P-algebra S.

Exercises

(50.1) Prove that the Cartan matrix of a nilpotent block with defect group P is the 1×1-matrix with single entry equal to $|P|$.

(50.2) Let b be a nilpotent block with defect group P and let $\overline{b}$ be its image in kG. Prove that if P is cyclic, then $kG\overline{b}$ has $|P|$ indecomposable modules up to isomorphism. [Hint: Use part (b) of Exercise 17.2.]

(50.3) Let S be an interior G-algebra, given by a group homomorphism $\rho : G \to S^*$, and let SG be the interior G-algebra defined in Remark 50.13.
 (a) Prove that the map $S \otimes_{\mathcal{O}} \mathcal{O}G \longrightarrow SG$ given by $s \otimes g \mapsto s\rho(g)^{-1}g$ is an isomorphism of interior G-algebras.
 (b) Suppose that $S = \mathcal{O}$ as $\mathcal{O}$-algebras, so that $S = \mathcal{O}(\rho)$ as interior G-algebras. Deduce from (a) that $\mathcal{O}(\rho) \otimes_{\mathcal{O}} \mathcal{O}G \cong \mathcal{O}G$.

(50.4) The purpose of this exercise is to prove the Frobenius theorem about p-nilpotent groups (Theorem 49.7). We work over k and we let b be the principal block of kG. Let $\pi : kGb \to k$ be the surjection onto the trivial interior G-algebra k (which exists by definition of the principal block). Finally let $H = \mathrm{Ker}(G \to (kGb)^*)$, called the kernel of the block b.
 (a) Prove that H is a normal subgroup of G of order prime to p. [Hint: Observe that kGb is a projective kG-module (under left multiplication) and show that kGb is both projective and trivial on restriction to H.]
 (b) Assume that the trivial module is the unique simple module of the principal block b. Prove that for every $g \in G$, there exists an integer n such that $g^{p^n} \in H$. [Hint: Show that $\mathrm{Ker}(\pi)$ is a nilpotent ideal and that $(g-1)b \in \mathrm{Ker}(\pi)$. Deduce that $(g-1)^{p^n} b = 0$ for some n.]
 (c) If the trivial module is the unique simple module of the principal block b, prove that G is p-nilpotent.
 (d) Prove the Frobenius theorem: if $N_G(Q)/C_G(Q)$ is a p-group for every p-subgroup Q of G, then G is p-nilpotent.

Notes on Section 50

Puig's theorem is of course due to Puig [1988b]. The proof given here uses some simplifications due to Linckelmann. The facts and question mentioned in Remarks 50.10 and 50.13 can be found in Puig [1988b]. In fact Puig has recently found a positive answer to the question raised in Remark 50.10. The question appearing in Remark 50.11 is also due to Puig but does not appear in his paper. Puig's theorem has been extended by Külshammer and Puig [1990] to the situation of a block of G lying over a nilpotent block of a normal subgroup H of G (see also Linckelmann and Puig [1987] for the special and easier case where the order of the quotient group G/H is prime to p). Puig's theorem has also been extended by Fan [1994] to the case where the residue field k is not algebraically closed.

§ 51 LIFTING THEOREM FOR NILPOTENT BLOCKS

We prove Proposition 50.1, which was needed for the main result of the previous section and which remained to be proved in characteristic zero. The result is an immediate consequence of a lifting theorem, whose proof occupies the whole of this section.

We first explain the difficulty of the situation. Suppose that $\mathcal{O}$ is a discrete valuation ring of characteristic zero (satisfying Assumption 42.1). Let b be a nilpotent block of $\mathcal{O}G$, let $\overline{b}$ be its image in kG, and let the interior P-algebra B be a source algebra of b. Then $\overline{B} = B/\mathfrak{p}B$ is a source algebra of $\overline{b}$ and the description of $\overline{B}$ is complete by the main result of the previous section (which is proved over k). We have $\overline{B} \cong \overline{S} \otimes_k kP$ where $\overline{S} = \mathrm{End}_k(V)$ is the endomorphism algebra of an endo-permutation kP-module V. If we knew the existence of an endo-permutation $\mathcal{O}P$-lattice L such that $L/\mathfrak{p}L \cong V$, then $S \otimes_{\mathcal{O}} \mathcal{O}P$ would be an obvious candidate for B, where $S = \mathrm{End}_{\mathcal{O}}(L)$. In fact, under the assumption that L exists, the proof that $B \cong S \otimes_{\mathcal{O}} \mathcal{O}P$ is easy. Clearly $S \otimes_{\mathcal{O}} \mathcal{O}P$ has a P-invariant basis, because S has one (by definition of an endo-permutation lattice) and $\mathcal{O}P$ has one too. Therefore we can apply Proposition 38.8 and the fact that

$$(S \otimes_{\mathcal{O}} \mathcal{O}P)/\mathfrak{p}(S \otimes_{\mathcal{O}} \mathcal{O}P) \cong \overline{S} \otimes_k kP \cong \overline{B}$$

to deduce that $S \otimes_{\mathcal{O}} \mathcal{O}P \cong B$.

Thus the difficulty is to lift the endo-permutation kP-module V to an endo-permutation $\mathcal{O}P$-lattice L, or equivalently to lift the Dade P-algebra $\overline{S}$ over k to a Dade P-algebra S over $\mathcal{O}$. This amounts to the question of the surjectivity of the map of Dade groups $\mathcal{D}_{\mathcal{O}}(P) \to \mathcal{D}_k(P)$, an open problem already mentioned in Section 29. However, in some special cases where this surjectivity is known to hold, this discussion provides an easier proof of Puig's theorem in characteristic zero. This is the case when P is cyclic (Exercise 51.2), and more generally when P is abelian (see Remark 29.7).

We are going to prove that V can be lifted to an $\mathcal{O}P$-lattice L, but we shall not prove directly that L is an endo-permutation $\mathcal{O}P$-lattice, and so we shall not be in a situation where we can apply the argument above to deduce the structure of the source algebra B. We shall rather prove more precisely that V lifts to a B-lattice L (this is more precise than just an $\mathcal{O}P$-lattice), and this will prove Proposition 50.1. Then Theorem 50.6 gives the structure of B. Thus if we follow the logical thread of the whole proof, we have to use twice the entire argument of the previous section, first over k and then over $\mathcal{O}$.

We have already mentioned that the next result is a consequence of the main theorem of the previous section. But as this theorem is not completely proved yet, we have to provide a proof of the following facts.

(51.1) LEMMA. *Let b be a nilpotent block of $\mathcal{O}G$, let $\bar{b}$ be its image in kG, let P_γ be a defect of b, let $B = (\mathcal{O}Gb)_\gamma$ be a source algebra of b, and let $\overline{B} = B/\mathfrak{p}B$.*

- (a) *There is a unique point of B, thus a unique simple $\overline{B}$-module V up to isomorphism. Moreover p does not divide $\dim_k(V)$.*
- (b) *There is a unique point of $\mathcal{O}Gb$, thus a unique simple $kG\bar{b}$-module V' up to isomorphism.*
- (c) *More generally, for every p-subgroup Q of P, there is a unique local point $\delta \in \mathcal{LP}((\mathcal{O}Gb)^Q)$ such that $Q_\delta \leq P_\gamma$.*

Proof. By reduction modulo $\mathfrak{p}$, it suffices to prove the statements over k. But the main theorem of the previous section is already proved over k and therefore so are its consequences. Statement 50.7 yields (a), Theorem 49.15 (that is, Corollary 50.8) yields (b), while (c) is proved in Corollary 49.16. □

Note for completeness that V (viewed as a kP-module by restriction) is a source module of the simple $kG\bar{b}$-module V' (Exercise 51.3). We can now state the main result of this section.

(51.2) THEOREM. *Suppose that $\mathcal{O}$ is a discrete valuation ring of characteristic zero (satisfying Assumption 42.1). Let b be a nilpotent block of $\mathcal{O}G$, let $\bar{b}$ be its image in kG, let P_γ be a defect of b, let $B = (\mathcal{O}Gb)_\gamma$ be a source algebra of b, and let $\overline{B} = B/\mathfrak{p}B$.*

- (a) *Let V be the unique simple $\overline{B}$-module (up to isomorphism). There exists a B-lattice L such that $L/\mathfrak{p}L \cong V$.*
- (b) *Let V' be the unique simple $kG\bar{b}$-module (up to isomorphism). There exists an $\mathcal{O}Gb$-lattice L' such that $L'/\mathfrak{p}L' \cong V'$.*

We shall only have to prove one of the statements (a) or (b), because any one of them immediately implies the other one. Indeed $\mathcal{O}Gb$ and B are Morita equivalent, so that the existence of L implies the existence of its Morita correspondent L', and conversely.

We first show that this theorem implies Proposition 50.1.

Proof of Proposition 50.1 over $\mathcal{O}$. Let V and L be as in the theorem. It follows from Nakayama's lemma (see Proposition 1.3) that the structural map $B \to \mathrm{End}_{\mathcal{O}}(L)$ is surjective, since by reduction modulo $\mathfrak{p}$, this map yields the surjection $\overline{B} \to \mathrm{End}_k(V)$. Moreover $\dim_{\mathcal{O}}(L) = \dim_k(V)$ is prime to p . Thus $S = \mathrm{End}_{\mathcal{O}}(L)$ is an $\mathcal{O}$-simple quotient of B of dimension prime to p , as was to be shown. □

We now prepare the proof of Theorem 51.2. As mentioned in Example 2.2, there is, up to isomorphism, a unique absolutely unramified complete discrete valuation ring $\mathcal{O}_{\mathrm{un}}$ with residue field k . Any ring $\mathcal{O}$ satisfying Assumption 42.1 is (up to isomorphism) a totally ramified extension of $\mathcal{O}_{\mathrm{un}}$. Thus both $\mathcal{O}_{\mathrm{un}}$ and $\mathcal{O}$ have residue field k . We refer the reader to Serre [1962] for details. We identify $\mathcal{O}_{\mathrm{un}}$ with a subring of $\mathcal{O}$ and we let K_{un} and K be the fields of fractions of $\mathcal{O}_{\mathrm{un}}$ and $\mathcal{O}$ respectively, so that K is an extension of K_{un} .

By the theorem on lifting idempotents, the block $\overline{b}$ of kG can be lifted to a block b_{un} of $\mathcal{O}_{\mathrm{un}}G$. The idempotent b_{un} can be viewed as an idempotent in $(\mathcal{O}G)^G$, and it must be equal to b since both b_{un} and b map to $\overline{b}$ in kG . This shows that the block b of $\mathcal{O}G$ belongs in fact to $\mathcal{O}_{\mathrm{un}}G$, and so $\mathcal{O}Gb \cong \mathcal{O} \otimes_{\mathcal{O}_{\mathrm{un}}} \mathcal{O}_{\mathrm{un}}Gb$. The same argument applies with an idempotent i in a source point γ of b , and it follows that $i\mathcal{O}Gbi \cong \mathcal{O} \otimes_{\mathcal{O}_{\mathrm{un}}} i\mathcal{O}_{\mathrm{un}}Gbi$. Thus if $B_{\mathrm{un}} = (\mathcal{O}_{\mathrm{un}}Gb)_\gamma$ is a source algebra of $\mathcal{O}_{\mathrm{un}}Gb$, then γ is still a source point of $\mathcal{O}Gb$ and we obtain the following result.

(51.3) LEMMA. *Let* $B_{\mathrm{un}} = (\mathcal{O}_{\mathrm{un}}Gb)_\gamma$ *be a source algebra of* $\mathcal{O}_{\mathrm{un}}Gb$. *Then*

$$B = (\mathcal{O}Gb)_\gamma \cong \mathcal{O} \otimes_{\mathcal{O}_{\mathrm{un}}} B_{\mathrm{un}}$$

is a source algebra of $\mathcal{O}Gb$.

It follows immediately from this lemma that it suffices to prove Theorem 51.2 over $\mathcal{O}_{\mathrm{un}}$, and then apply scalar extension from $\mathcal{O}_{\mathrm{un}}$ to $\mathcal{O}$. However, the first step consists in proving the theorem over a suitable Galois extension of $\mathcal{O}_{\mathrm{un}}$, and then going down to $\mathcal{O}_{\mathrm{un}}$. We let K_{sp} be a finite extension of K_{un} such that $K_{\mathrm{sp}}G$ is split, and we let $\mathcal{O}_{\mathrm{sp}}$ be the integral closure of $\mathcal{O}_{\mathrm{un}}$ in K_{sp} . Thus $\mathcal{O}_{\mathrm{sp}}$ is again a ring satisfying Assumption 42.1. We can always enlarge K_{sp} and assume that it is a Galois extension of K_{un} . This will be needed later. By a theorem of Brauer, we can choose for K_{sp} the field $K(\zeta)$, where ζ is a primitive $|G|_p$-th root of unity, because then all $|G|$-th roots of unity belong to K_{sp} , but we do not need this explicit choice. We let also $B_{\mathrm{sp}} = \mathcal{O}_{\mathrm{sp}} \otimes_{\mathcal{O}_{\mathrm{un}}} B_{\mathrm{un}}$, and this a source algebra of $\mathcal{O}_{\mathrm{sp}}Gb$ by Lemma 51.3. Finally $\mathfrak{p}_{\mathrm{sp}}$ denotes the maximal ideal of $\mathcal{O}_{\mathrm{sp}}$.

We are going to use decomposition theory to prove Theorem 51.2 over $\mathcal{O}_{\rm sp}$, but we first need some preparation. The first lemma is a general result about characters.

(51.4) LEMMA. *Let U be a cyclic group and let χ be the ordinary character of a $K_{\rm sp}U$-module M. Then $\prod_u \chi(u)$ is a rational integer, where the product runs over the set of elements $u \in U$ such that u is a generator of U.*

Proof. Let $n = |U|$. Extending scalars to a larger field does not change characters. Thus we can assume that $K_{\rm sp}$ contains all n-th roots of unity. If ζ is a primitive n-th root of unity, then $\mathbb{Q}(\zeta) \subset K_{\rm sp}$, and for every integer m prime to n, we let α_m be the automorphism of $\mathbb{Q}(\zeta)$ mapping ζ to ζ^m. By elementary field theory, every α_m extends to a field automorphism of $K_{\rm sp}$, still written α_m. In a matrix representation of M, one can apply α_m to each entry of the matrices and obtain a new representation of the group U. The new $K_{\rm sp}U$-module obtained in this way is written ${}^{(\alpha_m)}M$ and is called a *Galois conjugate* of M (see before Lemma 51.11 for another definition, and see Exercise 51.1). If ${}^{(\alpha_m)}\chi$ denotes the character of ${}^{(\alpha_m)}M$, then clearly $({}^{(\alpha_m)}\chi)(u) = \alpha_m(\chi(u))$ for every $u \in U$.

Now $\chi(u)$ is the sum of the eigenvalues of the action of u on M, and each of them is an n-th root of unity (Lemma 42.7), hence a power of ζ. Moreover if ζ^r is an eigenvalue of the action of u, then ζ^{rm} is an eigenvalue of the action of u^m, and conversely. Since $\zeta^{rm} = \alpha_m(\zeta^r)$, it follows that $\alpha_m(\chi(u)) = \chi(u^m)$.

Let S be the set of integers m such that $1 \leq m < n$ and $(m,n) = 1$. On the one hand $\{\alpha_m \mid m \in S\}$ is the group of all automorphisms of $\mathbb{Q}(\zeta)$, that is, the Galois group $Gal(\mathbb{Q}(\zeta)/Q)$. On the other hand if u is a generator of U, then $\{u^m \mid m \in S\}$ is the set of all generators of U. Therefore the product of the statement is

$$\prod_{m \in S} \chi(u^m) = \prod_{m \in S} \alpha_m(\chi(u)),$$

and this is clearly invariant under $Gal(\mathbb{Q}(\zeta)/Q)$. Therefore this product lies in $\mathbb{Q}$, hence in $\mathbb{Z}$ since it is integral over $\mathbb{Z}$ (because any root of unity is integral over $\mathbb{Z}$). □

We need some information about ordinary characters of a nilpotent block b. Since we shall always consider characters of absolutely simple modules, we need to work over the splitting field $K_{\rm sp}$. The next result asserts the existence of an ordinary character of height zero, which was proved in Exercise 46.3. We provide here a slightly different proof.

(51.5) LEMMA. *Let b be a block of $\mathcal{O}_{\mathrm{sp}}G$ with defect P_γ and let $i \in \gamma$. There exists an irreducible ordinary character χ of G associated with b such that p does not divide the integer $\chi(i)$.*

Proof. For simplicity of notation, write $\mathcal{O} = \mathcal{O}_{\mathrm{sp}}$ and $K = K_{\mathrm{sp}}$. Let $B = i\mathcal{O}Gbi = (\mathcal{O}Gb)_\gamma$ and $\overline{B} = B/\mathfrak{p}B$. Since B and $\mathcal{O}Gb$ are Morita equivalent, there is, by Exercise 42.5, a commutative diagram of Grothendieck groups

$$\begin{array}{ccc} R(K \otimes_{\mathcal{O}} B) & \xrightarrow{\sim} & R(KGb) \\ \Big\downarrow d_B & & \Big\downarrow d_{\mathcal{O}Gb} \\ R(\overline{B}) & \xrightarrow{\sim} & R(kG\bar{b}) \end{array}$$

where d_B and $d_{\mathcal{O}Gb}$ denote the respective decomposition maps. By part (c) of Theorem 42.11, $d_{\mathcal{O}Gb}$ is surjective, and therefore so is d_B. By Proposition 44.9 or Corollary 46.16, there exists a simple $\overline{B}$-module V of dimension prime to p. By surjectivity of d_B, there exist integers $n_{[M]}$ such that

$$[V] = \sum_{[M]} n_{[M]}\, d_B([M]) \in R(\overline{B}),$$

where $[M]$ runs over the isomorphism classes of simple $K \otimes_{\mathcal{O}} B$-modules. Taking the dimension of modules induces group homomorphisms

$$\dim_K : R(K \otimes_{\mathcal{O}} B) \longrightarrow \mathbb{Z} \qquad \text{and} \qquad \dim_k : R(\overline{B}) \longrightarrow \mathbb{Z},$$

and we have $\dim_k(d_B([M])) = \dim_K([M])$ by the definition of the decomposition map. Therefore

$$\dim_k(V) = \sum_{[M]} n_{[M]} \dim_K(M).$$

Since p does not divide $\dim_k(V)$, there exists a simple $K \otimes_{\mathcal{O}} B$-module M such that p does not divide $\dim_K(M)$.

Let M' be the simple KGb-module corresponding to M via the Morita equivalence. From the proof of Theorem 9.9, we know that the Morita equivalence maps M' to $iKGb \otimes_{KGb} M' \cong iM'$. Thus $M \cong iM'$ and it follows that p does not divide $\dim_K(iM')$. If χ is the character of M' (an irreducible ordinary character), then

$$\begin{aligned} \dim_K(iM') &= \mathrm{tr}(1; iM') = \mathrm{tr}(i; iM') = \mathrm{tr}(i; iM' \oplus (1-i)M') \\ &= \mathrm{tr}(i; M') = \chi(i), \end{aligned}$$

because the action of i is the identity on iM' and zero on $(1-i)M'$. The result follows. □

Returning to a nilpotent block b with defect P_γ, we consider now local pointed elements on $\mathcal{O}Gb$. If u_δ is a local pointed element, then the multiplicity module $V(\delta)$ is a simple $kC_G(u)$-module, and we need the following fact about the modular characters of such modules.

(51.6) LEMMA. *Let b be a nilpotent block with defect P_γ, let $u \in P$, and let ϕ and ψ be two irreducible modular characters of $kC_G(u)$ associated with b. Then*

$$\frac{1}{|C_G(u)|} \sum_{s \in C_G(u)_{\text{reg}}} \phi(s)\psi(s^{-1}) = \begin{cases} |C_P(u)|^{-1} & \textit{if } \phi = \psi, \\ 0 & \textit{if } \phi \neq \psi. \end{cases}$$

Proof. If ϕ is the modular character of a simple $kC_G(u)$-module W, let Φ be the modular character of the projective cover P_W of W. By the orthogonality relations for modular characters (Proposition 42.9), we have

$$\frac{1}{|C_G(u)|} \sum_{s \in C_G(u)_{\text{reg}}} \Phi(s)\psi(s^{-1}) = \begin{cases} 1 & \text{if } \phi = \psi, \\ 0 & \text{if } \phi \neq \psi. \end{cases}$$

Since b is nilpotent, so is every Brauer correspondent e of b (Proposition 49.14). Thus if W belongs to a block e of $kC_G(u)$, then W is the unique simple module in e (Lemma 51.1). Therefore W is the only composition factor of P_W, and its multiplicity is the Cartan integer $c = c_{W,W}$ (the unique Cartan integer of the algebra $kC_G(u)e$). It follows that $\Phi = c\phi$ and so

$$\frac{1}{|C_G(u)|} \sum_{s \in C_G(u)_{\text{reg}}} \phi(s)\psi(s^{-1}) = \begin{cases} c^{-1} & \text{if } \phi = \psi, \\ 0 & \text{if } \phi \neq \psi. \end{cases}$$

It remains to prove that $c = |C_P(u)|$. By Proposition 43.12, c can be computed from a source algebra of b: it is equal to the corresponding Cartan integer of $\overline{(\mathcal{O}Gb)_\gamma}(<u>)$. But if $\bar{b}$ and $\bar{\gamma}$ are the images of b and γ in kG, then clearly $\overline{(\mathcal{O}Gb)_\gamma}(<u>) = \overline{(kG\bar{b})_{\bar{\gamma}}}(<u>)$. Since we already know the structure of the source algebra over k, we can compute $\overline{(kG\bar{b})_{\bar{\gamma}}}(<u>)$ and its (unique) Cartan integer.

By the main theorem of the previous section, we have an isomorphism $(kG\bar{b})_{\bar{\gamma}} \cong S \otimes_k kP$, where S is a simple P-algebra with a P-invariant basis. By Proposition 28.3, it follows that

$$\overline{(kG\bar{b})_{\bar{\gamma}}}(<u>) \;\cong\; \overline{S}(<u>) \otimes_k \overline{kP}(<u>) \;\cong\; \overline{S}(<u>) \otimes_k kC_P(<u>),$$

using also Proposition 37.5. By Theorem 28.6, $\overline{S}(<u>)$ is a simple algebra. Therefore $\overline{(kG\bar{b})_{\bar{\gamma}}}(<u>)$ is Morita equivalent to $kC_P(u)$ (Exercise 9.5).

Since Cartan integers are preserved by Morita equivalences, we are left with the computation of the (unique) Cartan integer of $kC_P(u)$. Now $C_P(u)$ is a p-group, so that by Proposition 21.1 the trivial module k is the only simple $kC_P(u)$-module, $kC_P(u)$ is its projective cover, and the multiplicity of k as a composition factor of $kC_P(u)$ is equal to $|C_P(u)|$. Thus the unique Cartan integer of $kC_P(u)$ is $c_{k,k} = |C_P(u)|$. This completes the proof that the Cartan integer c is equal to $|C_P(u)|$. □

After all these technical lemmas, we can start the proof of the main result.

Proof of Theorem 51.2 over $\mathcal{O}_{\rm sp}$. We consider the nilpotent block b of $\mathcal{O}_{\rm sp}G$ and its image $\bar{b}$ in kG. By Lemma 51.1, there is a unique simple $kG\bar{b}$-module V' (up to isomorphism) and we have to prove that V' lifts to an $\mathcal{O}_{\rm sp}Gb$-lattice L'. Let ϕ be the modular character of V', that is, the unique irreducible modular character associated with b. By definition of the decomposition map d, it suffices to prove the existence of an irreducible ordinary character χ associated with b such that the decomposition number $d(\chi,\phi)$ is equal to 1. Indeed the uniqueness of ϕ then implies $d(\chi) = d(\chi,\phi)\phi = \phi$, so that if M' is a simple $K_{\rm sp}Gb$-module with character χ (which exists because $K_{\rm sp}$ is a splitting field), there exists an $\mathcal{O}_{\rm sp}Gb$-lattice L' such that $K_{\rm sp} \otimes_{\mathcal{O}_{\rm sp}} L' \cong M'$ and $L'/\mathfrak{p}_{\rm sp}L' \cong V'$.

By Lemma 51.5, there exists an irreducible ordinary character χ associated with b such that $\chi(i)$ is not divisible by p, where $i \in \gamma$. For this choice of χ, we are going to show that $d(\chi,\phi) = 1$. The proof is based on the computation of the arithmetic and geometric means of the numbers $|\chi(u_\delta)|^2$.

By the orthogonality relations (Corollary 42.5), and by the unique decomposition of any $g \in G$ as a product of a p-element u and a p-regular element $s \in C_G(u)$, we have

$$1 = \frac{1}{|G|}\sum_{g\in G}\chi(g)\chi(g^{-1}) = \frac{1}{|G|}\sum_{u\in G_p}\ \sum_{s\in C_G(u)_{\rm reg}}\chi(us)\chi(u^{-1}s^{-1}),$$

where G_p denotes the set of all p-elements of G. By Brauer's second main Theorem 43.4, we obtain

$$\begin{aligned}1 &= \frac{1}{|G|}\sum_{u\in G_p}\ \sum_{s\in C_G(u)_{\rm reg}}\ \sum_{\delta,\varepsilon\in\mathcal{LP}((\mathcal{O}_{\rm sp}G)^{<u>})}\chi(u_\delta)\,\phi_\delta(s)\,\chi(u_\varepsilon^{-1})\,\phi_\varepsilon(s^{-1})\\ &= \frac{1}{|G|}\sum_{u\in G_p}\ \sum_{\delta,\varepsilon\in\mathcal{LP}((\mathcal{O}_{\rm sp}G)^{<u>})}\chi(u_\delta)\,\chi(u_\varepsilon^{-1})\,\Big(\sum_{s\in C_G(u)_{\rm reg}}\phi_\delta(s)\,\phi_\varepsilon(s^{-1})\Big).\end{aligned}$$

Note that u_ε^{-1} denotes the local pointed element $(u^{-1})_\varepsilon$, and this makes sense since $<u> = <u^{-1}>$. By Lemma 51.6, the inner sum is zero if $\delta \neq \varepsilon$, while if $\delta = \varepsilon$, it is equal to

$$\sum_{s \in C_G(u)_{\mathrm{reg}}} \phi_\delta(s)\, \phi_\delta(s^{-1}) = |C_G(u)| \cdot |C_P(u)|^{-1} .$$

Moreover the sum over p-elements u and local points δ can be rewritten as the sum over local pointed elements u_δ. It follows that

$$1 = \frac{1}{|G|} \sum_{u_\delta} \frac{|C_G(u)|}{|C_P(u)|}\, \chi(u_\delta)\, \chi(u_\delta^{-1}) ,$$

where u_δ runs over all local pointed elements associated with b. Now $\chi(u_\delta)$ is the character of a module evaluated at u (Lemma 43.1) and $\chi(u_\delta^{-1})$ is the character of the same module evaluated at u^{-1}. Moreover $\chi(u_\delta)$ is a complex number (a sum of roots of unity by Lemma 42.7) and $\chi(u_\delta^{-1})$ is its complex conjugate (the sum of the corresponding inverse roots of unity). Therefore $\chi(u_\delta)\, \chi(u_\delta^{-1}) = |\chi(u_\delta)|^2$. Now we rewrite the above sum as a sum over a set $\mathcal{S}$ of representatives of the G-conjugacy classes of local pointed elements. Since the stabilizer of u_δ for the conjugation action of G is equal to $C_G(u)$ (because $C_G(u)$ acts trivially on the points $\delta \in \mathcal{LP}((\mathcal{O}_{\mathrm{sp}}G)^{<u>})$), the orbit of u_δ has $|G : C_G(u)|$ elements. Thus we obtain

$$1 = \sum_{u_\delta \in \mathcal{S}} \frac{1}{|C_P(u)|}\, |\chi(u_\delta)|^2 .$$

Since every local pointed element is contained in a defect of b and since all defects are conjugate to P_γ, we can choose $\mathcal{S}$ such that $u_\delta \in P_\gamma$ for every $u_\delta \in \mathcal{S}$. But by the definition of a nilpotent block, any two G-conjugate local pointed elements contained in P_γ must be conjugate under P (because P controls fusion in $\mathcal{L}_G(b)_{\leq P_\gamma}$). Therefore $\mathcal{S}$ is also a set of representatives of the P-conjugacy classes of local pointed elements contained in P_γ. Rewriting the sum as a sum over all $u_\delta \in P_\gamma$, we have

$$1 = \sum_{u_\delta \in P_\gamma} \frac{1}{|P|}\, |\chi(u_\delta)|^2 ,$$

because $C_P(u)$ is the stabilizer of u_δ and its orbit has $|P : C_P(u)|$ elements. Finally for every $u \in P$, there is by Lemma 51.1 a unique local point δ such that $u_\delta \in P_\gamma$. If this unique local point is written $\delta(u)$, we have

$$1 = \frac{1}{|P|} \sum_{u \in P} |\chi(u_{\delta(u)})|^2 , \tag{51.7}$$

and this completes the computation of the arithmetic mean of the numbers $|\chi(u_{\delta(u)})|^2$.

Since, by the choice of χ, the integer $\chi(i)$ is prime to p, its image in k is non-zero and therefore $\chi(i) \in \mathcal{O}_{\rm sp}^*$. Now for every $u \in P$, $\chi(ui)$ is a sum of p^n-th roots of unity (for some n) and each such root of unity maps to 1_k by reduction modulo $\mathfrak{p}_{\rm sp}$. Thus $\chi(ui) \equiv \chi(i) \pmod{\mathfrak{p}_{\rm sp}}$ and so $\chi(ui) \neq 0$. Since $u_{\delta(u)}$ is the unique local pointed element such that $u_{\delta(u)} \in P_\gamma$, we have

$$i = r^P_{<u>}(i) = j_1 + \ldots + j_m + e\,,$$

where $j_r \in \delta(u)$ for $1 \leq r \leq m$, and where e is a sum of primitive idempotents belonging to non-local points of $(\mathcal{O}_{\rm sp}Gb)^{<u>}$. We have $\chi(ue) = 0$ by Proposition 43.3 and $\chi(uj_r) = \chi(u_{\delta(u)})$ for every r. Therefore $\chi(ui) = m\,\chi(u_{\delta(u)})$ and so $\chi(u_{\delta(u)}) \neq 0$.

For a fixed a cyclic subgroup U of P, let δ be the unique local point of $(\mathcal{O}_{\rm sp}Gb)^U$ such that $U_\delta \leq P_\gamma$, so that $\delta = \delta(u)$ for every u generating U. Since $\chi(u_\delta)$ is the evaluation at u of some character (Lemma 43.1), we can apply Lemma 51.4 to this character. Thus $\prod_u \chi(u_\delta)$ is a rational integer, where u runs over all elements of U such that $<u> = U$. Grouping the elements of P according to the cyclic subgroup they generate and applying this argument to each such subgroup, we deduce that $\prod_{u\in P} |\chi(u_{\delta(u)})|^2$ is a positive integer, hence ≥ 1. Therefore

$$\text{(51.8)} \qquad \Big(\prod_{u\in P} |\chi(u_{\delta(u)})|^2\Big)^{1/|P|} \;\geq\; 1\,.$$

This inequality is all we need concerning the geometric mean of the numbers $|\chi(u_{\delta(u)})|^2$.

A well-known result asserts that the geometric mean is always smaller than or equal to the arithmetic mean, with equality only when all the numbers are equal (see Hardy–Littlewood–Pólya [1952]). In our situation, the arithmetic mean 51.7 is equal to 1, while the geometric mean 51.8 is ≥ 1. It follows that all the numbers $|\chi(u_{\delta(u)})|^2$ are equal, and since their mean is 1, we have $|\chi(u_{\delta(u)})| = 1$ for every local pointed element $u_{\delta(u)}$. Thus all generalized decomposition numbers corresponding to the ordinary character χ have norm 1.

When $u = 1$, the unique point $\delta(1)$ corresponds to the unique modular character $\phi_{\delta(1)} = \phi$ and we obtain the ordinary decomposition number $\chi(1_{\delta(1)}) = d(\chi,\phi)$. Since an ordinary decomposition number is always a positive integer, we deduce that $d(\chi,\phi) = 1$, as was to be shown. □

Recall that we have chosen K_{sp} to be a Galois extension of K_{un} (such that $K_{\mathrm{sp}}Gb$ is split). Let H be the Galois group of the extension. Then $K_{\mathrm{sp}} \otimes_{\mathcal{O}_{\mathrm{sp}}} B_{\mathrm{sp}}$ is split too, because it is Morita equivalent to $K_{\mathrm{sp}}Gb$ (see Exercise 9.7). By Theorem 51.2 over $\mathcal{O}_{\mathrm{sp}}$, we have a B_{sp}-lattice L_{sp} lifting the unique simple module V for $B_{\mathrm{sp}}/\mathfrak{p}_{\mathrm{sp}}B_{\mathrm{sp}}$ (but L_{sp} is not necessarily unique). We want to show that L_{sp} can be realized over $\mathcal{O}_{\mathrm{un}}$, for a suitable choice of L_{sp}.

Since the dimension of L_{sp} is prime to p (because p does not divide $\dim_k(V)$), we can apply Proposition 21.5. Thus L_{sp} can be chosen such that its determinant is one on restriction to the action of P, and we now fix this choice of L_{sp}. Thus $\det(u{\cdot}1_{S_{\mathrm{sp}}}) = 1$ for every $u \in P$, where $S_{\mathrm{sp}} = \mathrm{End}_{\mathcal{O}_{\mathrm{sp}}}(L_{\mathrm{sp}})$. When S_{sp} is fixed as a P-algebra, then L_{sp} is unique (up to isomorphism) with the additional condition that its determinant is one. We wish to prove the stronger property that L_{sp} is the unique B_{sp}-lattice of determinant one which lifts V. One way would be to note that any $\mathcal{O}_{\mathrm{sp}}$-simple quotient of B_{sp} of dimension $\dim_k(V)$ lifts the simple quotient $\mathrm{End}_k(V)$ and is necessarily a Dade P-algebra (by the proof of Theorem 50.6), hence is uniquely determined (Corollary 29.5), proving the uniqueness of S_{sp}. This is essentially the approach used in Proposition 50.12. For the sake of variety, we give here a more elementary proof.

(51.9) LEMMA. *With the notation above, L_{sp} is (up to isomorphism) the unique B_{sp}-lattice of determinant one which lifts V. More precisely L_{sp} is (up to isomorphism) the unique B_{sp}-lattice of determinant one and dimension n, where $n = \dim_k(V)$.*

Proof. We have already proved Theorem 51.2 over $\mathcal{O}_{\mathrm{sp}}$ and this implies Proposition 50.1 (as we have seen at the beginning of this section). Since Proposition 50.1 implies the main structure theorem 50.6, we have

$$B_{\mathrm{sp}} \cong S_{\mathrm{sp}} \otimes_{\mathcal{O}_{\mathrm{sp}}} \mathcal{O}_{\mathrm{sp}}P\,.$$

Now by Exercise 9.5, $S_{\mathrm{sp}} \otimes_{\mathcal{O}_{\mathrm{sp}}} \mathcal{O}_{\mathrm{sp}}P$ is Morita equivalent to $\mathcal{O}_{\mathrm{sp}}P$, and for any $\mathcal{O}_{\mathrm{sp}}P$-module X, the $S_{\mathrm{sp}} \otimes_{\mathcal{O}_{\mathrm{sp}}} \mathcal{O}_{\mathrm{sp}}P$-module $L_{\mathrm{sp}} \otimes_{\mathcal{O}_{\mathrm{sp}}} X$ is its Morita correspondent. Therefore any $S_{\mathrm{sp}} \otimes_{\mathcal{O}_{\mathrm{sp}}} \mathcal{O}_{\mathrm{sp}}P$-lattice of dimension $n = \dim_k(V) = \dim_{\mathcal{O}_{\mathrm{sp}}}(L_{\mathrm{sp}})$ is isomorphic to $L_{\mathrm{sp}} \otimes_{\mathcal{O}_{\mathrm{sp}}} X$ for some one-dimensional $\mathcal{O}_{\mathrm{sp}}P$-lattice X. If X is given by a group homomorphism $\lambda : P \to \mathcal{O}^*$, then the determinant of u acting on $L_{\mathrm{sp}} \otimes_{\mathcal{O}_{\mathrm{sp}}} X$ is equal to $\lambda(u)^n$, because the determinant of L_{sp} is one. Since the dimension n is prime to p (Lemma 51.1), this determinant can be one only if $\lambda(u) = 1$, in which case X is trivial and $L_{\mathrm{sp}} \otimes_{\mathcal{O}_{\mathrm{sp}}} X \cong L_{\mathrm{sp}}$. This completes the proof. □

The proof of Theorem 51.2 over $\mathcal{O}_{\rm un}$ is based on a Galois descent from $\mathcal{O}_{\rm sp}$ to $\mathcal{O}_{\rm un}$. We need two lemmas.

(51.10) LEMMA. *Let D be a finite dimensional division algebra over the field $K_{\rm un}$. Then D is commutative, that is, D is a field.*

Proof. As in the case of field extensions, the discrete valuation of $K_{\rm un}$ extends uniquely to a discrete valuation v of D (see Reiner [1975], § 12). Let $\mathcal{O}_D$ be the valuation ring of v, that is, the subring of D consisting of all $a \in D$ such that $v(a) \geq 0$. Then $\mathcal{O}_D$ is a (not necessarily commutative) discrete valuation ring. Let Π be a generator of the maximal ideal of $\mathcal{O}_D$ consisting of all $a \in \mathcal{O}_D$ such that $v(a) > 0$. Similarly let π be a generator of the maximal ideal $\mathfrak{p}_{\rm un}$ of $\mathcal{O}_{\rm un}$. The quotient $\mathcal{O}_D/\Pi\mathcal{O}_D$ is a finite dimensional division algebra over $\mathcal{O}_{\rm un}/\pi\mathcal{O}_{\rm un} = k$. Since k is algebraically closed, we have $\mathcal{O}_D/\Pi\mathcal{O}_D = k$ (that is, the extension $D/K_{\rm un}$ is totally ramified). We denote by $\overline{a}$ the image of $a \in \mathcal{O}_D$ in the residue field k.

Let $a \in \mathcal{O}_D$. Since $\mathcal{O}_D$ and $\mathcal{O}_{\rm un}$ have the same residue field k, there exists $b_0 \in \mathcal{O}_{\rm un}$ such that $\overline{a} = \overline{b}_0$. Therefore $a - b_0 = \Pi a_1$ for a uniquely determined $a_1 \in \mathcal{O}_D$. Similarly there exists $b_1 \in \mathcal{O}_{\rm un}$ such that $\overline{a}_1 = \overline{b}_1$, and $a_1 - b_1 = \Pi a_2$ for a uniquely determined $a_2 \in \mathcal{O}_D$. Continuing in this way, we obtain a sequence of elements $b_r \in \mathcal{O}_{\rm un}$ such that

$$a \equiv b_0 + \Pi b_1 + \ldots + \Pi^r b_r \pmod{\Pi^{r+1}\mathcal{O}_D}\,.$$

This means that the Cauchy sequence $(b_0 + \Pi b_1 + \ldots + \Pi^r b_r)_{r \geq 0}$ converges to a and we can write a as an infinite series

$$a = b_0 + \Pi b_1 + \ldots + \Pi^r b_r + \ldots\,.$$

This shows that $\mathcal{O}_D$ is commutative, since it is the closure of the commutative subring generated by $\mathcal{O}_{\rm un}$ and Π. Therefore D is commutative, because it is generated by $\mathcal{O}_D$ and Π^{-1}. □

Let $F/K_{\rm un}$ be a Galois extension with Galois group H and let A be a finite dimensional $K_{\rm un}$-algebra. Then $F \otimes_{K_{\rm un}} A$ is a finite dimensional F-algebra and, for any A-module N, $F \otimes_{K_{\rm un}} N$ becomes an $F \otimes_{K_{\rm un}} A$-module. Also H acts on $F \otimes_{K_{\rm un}} A$ via $h(f \otimes a) = h(f) \otimes a$, for $h \in H$, $f \in F$ and $a \in A$. The action of h is a $K_{\rm un}$-algebra automorphism (but not an F-algebra automorphism). Note that the subalgebra of fixed elements $(F \otimes_{K_{\rm un}} A)^H$ is isomorphic to $K_{\rm un} \otimes_{K_{\rm un}} A \cong A$. For any $F \otimes_{K_{\rm un}} A$-module M, the *Galois conjugate* ${}^hM$ is obtained from M by restriction along h^{-1} (that is, ${}^hM = M$ as $K_{\rm un}$-vector space, and the action of $F \otimes_{K_{\rm un}} A$ is given by the automorphism h^{-1} followed by the old module structure of M).

(51.11) LEMMA. *Let* F *be a Galois extension of* K_{un} *with Galois group* H, *let* A *be a semi-simple* K_{un}*-algebra, and let* M *be a simple* $F \otimes_{K_{\mathrm{un}}} A$*-module. If* $M \cong {}^hM$ *for every* $h \in H$, *then there exists a simple* A*-module* N *such that* $F \otimes_{K_{\mathrm{un}}} N \cong M$.

Proof. Write $A \cong \prod_r A_r$ where each A_r is a simple K_{un}-algebra. Then $F \otimes_{K_{\mathrm{un}}} A \cong \prod_r F \otimes_{K_{\mathrm{un}}} A_r$, and since M is simple, it is a module over $F \otimes_{K_{\mathrm{un}}} A_r$ for some r, with zero action of the other factors. Therefore it suffices to prove the lemma when A is simple. Thus we can assume that $A = M_n(D)$ is a simple K_{un}-algebra, where D is a finite dimensional division algebra over K_{un}.

By Lemma 51.10, D is commutative and so $F \otimes_{K_{\mathrm{un}}} D$ is a product of fields, say $F \otimes_{K_{\mathrm{un}}} D \cong \prod_j D_j$. Explicitly, if $D \cong K_{\mathrm{un}}[X]/(f)$ for some irreducible polynomial f, then

$$F \otimes_{K_{\mathrm{un}}} D \;\cong\; F[X]/(f) \;\cong\; \prod_j F[X]/(f_j)\,,$$

where $f = \prod_j f_j$ is the decomposition of f as a product of irreducible polynomials over F. Note that the second isomorphism holds because the f_j's are pairwise coprime, since an irreducible polynomial in characteristic zero is separable. Note also that the separability of field extensions in characteristic zero implies that D is generated by a single element over K_{un}, hence is indeed isomorphic to $K_{\mathrm{un}}[X]/(f)$ for some f. We let $1_D = \sum_j e_j$ be the idempotent decomposition corresponding to the product decomposition $F \otimes_{K_{\mathrm{un}}} D \cong \prod_j D_j$.

The action of the Galois group H on $F \otimes_{K_{\mathrm{un}}} D$ necessarily permutes the factors D_j (hence the corresponding idempotents e_j), and this permutation is transitive. Indeed if e is the sum of all idempotents e_j in some H-orbit, then

$$e \in (F \otimes_{K_{\mathrm{un}}} D)^H = K_{\mathrm{un}} \otimes_{K_{\mathrm{un}}} D \cong D\,,$$

forcing $e = 1$ since D has no non-trivial idempotent. This means that all e_j's belong to this H-orbit, proving the transitivity.

Now we have

$$\begin{aligned} F \otimes_{K_{\mathrm{un}}} A \;&=\; F \otimes_{K_{\mathrm{un}}} M_n(D) \;\cong\; M_n(F \otimes_{K_{\mathrm{un}}} D) \\ &=\; M_n\big(\prod_j D_j\big) \;\cong\; \prod_j M_n(D_j) \end{aligned}$$

and clearly H again transitively permutes the factors of this product. In fact $1 = \sum_j e_j$ is again the idempotent decomposition corresponding to the product decomposition of $F \otimes_{K_{\mathrm{un}}} M_n(D)$. By assumption, M is a simple $F \otimes_{K_{\rm un}} A$-module, hence a simple $M_n(D_j)$-module for some j, with zero action of the other factors. Thus M is characterized by the fact that e_j acts as the identity on M and $e_{j'}$ annihilates M for $j' \neq j$.

Let $M_n(D_{j'})$ be any factor of $F \otimes_{K_{\rm un}} A$. By transitivity, there exists $h \in H$ such that $e_{j'} = h(e_j)$. If M' is a simple $M_n(D_{j'})$-module (unique up to isomorphism), then $e_{j'}$ acts as the identity on M'. It follows that ${}^hM \cong M'$, because the action of $e_{j'}$ on ${}^hM$ is equal to the action of $h^{-1}(e_{j'}) = e_j$ on M, and this is the identity. But since $M \cong {}^hM$ by assumption, we have $M \cong M'$, hence $e_j = e_{j'}$. Since j' was arbitrary, this shows that there is a single factor in the above product. Thus $F \otimes_{K_{\rm un}} D$ remains a field after scalar extension, and $F \otimes_{K_{\rm un}} M_n(D) \cong M_n(F \otimes_{K_{\rm un}} D)$ remains a matrix algebra. It is now clear that if N is a simple $M_n(D)$-module, then $F \otimes_{K_{\rm un}} N$ remains a simple $F \otimes_{K_{\rm un}} M_n(D)$-module. Therefore, since there is a unique simple module up to isomorphism, we obtain $F \otimes_{K_{\rm un}} N \cong M$, as was to be shown. □

Now we can prove Theorem 51.2 over $\mathcal{O}_{\rm un}$. In fact we are going to establish a more precise result, but we first recall the notation. Let b be a nilpotent block of $\mathcal{O}_{\rm un}G$, let the interior P-algebra $B_{\rm un}$ be a source algebra of b, let $\overline{B} = B_{\rm un}/\mathfrak{p}_{\rm un}B_{\rm un}$, and let V be the unique simple $\overline{B}$-module (up to isomorphism). Let $K_{\rm sp}$ be a Galois extension of $K_{\rm un}$ such that $K_{\rm sp}Gb$ is split, let $\mathcal{O}_{\rm sp}$ be the integral closure of $\mathcal{O}_{\rm un}$ in $K_{\rm sp}$, let $B_{\rm sp} = \mathcal{O}_{\rm sp} \otimes_{\mathcal{O}_{\rm un}} B_{\rm un}$ be a source algebra of b (viewed as a block of $\mathcal{O}_{\rm sp}G$, see Lemma 51.3), and let $L_{\rm sp}$ be the unique $B_{\rm sp}$-lattice of determinant one which lifts V. Note that since $\mathcal{O}_{\rm sp}/\mathfrak{p}_{\rm sp} \cong \mathcal{O}_{\rm un}/\mathfrak{p}_{\rm un} \cong k$ (totally ramified extension), we have $B_{\rm sp}/\mathfrak{p}_{\rm sp}B_{\rm sp} \cong B_{\rm un}/\mathfrak{p}_{\rm un}B_{\rm un} = \overline{B}$.

(51.12) PROPOSITION. *With the notation above, let $L_{\rm sp}$ be the unique $B_{\rm sp}$-lattice of determinant one which lifts V. There exists a $B_{\rm un}$-lattice $L_{\rm un}$ such that $B_{\rm sp} \otimes_{\mathcal{O}_{\rm un}} L_{\rm un} \cong L_{\rm sp}$. Moreover $L_{\rm un}$ is a $B_{\rm un}$-lattice of determinant one which lifts V and is the unique $B_{\rm un}$-lattice (up to isomorphism) with this property.*

Proof. Let $n = \dim_k(V) = \dim_{\mathcal{O}_{\rm sp}}(L_{\rm sp})$. Let H be the Galois group of the extension $K_{\rm sp}$ of $K_{\rm un}$. The group H acts on the ring $\mathcal{O}_{\rm sp}$, hence also on $B_{\rm sp} = \mathcal{O}_{\rm sp} \otimes_{\mathcal{O}_{\rm un}} B_{\rm un}$. Any Galois conjugate of $L_{\rm sp}$ is again a $B_{\rm sp}$-lattice of dimension n, and moreover it also has determinant one (Exercise 51.1). Therefore, by the uniqueness of $L_{\rm sp}$ (Lemma 51.9), any Galois conjugate of $L_{\rm sp}$ is isomorphic to $L_{\rm sp}$.

In the sequel, we shall freely use the following fact (see Exercise 42.5): for every $K_{\rm sp} \otimes_{\mathcal{O}_{\rm sp}} B_{\rm sp}$-module N, there exists a $B_{\rm sp}$-lattice N_0 such that $K_{\rm sp}\otimes_{\mathcal{O}_{\rm sp}} N_0 \cong N$. We first prove that the $K_{\rm sp}\otimes_{\mathcal{O}_{\rm sp}} B_{\rm sp}$-module $M_{\rm sp}=K_{\rm sp}\otimes_{\mathcal{O}_{\rm sp}} L_{\rm sp}$ is simple. Note that

$$\dim_{K_{\rm sp}}(M_{\rm sp})=\dim_{\mathcal{O}_{\rm sp}}(L_{\rm sp})=\dim_k(V)=n\,.$$

On the other hand the dimension of any $\overline{B}$-module is a multiple of n because V is the unique simple $\overline{B}$-module. If N is a non-zero submodule of $M_{\rm sp}$ and if N_0 is as above, then $N_0/\mathfrak{p}_{\rm sp}N_0$ has dimension $\leq n$, thus equal to n, forcing $\dim_{K_{\rm sp}}(N)=n$ and $N=M_{\rm sp}$. Alternatively, the simplicity of $M_{\rm sp}$ follows from the definition of the decomposition map (Exercise 42.5) and the fact that the decomposition of $M_{\rm sp}$ is the simple module V.

The $K_{\rm un}$-algebra $K_{\rm un}\otimes_{\mathcal{O}_{\rm un}} B_{\rm un}$ is semi-simple, because it is Morita equivalent to $K_{\rm un}Gb$ (Exercise 9.7) and $K_{\rm un}Gb$ is semi-simple (Exercise 17.6). Now $M_{\rm sp}$ is a simple module for the extended algebra

$$K_{\rm sp}\otimes_{K_{\rm un}}(K_{\rm un}\otimes_{\mathcal{O}_{\rm un}} B_{\rm un})\cong K_{\rm sp}\otimes_{\mathcal{O}_{\rm sp}}\mathcal{O}_{\rm sp}\otimes_{\mathcal{O}_{\rm un}} B_{\rm un}\cong K_{\rm sp}\otimes_{\mathcal{O}_{\rm sp}} B_{\rm sp}\,.$$

Since $L_{\rm sp}$ is isomorphic to its Galois conjugates, so is $M_{\rm sp}$. Therefore, by Lemma 51.11, there exists a $K_{\rm un}\otimes_{\mathcal{O}_{\rm un}} B_{\rm un}$-module $M_{\rm un}$ such that $K_{\rm sp}\otimes_{K_{\rm un}} M_{\rm un}\cong M_{\rm sp}$.

Now let $L_{\rm un}$ be any $B_{\rm un}$-lattice such that $K_{\rm un}\otimes_{\mathcal{O}_{\rm un}} L_{\rm un}\cong M_{\rm un}$. Clearly $L_{\rm un}$ has dimension n and determinant one, because these properties of $L_{\rm sp}$ are inherited by $M_{\rm sp}$, $M_{\rm un}$ and $L_{\rm un}$. Therefore we have $\mathcal{O}_{\rm sp}\otimes_{\mathcal{O}_{\rm un}} L_{\rm un}\cong L_{\rm sp}$ by the uniqueness of $L_{\rm sp}$ (Lemma 51.9). Moreover $L_{\rm un}/\mathfrak{p}_{\rm un}L_{\rm un}$ is a $\overline{B}$-module of dimension n, hence isomorphic to V. Alternatively, since $\mathcal{O}_{\rm sp}$ is a totally ramified extension of $\mathcal{O}_{\rm un}$, we have $L_{\rm un}/\mathfrak{p}_{\rm un}L_{\rm un}\cong L_{\rm sp}/\mathfrak{p}_{\rm sp}L_{\rm sp}\cong V$.

Finally the uniqueness of $L_{\rm un}$ follows from that of $L_{\rm sp}$. Indeed if $L'_{\rm un}$ is a $B_{\rm un}$-lattice of dimension n and determinant one, then we have $\mathcal{O}_{\rm sp}\otimes_{\mathcal{O}_{\rm un}} L'_{\rm un}\cong L_{\rm sp}$ by the uniqueness of $L_{\rm sp}$. Now we view all $B_{\rm sp}$-lattices as $B_{\rm un}$-lattices by restriction of scalars (denoted by $\mathrm{Res}_{\mathcal{O}_{\rm un}}$), and we have

$$\mathrm{Res}_{\mathcal{O}_{\rm un}}(\mathcal{O}_{\rm sp}\otimes_{\mathcal{O}_{\rm un}} L'_{\rm un})\cong \mathrm{Res}_{\mathcal{O}_{\rm un}}(L_{\rm sp})\cong \mathrm{Res}_{\mathcal{O}_{\rm un}}(\mathcal{O}_{\rm sp}\otimes_{\mathcal{O}_{\rm un}} L_{\rm un})\,.$$

Since $\mathcal{O}_{\rm sp}$ is a torsion-free $\mathcal{O}_{\rm un}$-module and since $\mathcal{O}_{\rm un}$ is a principal ideal domain, $\mathcal{O}_{\rm sp}$ is a free $\mathcal{O}_{\rm un}$-module (Proposition 1.5) and its dimension is $m=[K_{\rm sp}:K_{\rm un}]$. The $B_{\rm un}$-lattice $\mathrm{Res}_{\mathcal{O}_{\rm un}}(\mathcal{O}_{\rm sp}\otimes_{\mathcal{O}_{\rm un}} L_{\rm un})$ is therefore isomorphic to the direct sum of m copies of $L_{\rm un}$, and similarly with $L'_{\rm un}$. By the Krull–Schmidt theorem, it follows that $L_{\rm un}\cong L'_{\rm un}$. This completes the proof of the proposition. □

In particular, this proposition proves Theorem 51.2 over $\mathcal{O}_{\mathrm{un}}$. We have already mentioned that this implies the result over $\mathcal{O}$, because $\mathcal{O}$ is an extension of $\mathcal{O}_{\mathrm{un}}$. Therefore the proof of Theorem 51.2 is now complete. This theorem in turn implies Proposition 50.1 and hence Theorem 50.6. Thus we have now completed the proof of Puig's theorem in characteristic zero.

Exercises

(51.1) Let L be an $\mathcal{O}G$-lattice of dimension n and let h be a Galois automorphism of $\mathcal{O}$.

(a) Let $\rho : G \to GL_n(\mathcal{O})$ be a representation of G affording L relative to some $\mathcal{O}$-basis of L . By making h act on each matrix coefficient, h induces an automorphism $\widetilde{h}$ of $GL_n(\mathcal{O})$. Prove that the representation $\widetilde{h}\,\rho$ affords the $\mathcal{O}G$-lattice ${}^hL$, the Galois conjugate of L .

(b) Deduce from (a) that if L has determinant one, then so does ${}^hL$.

(51.2) Let b be a nilpotent block with a cyclic defect group P . Let the interior P-algebra B be a source algebra of b , let $\overline{B} = B/\mathfrak{p}B$, and let V be the unique simple $\overline{B}$-module (up to isomorphism). By Theorem 50.6 over k , $\mathrm{Res}_P(V)$ is known to be an endo-permutation kP-module.

(a) Prove directly that V can be lifted to an $\mathcal{O}P$-lattice L . [Hint: Use Exercise 28.3 and the fact that, for every p-group Q , the indecomposable kQ-module of dimension $|Q| - 1$ always lift to $\mathcal{O}$, namely to the augmentation ideal of $\mathcal{O}Q$.]

(b) Prove that the structure of B can be directly deduced from the structure of $\overline{B}$. [Hint: Use (a) and Proposition 38.8.]

(51.3) Let the interior P-algebra B be a source algebra of a nilpotent block b , let $\overline{B} = B/\mathfrak{p}B$, and let V be the unique simple $\overline{B}$-module (up to isomorphism). Prove that the unique simple $kG\bar{b}$-module V' (up to isomorphism) has vertex P and source $\mathrm{Res}_P(V)$. [Hint: Use Proposition 38.3.]

Notes on Section 51

Theorem 51.2 is due to Puig [1988b]. We have followed his proof, except for some simplifications in the Galois descent from K_{sp} to K_{un} .

§ 52 THE ORDINARY CHARACTERS OF A NILPOTENT BLOCK

The generalized decomposition numbers of a nilpotent block b can be described in detail, using the structure of a source algebra of b. This is used to give explicit formulas for the values of the ordinary characters of b. Throughout this section, $\mathcal{O}$ denotes a discrete valuation ring of characterirstic zero (satisfying Assumption 42.1), and K denotes the field of fractions of $\mathcal{O}$.

For the rest of this section, we fix the following notation. Let b be a nilpotent block of $\mathcal{O}G$ with defect P_γ and let $B = (\mathcal{O}Gb)_\gamma$ be a source algebra of b. By Theorem 50.6, we have $B \cong S \otimes_{\mathcal{O}} \mathcal{O}P$, where $S = \mathrm{End}_{\mathcal{O}}(L)$ is the endomorphism algebra of an indecomposable endo-permutation $\mathcal{O}P$-lattice L with vertex P. By Proposition 50.12, we can assume that the determinant of L is one, in which case L is uniquely determined. We make this choice throughout this section. We want to compute the generalized decomposition numbers of b. By Proposition 43.10, they are equal to the numbers $\chi(u_\delta)$, where χ is an ordinary character of $K \otimes_{\mathcal{O}} B$ and u_δ is a local pointed element on B. The main ingredient is the computation of the values of the character of the $\mathcal{O}P$-lattice L.

Let ρ_L be the ordinary character of the $\mathcal{O}P$-lattice L. A crucial fact is that the values of ρ_L on elements of P are always rational integers. This will be a consequence of the following result. Recall that there is, up to isomorphism, a unique absolutely unramified complete discrete valuation ring $\mathcal{O}_{\mathrm{un}}$ of characteristic zero with residue field k. Moreover $\mathcal{O}_{\mathrm{un}}$ is isomorphic to a subring of $\mathcal{O}$.

(52.1) LEMMA. *Let $\mathcal{O}_{\mathrm{un}}$ be as above and let ζ be a p^n-th root of unity (for some integer $n \geq 1$). Then $\mathcal{O}_{\mathrm{un}} \cap \mathbb{Z}[\zeta] = \mathbb{Z}$ (the intersection taking place in $\mathcal{O}_{\mathrm{un}}[\zeta]$).*

Proof. The cyclotomic polynomial

$$f(t) = t^{p^{n-1}(p-1)} + t^{p^{n-1}(p-2)} + \ldots + t^{p^{n-1}} + 1$$

is the minimal polynomial of ζ over $\mathbb{Q}$ (see Ribenboim [1972]). We want to show that $f(t)$ remains irreducible over K_{un} (where K_{un} is the field of fractions of $\mathcal{O}_{\mathrm{un}}$). The degree of the extension $K_{\mathrm{un}}[\zeta]/K_{\mathrm{un}}$ is at most $\phi(p^n)$, where $\phi(p^n) = p^{n-1}(p-1)$ is the Euler function of p^n (because the minimal polynomial of ζ divides $f(t)$). Now it is well known that there exists an invertible element $a \in \mathbb{Z}[\zeta]^*$ such that $p = a(1-\zeta)^{\phi(p^n)}$ (see Ribenboim [1972], Chapter 10, Proposition 3A). By definition of $\mathcal{O}_{\mathrm{un}}$, the maximal ideal of $\mathcal{O}_{\mathrm{un}}$ is generated by p. If $\mathcal{O}'$ denotes the integral closure of $\mathcal{O}_{\mathrm{un}}$ in $K_{\mathrm{un}}[\zeta]$ (in fact $\mathcal{O}' = \mathcal{O}_{\mathrm{un}}[\zeta]$), and if π is a generator of the maximal ideal of $\mathcal{O}'$, then $1-\zeta = b\pi^m$ for some invertible element b and some integer $m \geq 1$. Therefore $p = c\pi^{m\phi(p^n)}$ for some invertible element c, and this shows that the ramification index of the extension $K_{\mathrm{un}}[\zeta]/K_{\mathrm{un}}$ is equal to $m\,\phi(p^n)$. But the ramification index is always bounded by the degree $[K_{\mathrm{un}}[\zeta] : K_{\mathrm{un}}]$ of the extension (in fact they are equal for a totally ramified extension). Therefore

$$m\,\phi(p^n) \leq [K_{\mathrm{un}}[\zeta] : K_{\mathrm{un}}] \leq \phi(p^n)\,,$$

forcing $m = 1$ and $[K_{\mathrm{un}}[\zeta] : K_{\mathrm{un}}] = \phi(p^n)$. This last equation means that $f(t)$ remains the minimal polynomial of ζ over K_{un}.

Now $\mathcal{O}_{\mathrm{un}}[\zeta] \cong \mathcal{O}_{\mathrm{un}}[t]/(f(t))$ is a free $\mathcal{O}_{\mathrm{un}}$-module of dimension $\phi(p^n)$. Therefore

$$\{1, \zeta, \zeta^2, \ldots, \zeta^{\phi(p^n)-1}\}$$

is a basis of both $\mathbb{Z}[\zeta]$ over $\mathbb{Z}$ and $\mathcal{O}_{\mathrm{un}}[\zeta]$ over $\mathcal{O}_{\mathrm{un}}$. It follows immediately that $\mathcal{O}_{\mathrm{un}} \cap \mathbb{Z}[\zeta] = \mathbb{Z}$. □

(52.2) COROLLARY. *The character ρ_L of the $\mathcal{O}P$-lattice L has values in $\mathbb{Z}$ on elements of P.*

Proof. By Proposition 51.12, L can be realized over $\mathcal{O}_{\mathrm{un}}$, using the fact that the determinant of L is one. Therefore ρ_L has values in $\mathcal{O}_{\mathrm{un}}$. On the other hand $\rho_L(u)$ is a sum of $|P|$-th roots of unity for every $u \in P$, hence belongs to $\mathbb{Z}[\zeta]$, where ζ is a primitive $|P|$-th root of unity. Thus $\rho_L(u) \in \mathcal{O}_{\mathrm{un}} \cap \mathbb{Z}[\zeta] = \mathbb{Z}$, by Lemma 52.1. □

We state our next result for the character ρ_N of an arbitrary endo-permutation $\mathcal{O}P$-lattice N. First we extend the function ρ_N to a function defined on the whole of $T = \mathrm{End}_{\mathcal{O}}(N)$, namely $\rho_N(a) = \mathrm{tr}(a; N)$ for every $a \in T$. If u_δ is a local pointed element on T, we define $\rho_N(u_\delta) = \rho_N(uj)$ where $j \in \delta$. Since a character is constant on a conjugacy class, this definition is independent of the choice of j in δ. This is analogous to the definition of generalized decomposition numbers, except that we are now considering local pointed elements on a P-algebra which is not a group algebra (we have already done so with source algebras, see Proposition 43.10). Recall that for every subgroup Q of P, either $\overline{T}(Q) = 0$ or there is exactly one local point δ of T^Q (Proposition 28.8). When N is indecomposable with vertex P (and this is the case for L), then only the second possibility occurs.

(52.3) PROPOSITION. *Let N be an endo-permutation $\mathcal{O}P$-lattice, let $T = \mathrm{End}_{\mathcal{O}}(N)$, and assume that the character ρ_N has values in $\mathbb{Z}$ on elements of P.*

(a) *For every local pointed element u_ε on T, we have $\rho_N(u_\varepsilon) = \pm 1$.*

(b) *Let $u \in P$ be such that $\overline{T}(<u>) \neq 0$, let ε be the unique local point of $T^{<u>}$, and let m_ε be the multiplicity of ε. Then we have $\rho_N(u) = \rho_N(u_\varepsilon)m_\varepsilon = \pm m_\varepsilon$.*

Proof. By Exercise 10.6, the $\mathcal{O}P$-module structure of T (for the conjugation action of P) is isomorphic to $T \cong N^* \otimes_{\mathcal{O}} N$. If $u \in P$, then by Exercise 42.1, $\rho_{N^*}(u) = \overline{\rho_N(u)}$ (the complex conjugate), and therefore $\rho_{N^*}(u) = \rho_N(u)$ since $\rho_N(u) \in \mathbb{Z}$ by assumption. Therefore we have

$$\rho_T(u) = \rho_{N^*}(u)\rho_N(u) = \rho_N(u)^2 .$$

On the other hand T is a permutation $\mathcal{O}P$-lattice by definition of an endo-permutation lattice. If X is a P-invariant basis of T, then, with respect to this basis, the matrix of the action of u has a diagonal entry 1 for each $x \in X^{<u>}$, and all the other diagonal entries are zero (because the other basis elements are permuted non-trivially). Therefore $\rho_T(u) = |X^{<u>}|$, the number of fixed elements.

Now $br_P(X^{<u>})$ is a basis of $\overline{T}(<u>)$ (Proposition 27.6), and therefore $|X^{<u>}| = \dim_k(\overline{T}(<u>))$. Moreover by Proposition 28.8, $\overline{T}(<u>)$ is a simple algebra and is the multiplicity algebra of the unique local point ε of $T^{<u>}$. Thus its dimension is m_ε^2. Summarizing all these equalities, we have

$$\rho_N(u)^2 = \rho_T(u) = |X^{<u>}| = \dim_k(\overline{T}(<u>)) = m_\varepsilon^2 ,$$

and it follows that $\rho_N(u) = \pm m_\varepsilon$.

By definition of the multiplicity m_ε, there exists an orthogonal decomposition $1_T = (\sum_{r=1}^{m_\varepsilon} j_r) + e$, where $j_r \in \varepsilon$ for each r, and where e is a sum of idempotents belonging to points ε' of $T^{<u>}$ distinct from ε. Since each such point ε' is not local by the uniqueness of ε, we have $\rho_N(uj) = 0$ for every $j \in \varepsilon'$. Indeed this follows from the argument of Proposition 43.3, which applies without change to our situation, namely to local pointed elements on T rather than local pointed elements on $\mathcal{O}G$ (Exercise 52.1). It follows that $\rho_N(ue) = 0$. Therefore

$$\rho_N(u) = \rho_N(u{\cdot}1_T) = \Big(\sum_{r=1}^{m_\varepsilon} \rho_N(uj_r)\Big) + \rho_N(ue) = m_\varepsilon{\cdot}\rho_N(u_\varepsilon) .$$

Since we have seen above that $\rho_N(u) = \pm m_\varepsilon$, we have $\rho_N(u_\varepsilon) = \pm 1$ and the proof is complete. □

(52.4) REMARK. The assumption that the character values are integers can always be satisfied, provided N is replaced by $N \otimes_{\mathcal{O}} \mathcal{O}(\lambda)$, where $\mathcal{O}(\lambda)$ is some one-dimensional representation given by a group homomorphism $\lambda : P \to \mathcal{O}^*$. If T is any Dade P-algebra, we know that there exist several interior P-algebra structures on T, corresponding to endo-permutation modules which only differ by a one-dimensional character $\lambda : P \to \mathcal{O}^*$ (Propositions 21.5 and 28.12). It can be shown that there is always one of these structures which yields an $\mathcal{O}P$-lattice having an integral valued character.

We return to the situation of a nilpotent block b and its source algebra $B \cong S \otimes_{\mathcal{O}} \mathcal{O}P$. We first need to understand better the pointed groups on $S \otimes_{\mathcal{O}} \mathcal{O}P$.

(52.5) LEMMA. *Let $s : S \to S \otimes_{\mathcal{O}} \mathcal{O}P$ be the homomorphism of P-algebras defined by $s(a) = a \otimes 1_{\mathcal{O}P}$. Then s induces an order preserving bijection between the set of pointed groups on S and the set of pointed groups on $S \otimes_{\mathcal{O}} \mathcal{O}P$. Moreover a pointed group on S is local if and only if its image is local.*

Proof. By Lemma 50.2 and its proof, the augmentation homomorphism $h_S : S \otimes_{\mathcal{O}} \mathcal{O}P \to S$ is a strict covering homomorphism, and s is a section of h_S (only as a P-algebra, not with respect to the interior structure). Therefore h_S induces an order preserving bijection between the set of pointed groups on $S \otimes_{\mathcal{O}} \mathcal{O}P$ and the set of pointed groups on S. This forces s to induce the inverse bijection. Indeed let j be a primitive idempotent of S^Q (for some subgroup Q), and choose a primitive decomposition $s(j) = \sum_i i$ in $(S \otimes_{\mathcal{O}} \mathcal{O}P)^Q$. Then each i maps via h_S to a primitive idempotent of S^Q (because h_S is a strict covering homomorphism), and therefore $j = h_S s(j) = \sum_i h_S(i)$ is a primitive decomposition in S^Q. Since j is primitive, there is only one term in the sum, showing that $s(j)$ is primitive in $(S \otimes_{\mathcal{O}} \mathcal{O}P)^Q$. Thus s induces a map between pointed groups. Clearly this map can only be the inverse of the map induced by h_S. The additional statements follow from the fact that they hold for the map induced by h_S (because h_S is a covering homomorphism). □

Now we describe the irreducible characters of $K \otimes_{\mathcal{O}} B$. For simplicity, we write $S_K = K \otimes_{\mathcal{O}} S$, and similarly $L_K = K \otimes_{\mathcal{O}} L$, so that we have $S_K = \mathrm{End}_K(L_K)$ and $K \otimes_{\mathcal{O}} B \cong S_K \otimes_K KP$. Also ρ_{L_K} denotes the character of L_K, a function defined on the whole of S_K. If f is a function on S_K and g is a function on KP, we write $f{\cdot}g$ for the function defined by

$$(f{\cdot}g)(s \otimes a) = f(s)g(a)\,, \qquad s \in S_K,\ a \in KP\,.$$

We also write $\mathrm{Irr}(KP)$ for the set of irreducible characters of KP. With this notation we have the following description of the characters of $K \otimes_{\mathcal{O}} B$.

(52.6) LEMMA. *The set of functions* $\{\rho_{L_K}\cdot\lambda \mid \lambda \in \mathrm{Irr}(KP)\}$ *is the set of all irreducible characters of* $K \otimes_{\mathcal{O}} B \cong S_K \otimes_K KP$.

Proof. Recall that, since S is $\mathcal{O}$-simple, $S \otimes_{\mathcal{O}} \mathcal{O}P$ is Morita equivalent to $\mathcal{O}P$ and the Morita correspondent of an $\mathcal{O}P$-lattice N is the $S \otimes_{\mathcal{O}} \mathcal{O}P$-lattice $L \otimes_{\mathcal{O}} N$ (Exercise 9.5). Tensoring everything with K, we have similarly a Morita equivalence between KP and $S_K \otimes_K KP$ (Exercise 9.7), and the Morita correspondent of a KP-module M is the $S_K \otimes_K KP$-module $L_K \otimes_K M$. Therefore any simple $K \otimes_{\mathcal{O}} B$-module is isomorphic to $L_K \otimes_K M$ for some simple KP-module M , and its character is $\rho_{L_K}\cdot\chi_M$, where χ_M is the character of M (because traces behave multiplicatively with respect to tensor products). Conversely for any simple KP-module M , the character $\rho_{L_K}\cdot\chi_M$ is the character of the simple $K \otimes_{\mathcal{O}} B$-module $L_K \otimes_K M$. □

In order to describe character values using Brauer's second main theorem, we need to know the set of local points $\mathcal{LP}((\mathcal{O}Gb)^{<u>})$. This is our next result.

(52.7) LEMMA. *Let* u *be a* p*-element of* G . *Then* $\mathcal{LP}((\mathcal{O}Gb)^{<u>})$ *is in bijection with* $P\backslash T_G(u,P)/C_G(u)$, *where* $T_G(u,P) = \{g \in G \mid {}^g u \in P\}$. *The bijection maps the local point* δ *to the double coset* $PgC_G(u)$, *where* g *is such that* ${}^g(u_\delta) \in P_\gamma$.

Proof. Since all defects of b are conjugate, any local pointed element u_δ is contained in a conjugate of P_γ . Thus there exists $g \in G$ such that ${}^g(u_\delta) \in P_\gamma$. In particular $g \in T_G(u,P)$. If g' also satisfies ${}^{g'}(u_\delta) \in P_\gamma$, then ${}^g(u_\delta) \in P_\gamma$ and ${}^{g'g^{-1}}({}^g(u_\delta)) \in P_\gamma$. By the definition of a nilpotent block, it follows that $g'g^{-1} \in PC_G({}^g u) = PgC_G(u)g^{-1}$, and therefore $g' \in PgC_G(u)$. This shows that the map $\delta \mapsto PgC_G(u)$ is well-defined.

If $g \in T_G(u,P)$, then ${}^g u \in P$ and $({}^g u)_\varepsilon \in P_\gamma$ for some local point $\varepsilon \in \mathcal{LP}((\mathcal{O}Gb)^{<{}^g u>})$ (and in fact ε is unique by Corollary 49.16). Now ${}^{g^{-1}}\varepsilon \in \mathcal{LP}((\mathcal{O}Gb)^{<u>})$ is mapped to the double coset of g , proving the surjectivity of the map.

If δ and δ' are mapped to the same double coset $PgC_G(u)$, then ${}^g(u_\delta) \in P_\gamma$ and ${}^g(u_{\delta'}) \in P_\gamma$. By Corollary 49.16, ${}^g\delta$ is the unique local point of $(\mathcal{O}Gb)^{<{}^g u>}$ such that $({}^g u)_{{}^g\delta} \in P_\gamma$. Therefore ${}^g\delta = {}^g(\delta')$ and so $\delta = \delta'$, proving the injectivity of the map. □

Any block with a central defect group P is nilpotent (Corollary 49.11), and in that case we have seen in Example 43.11 that the generalized decomposition matrix is the ordinary character table of KP. We prove now that almost the same result holds for arbitrary nilpotent blocks. The only difference lies in the fact that some signs occur, which we now define. For every $u \in P$, let $\varepsilon(u)$ be the unique local point of $S^{<u>}$. Remember that $S = \mathrm{End}_{\mathcal{O}}(L)$ is the endomorphism algebra of a uniquely determined indecomposable endo-permutation $\mathcal{O}P$-lattice L with vertex P and determinant one. By Corollary 52.2, the character ρ_L has values in $\mathbb{Z}$ on elements of P, and therefore Proposition 52.3 applies. We define $\omega(u) = \rho_L(u_{\varepsilon(u)}) = \pm 1$ (see Proposition 52.3).

(52.8) THEOREM. *Assume that $\mathcal{O}$ is a complete discrete valuation ring of characteristic zero and let K be the field of fractions of $\mathcal{O}$. Let b be a nilpotent block of $\mathcal{O}G$ with defect P_γ and let $\mathrm{Irr}(KGb)$ be the set of irreducible ordinary characters of b.*

(a) There is a unique bijection

$$\mathrm{Irr}(KP) \longrightarrow \mathrm{Irr}(KGb)\,, \qquad \lambda \mapsto \chi_\lambda$$

with the following property: for every local pointed element $u_\delta \in P_\gamma$, the generalized decomposition number $\chi_\lambda(u_\delta)$ is equal to

$$\chi_\lambda(u_\delta) = \omega(u)\lambda(u)\,,$$

where $\omega(u) = \pm 1$ is defined above.

(b) For every p-element u of G and every $s \in C_G(u)_{\mathrm{reg}}$, we have

$$\chi_\lambda(us) = \sum_{g \in [P\backslash T_G(u,P)/C_G(u)]} \omega({}^g u)\lambda({}^g u)\phi_\delta(s)\,,$$

where δ is the unique local point of $(\mathcal{O}Gb)^{<u>}$ such that ${}^g(u_\delta) \leq P_\gamma$, and where ϕ_δ is the modular character of $C_G(u)$ corresponding to δ. Moreover every term in the above sum is independent of the choice of g in its double coset.

Proof. (a) Let $B = (\mathcal{O}Gb)_\gamma \cong S \otimes_{\mathcal{O}} \mathcal{O}P$ be a source algebra of b. Then $\mathcal{O}Gb$ is Morita equivalent to B (Proposition 38.2) and B is in turn Morita equivalent to $\mathcal{O}P$ (Exercise 9.5). Therefore KGb is Morita equivalent to KP (Exercise 9.7) and the equivalence induces a bijection $\mathrm{Irr}(KGb) \to \mathrm{Irr}(KP)$. We write χ_λ for the image of $\lambda \in \mathrm{Irr}(KP)$ under the inverse bijection and we want to prove that this bijection satisfies the required property. Note that the bijection is obtained as the composite of the two bijections $\mathrm{Irr}(KGb) \xrightarrow{\sim} \mathrm{Irr}(K \otimes_{\mathcal{O}} B) \xrightarrow{\sim} \mathrm{Irr}(KP)$ and that the character of $K \otimes_{\mathcal{O}} B \cong S_K \otimes_K KP$ which corresponds to $\lambda \in \mathrm{Irr}(KP)$ and $\chi_\lambda \in \mathrm{Irr}(KGb)$ is equal to $\rho_{L_K} \cdot \lambda$ (see Lemma 52.6 and its proof).

Any local pointed element u_δ on $\mathcal{O}Gb$ such that $u_\delta \in P_\gamma$ is the image of a local pointed element on B via the associated embedding $\mathcal{F}_\gamma : B \to \mathrm{Res}_P^G(\mathcal{O}Gb)$. Moreover we know that the generalized decomposition number $\chi_\lambda(u_\delta)$ can be computed from the source algebra B, using the Morita correspondent of χ_λ (Proposition 43.10). Thus we have to compute $(\rho_{L_K} \cdot \lambda)(u_\delta)$, where u_δ is a local pointed element on $B \cong S \otimes_{\mathcal{O}} \mathcal{O}P$.

By Lemma 52.5, there is a local pointed element u_ε on S such that δ is the image of ε via the map $s : S \to S \otimes_{\mathcal{O}} \mathcal{O}P$ defined by $a \mapsto a \otimes 1_{\mathcal{O}P}$. Moreover $\varepsilon = \varepsilon(u)$ is the unique local point of $S^{<u>}$ (Proposition 28.8). Therefore if $j \in \varepsilon(u)$, then $(j \otimes 1_{\mathcal{O}P}) \in \delta$ and we obtain

$$\begin{aligned}(\rho_{L_K} \cdot \lambda)(u_\delta) &= (\rho_{L_K} \cdot \lambda)(u(j \otimes 1_{\mathcal{O}P})) = (\rho_{L_K} \cdot \lambda)(uj \otimes u) \\ &= \rho_{L_K}(uj)\lambda(u) = \rho_L(u_{\varepsilon(u)})\lambda(u) = \omega(u)\lambda(u),\end{aligned}$$

because obviously ρ_L is the restriction to S of the character ρ_{L_K} on S_K.

In order to prove the uniqueness of the bijection, we note that the required property about generalized decomposition numbers determines uniquely all values of the character χ_λ, as we shall see in the proof of (b). Thus χ_λ is uniquely determined by λ.

(b) By Brauer's second main Theorem 43.4, Lemma 52.7, and the fact that any character is constant on a conjugacy class, we have

$$\begin{aligned}\chi_\lambda(us) &= \sum_{\delta \in \mathcal{LP}((\mathcal{O}Gb)^{<u>})} \chi_\lambda(u_\delta)\, \phi_\delta(s) \\ &= \sum_{g \in [P \backslash T_G(u,P)/C_G(u)]} \chi_\lambda({}^g(u_\delta))\, \phi_\delta(s).\end{aligned}$$

In the second expression, δ denotes the unique local point of $(\mathcal{O}Gb)^{<u>}$ corresponding to g under the bijection of Lemma 52.7. Explicitly, δ is the unique local point such that ${}^g(u_\delta) \leq P_\gamma$. But since ${}^g(u_\delta) \leq P_\gamma$, we have $\chi_\lambda({}^g(u_\delta)) = \omega({}^g u)\lambda({}^g u)$ by part (a). Finally the property that $\chi_\lambda({}^g(u_\delta))$ is independent of the choice of g in the double coset $PgC_G(u)$ is again a consequence of the fact that a character is constant on a conjugacy class. □

Note that the signs $\omega(u)$ may have the value -1 in some examples (Exercise 52.2).

Exercises

(52.1) Suppose that $\mathcal{O}$ is a complete discrete valuation ring of characteristic zero. Let L be an $\mathcal{O}G$-lattice, let ρ_L be the character of L, let $S = \mathrm{End}_{\mathcal{O}}(L)$, and let u_ε be a pointed element on S. Prove that if the point ε is not local, then $\rho_N(u_\varepsilon) = 0$. [Hint: Show that the argument of Proposition 43.3 applies without change.]

(52.2) Suppose that $\mathcal{O}$ is a complete discrete valuation ring of characteristic zero and let K be the field of fractions of $\mathcal{O}$. Let Q_8 be the quaternion group of order 8, generated by i and j. Thus $z = i^2 = j^2 = (ij)^2$ is the central element of order 2 and $ji = zij$. Let $G = Q_8 \rtimes P$ be the semi-direct product of Q_8 with the cyclic group P of order 3, where a generator u of P acts on Q_8 by a cyclic permutation of i, j and ij. We work with the prime $p = 3$.

(a) Let L be the $\mathcal{O}Q_8$-lattice of dimension 2 defined by the representation

$$i \mapsto \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \qquad j \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Prove that $L_K = K \otimes_{\mathcal{O}} L$ is the unique simple KQ_8-module of dimension 2 (up to isomorphism), and that the corresponding primitive idempotent of ZKQ_8 is $b = (1-z)/2$.

(b) Prove that b is a block of $\mathcal{O}G$ and that b is nilpotent.

(c) Prove that the action of P on the group Q_8 induces an action of P on $S = \mathrm{End}_{\mathcal{O}}(L)$. Prove that this P-algebra structure lifts uniquely to an interior P-algebra structure with determinant one and compute the image of u in S.

(d) Prove that b is primitive in $(\mathcal{O}G)^P$, so that $B = \mathrm{Res}^G_P(\mathcal{O}Gb)$ is a source algebra of b. Prove also that $B \cong S \otimes_{\mathcal{O}} \mathcal{O}P$.

(e) Prove that $\rho_L(u) = \omega(u) = -1$.

(f) Prove that KGb has three irreducible characters and compute their values using Theorem 52.8.

Notes on Section 52

Theorem 52.8 (in a slightly different form) is due to Broué and Puig [1980b]. The present approach using source algebras is due to Puig [1988b]. A proof of the fact mentioned in Remark 52.4 can be found in Puig [1988d].

CHAPTER 8

Green functors and maximal ideals

In this final chapter, we show that the defect theory of Chapter 3 can be carried out in a much more general context. We replace G-algebras over our usual base ring $\mathcal{O}$ by Green functors over an arbitrary commutative ring R and we work with maximal ideals rather than idempotents. We prove the existence of defect groups and sources and we show that the Puig and Green correspondences hold in this context. We also show that the defect theory can be entirely reinterpreted in terms of functorial ideals in Green functors.

Throughout this chapter, G denotes a finite group and R denotes a commutative ring with a unity element. In contrast with the convention used in the previous chapters, we do not require R-modules to be finitely generated, so that in particular R-algebras need not be finitely generated as R-modules.

§ 53 MACKEY FUNCTORS AND GREEN FUNCTORS

In this section, we define Mackey and Green functors and give several examples.

Let $\mathcal{S}(G)$ be the set of all subgroups of G. A *Mackey functor* M for G over R is a family of R-modules $M(H)$, where H runs over the set $\mathcal{S}(G)$, together with R-linear maps

$$\begin{aligned} r^H_K &: M(H) \longrightarrow M(K)\,, \\ t^H_K &: M(K) \longrightarrow M(H)\,, \\ c_{g,H} &: M(H) \longrightarrow M({}^gH)\,, \end{aligned}$$

where $K \leq H$, $g \in G$ and ${}^gH = gHg^{-1}$, such that the following axioms are satisfied: for all $g, h \in G$ and $H, K, L \in \mathcal{S}(G)$,

(i) $r^K_L\, r^H_K = r^H_L$ and $t^H_K\, t^K_L = t^H_L$ if $L \leq K \leq H$,
(ii) $r^H_H = t^H_H = id_{M(H)}$,
(iii) $c_{gh,H} = c_{g,{}^hH}\, c_{h,H}$,
(iv) $c_h : M(H) \to M(H)$ is the identity if $h \in H$,
(v) $c_{g,K}\, r^H_K = r^{\,{}^gH}_{\,{}^gK}\, c_{g,H}$ and $c_{g,H}\, t^H_K = t^{\,{}^gH}_{\,{}^gK}\, c_{g,K}$ if $K \leq H$,
(vi) (Mackey axiom) if $L, K \leq H$,

$$r^H_L\, t^H_K = \sum_{h \in [L\backslash H/K]} t^L_{L\cap {}^hK}\, r^{\,{}^hK}_{L\cap {}^hK}\, c_{h,K}$$

where $[L\backslash H/K]$ denotes a set of representatives of the (L, K)-double cosets LhK with $h \in H$.

It is an easy exercise to show that the formula in the Mackey axiom does not depend on the choice of representatives of double cosets, using axioms (iii), (iv) and (v). The maps r^H_K are called the *restriction* maps, the maps t^H_K are called the *transfer* maps (or also *induction* maps), and the maps $c_{g,H}$ are called the *conjugation* maps.

Every conjugation map $c_{g,H}$ is an isomorphism, because it has the inverse $c_{g^{-1},{}^gH}$. More precisely, by axiom (iii), G acts on the R-module $\prod_{H\in\mathcal{S}(G)} M(H)$ as a group of R-linear automorphisms. For this reason, we shall from now on write the conjugation maps as a left action, by defining

$${}^gm = c_{g,H}(m) \qquad \text{for } m \in M(H) \text{ and } g \in G\,.$$

Moreover the subgroup $N_G(H)$ stabilizes $M(H)$ and by axiom (iv), the quotient $\overline{N}_G(H) = N_G(H)/H$ acts on $M(H)$ as a group of R-linear automorphisms. In other words $M(H)$ is an $R\overline{N}_G(H)$-module and in particular $M(1)$ is an RG-module. Here RG denotes the group algebra of G with coefficients in R. Thus a Mackey functor can be viewed as a family of modules, one for each group algebra $R\overline{N}_G(H)$, related to one another by restriction and transfer maps.

The concept of Green functor is the analogous notion with a multiplicative structure. A *Green functor* for G over R (also called a *G-functor* over R) is a Mackey functor A such that $A(H)$ is endowed with an associative R-algebra structure with a unity element (for every $H \in \mathcal{S}(G)$) and such that the following axioms are satisfied:

(vii) All restriction maps $r^H_K : A(H) \to A(K)$ and conjugation maps $c_{g,H} : A(H) \to A({}^gH)$ are unitary homomorphisms of R-algebras.

(viii) (Frobenius axiom) If $K \leq H$, $a \in A(K)$ and $b \in A(H)$, then

$$t^H_K(a \cdot r^H_K(b)) = t^H_K(a) \cdot b \qquad \text{and} \qquad t^H_K(r^H_K(b) \cdot a) = b \cdot t^H_K(a) .$$

We emphasize that t^H_K is not a ring homomorphism. In fact the Frobenius axiom implies that the image of t^H_K is a two-sided ideal of $A(H)$. The two formulas in the Frobenius axiom are also known as the *projection formulas.*

Since the conjugation maps are unitary homomorphisms of R-algebras, G acts on $\prod_{H \in \mathcal{S}(G)} A(H)$ as a group of algebra automorphisms, and in particular $\overline{N}_G(H)$ acts on $A(H)$ as a group of algebra automorphisms. In other words $A(H)$ is an $\overline{N}_G(H)$-algebra, and in particular $A(1)$ is a G-algebra. Here a *G-algebra* over R is an associative R-algebra with a unity element endowed with an action of G by algebra automorphisms. In contrast with the previous notion of G-algebra over $\mathcal{O}$, we do not require R-algebras to be finitely generated as R-modules.

(53.1) EXAMPLE. If M is a left RG-module, we define a Mackey functor F_M as follows. For every subgroup H of G, we let $F_M(H) = M^H$, the R-submodule of H-fixed elements of M. The restriction maps are the inclusions $r^H_K : M^H \to M^K$, the transfer maps are the relative trace maps $t^H_K : M^K \to M^H$ defined by $t^H_K(m) = \sum_{h \in [H/K]} h{\cdot}m$ for $m \in M^K$, and the conjugation maps are defined by ${}^gm = g{\cdot}m$ (for $g \in G$ and $m \in M$). The proof that all the axioms are satisfied is left to the reader. It is identical with the proof of Proposition 11.4. Note that the RG-module M itself is recovered from F_M because $F_M(1) = M$. This implies that the category of RG-modules is embedded in the category of Mackey functors for G. But the category of Mackey functors is much larger. The Mackey functor F_M satisfies the additional condition

$$t^H_K r^H_K(m) = |H : K|{\cdot}m \qquad \text{for } K \leq H \text{ and } m \in M^H .$$

A Mackey functor with this property is called *cohomological.*

(53.2) EXAMPLE. If A is a G-algebra over R, the Mackey functor F_A defined in the previous example has a multiplicative structure and is in fact a cohomological Green functor for G. The proof was given in Proposition 11.4. Again the G-algebra A is recovered from F_A because we have $F_A(1) = A$. Many results about a G-algebra A (for instance the defect theory of Chapter 3 when $R = \mathcal{O}$) can be viewed as results about the Green functor F_A. The aim of this chapter is to generalize some of these results to arbitrary Green functors. Thus the Green functors F_A are fundamental examples in the sequel.

(53.3) EXAMPLE. Let M be an RG-module and n a positive integer. For every subgroup H of G, define $H^n(H, M)$ to be the n-th cohomology group of H with coefficients in M (or more precisely in $\mathrm{Res}^G_H(M)$). If $K \le H$ and $g \in G$, let

$$\begin{aligned} r^H_K &: H^n(H, M) \to H^n(K, M), \\ t^H_K &: H^n(K, M) \to H^n(H, M), \\ c_{g,H} &: H^n(H, M) \to H^n({}^gH, M) \end{aligned}$$

be the restriction map, the transfer (or corestriction) map and the conjugation map respectively. Then $H^n(-, M)$ is a Mackey functor. This standard fact of cohomology theory is proved for instance in the book of Brown [1982]. Moreover this Mackey functor is cohomological (and this explains the terminology). When $n = 0$, we recover the Mackey functor F_M. Similarly the family of graded modules

$$H^*(H, M) = \bigoplus_{n \ge 0} H^n(H, M), \qquad H \in \mathcal{S}(G),$$

is a Mackey functor. One also gets Mackey functors if one works with homology or Tate's cohomology.

(53.4) EXAMPLE. Let M be an RG-module. For every subgroup H of G, the cohomology group

$$H^*(H, \mathrm{End}_R(M)) \cong \mathrm{Ext}^*_{RH}(M, M)$$

has an R-algebra structure given by the Yoneda product. The corresponding Mackey functor (defined in the previous example) is a cohomological Green functor. This example has been particularly considered when R is an algebraically closed field of non-zero characteristic p. We refer the reader to the book by Benson [1991] for more details.

(53.5) EXAMPLE. For every subgroup H of G, let $R_{\mathbb{C}}(H)$ be the ring of ordinary characters of H. The restriction, induction and conjugation of characters induce maps

$$r_K^H : R_{\mathbb{C}}(H) \longrightarrow R_{\mathbb{C}}(K)\,,$$
$$t_K^H : R_{\mathbb{C}}(K) \longrightarrow R_{\mathbb{C}}(H)\,,$$
$$c_{g,H} : R_{\mathbb{C}}(H) \longrightarrow R_{\mathbb{C}}({}^gH)\,,$$

making $R_{\mathbb{C}}$ into a Green functor over $\mathbb{Z}$. One can also view $R_{\mathbb{C}}(H)$ as the Grothendieck group of $\mathbb{C}H$-modules. Details can be found in many textbooks, for instance Curtis–Reiner [1981].

(53.6) EXAMPLE. The previous example can be generalized to many types of Grothendieck group constructions. For instance, if k is a field of characteristic p, let $R_k(H)$ be the Grothendieck ring of kG-modules with respect to all short exact sequences. If k is large enough, $R_k(H)$ is isomorphic to the ring of modular characters of H. There is also the Grothendieck group $A(H)$ of kG-modules with respect to split short exact sequences, called the *Green ring* of H (or the representation ring of H). Both $R_k(H)$ and $A(H)$ are rings for the multiplication induced by the tensor product of kH-modules. Restriction, induction, and conjugation of modules induce maps making R_k and A into Green functors for G over $\mathbb{Z}$. More details can be found in many textbooks, for instance Curtis–Reiner [1987], Feit [1982], Benson [1991].

(53.7) EXAMPLE. Another example of Grothendieck group construction is the *Burnside ring* $B(H)$ of H, which is the Grothendieck ring of finite H-sets, with addition induced by disjoint union, and multiplication induced by cartesian product. Restriction, induction, and conjugation induce maps making B into a Green functor for G over $\mathbb{Z}$, called the *Burnside functor*. In the same way as the ring $\mathbb{Z}$ is universal in the category of rings, the Burnside functor B is universal in the category of Green functors: for every Green functor A, there exists a unique unitary homomorphism of Green functors $B \to A$. Details can be found in Exercise 53.5 or in the books by tom Dieck [1979, 1987].

(53.8) EXAMPLE. The topological K-theory of classifying spaces gives another example of Green functor. For every subgroup H of G, let BH be the classifying space of H and consider the Grothendieck ring $K(H)$ of complex vector bundles on BH. If $J \leq H$, the natural covering map $BJ \to BH$ induces both a restriction map $r_J^H : K(H) \to K(J)$ and a transfer map $t_J^H : K(J) \to K(H)$ and it turns out that K is a Green functor for G over $\mathbb{Z}$. If $R_{\mathbb{C}}(H)$ denotes the character ring of Example 53.5, there is a natural homomorphism of Green functors $R_{\mathbb{C}} \to K$, and Atiyah's theorem asserts that this induces an isomorphism $\widehat{R}_{\mathbb{C}} \xrightarrow{\sim} K$, where $\widehat{R}_{\mathbb{C}}(H)$ denotes the completion of $R_{\mathbb{C}}(H)$ with respect to the ideal of characters of dimension zero. More information can be found in the paper by Atiyah [1961].

(53.9) EXAMPLE. The algebraic K-theory of group rings gives another source of examples of Mackey functors. If F is a commutative ring with a unity element, the family of groups $K_0(FH)$ for $H \in \mathcal{S}(G)$ is a Mackey functor. When F is a suitable ring such as the ring of integers, there are variations on this theme: the groups $SK_0(FH)$ and the Whitehead groups $Wh(H)$ also give rise to Mackey functors for G. We refer to the book by Oliver [1988] for more details.

(53.10) EXAMPLE. The algebraic K-theory of fields also yields Mackey functors. If E is a finite Galois extension of a field F with Galois group G, then the family of groups $K_i(E^H)$ for $H \in \mathcal{S}(G)$ is a Mackey functor. Here K_i can be understood as either the Milnor or the Quillen K-theory. The transfer maps for Quillen's K-theory are defined in the original paper of Quillen [1973]. The transfer maps for Milnor's K-theory are introduced by Bass and Tate [1973] and it is proved in Kato [1980] that this definition is independent of the choices which were used by Bass and Tate.

(53.11) EXAMPLE. Witt rings give rise to Mackey functors in two different ways. If E is a finite Galois extension of a field F with Galois group G, then the family of Witt rings $W(E^H)$ for $H \in \mathcal{S}(G)$ is a Green functor. If $K \leq H$, the restriction map $W(H) \to W(K)$ is induced by scalar extension from E^H to E^K, while the transfer map is Scharlau's transfer (defined by means of the trace map of the extension E^K/E^H). If now F is a fixed field, there is another Mackey functor consisting, for $H \in \mathcal{S}(G)$, of the equivariant Witt rings $W(H,F)$ (constructed using H-invariant non-degenerate symmetric bilinear forms on FH-modules). More details about both constructions can be found in the paper of Dress [1975].

(53.12) EXAMPLE. Associated with field extensions, we also have ideal class groups. If E is a finite Galois extension of a number field F with Galois group G, then the family of groups $\mathcal{C}(E^H)$ for $H \in \mathcal{S}(G)$ is a Mackey functor. Here $\mathcal{C}(E^H)$ denotes the ideal class group of the ring of integers in E^H. If $K \leq H$, the restriction map $\mathcal{C}(E^H) \to \mathcal{C}(E^K)$ is induced by scalar extension from E^H to E^K, while the transfer map is induced by the norm map. Details can be found in many textbooks about algebraic number theory.

(53.13) EXAMPLE. The surgery obstruction groups, also called L-groups, form a Mackey functor. More details can be found in Dress [1975].

In Examples 53.7 and 53.8, we have mentioned homomorphisms, which we now define in a precise fashion. If M and N are two Mackey functors for G over R, a *homomorphism of Mackey functors* $f : M \to N$ is a family of R-linear maps $f(H) : M(H) \to N(H)$, where H runs over $\mathcal{S}(G)$, such that the following properties hold: for all $g \in G$ and $H, K \in \mathcal{S}(G)$ with $K \leq H$,
(i) $f(K)\, r^H_K = r^H_K\, f(H)$,
(ii) $f(H)\, t^H_K = t^H_K\, f(K)$,
(iii) $f({}^gH)\, c_{g,H} = c_{g,H}\, f(H)$.
If A and B are two Green functors for G, a *homomorphism of Green functors* $f : A \to B$ is a homomorphism of Mackey functors such that $f(H)$ is a homomorphism of R-algebras for every $H \in \mathcal{S}(G)$. Moreover f is called *unitary* if every $f(H)$ is unitary. We shall only deal with unitary homomorphisms throughout this chapter.

A *subfunctor* of a Mackey functor M is a Mackey functor N such that $N(H)$ is an R-submodule of $M(H)$ for every $H \in \mathcal{S}(G)$ and the inclusion $N \to M$ is a homomorphism of Mackey functors. Equivalently, N consists of a family of R-submodules $N(H)$ such that the following conditions are satisfied: for all $g \in G$ and $H, K \in \mathcal{S}(G)$ with $K \leq H$,

$$r^H_K(N(H)) \subseteq N(K)\,, \qquad t^H_K(N(K)) \subseteq N(H)\,, \qquad c_{g,H}(N(H)) \subseteq N({}^gH)\,.$$

If A is a Green functor, a *functorial ideal* of A is a subfunctor I of A (as a Mackey functor) such that $I(H)$ is an ideal of $A(H)$ for every $H \in \mathcal{S}(G)$. Recall that an ideal always means a two-sided ideal.

If N is a subfunctor of a Mackey functor M, the *quotient functor* M/N is the Mackey functor defined by $(M/N)(H) = M(H)/N(H)$ for every $H \in \mathcal{S}(G)$, with restriction, transfer, and conjugation maps induced by those of M. If A is a Green functor and if I is a functorial ideal of A, then the Mackey functor A/I inherits in fact a Green functor structure for G.

If M is a Mackey functor for G and if H is a subgroup of G, we define the restriction $\mathrm{Res}^G_H(M)$ to be the Mackey functor for H given by $\mathrm{Res}^G_H(M)(S) = M(S)$ for every subgroup $S \leq H$, with restriction, transfer, and conjugation maps equal to those of M. If A is a Green functor for G, then obviously $\mathrm{Res}^G_H(A)$ is a Green functor for H.

Exercises

(53.1) In the definition of a Mackey functor, prove that the formula in the Mackey axiom does not depend on the choice of representatives of double cosets. [Hint: Use axioms (iii), (iv) and (v).]

(53.2) Let M be an RG-module. For every subgroup H of G, define $Q_M(H) = M_H$, the largest quotient of M (as an R-module) on which H acts trivially. If $K \leq H$, let $t_K^H : M_K \to M_H$ be the canonical surjection and let $r_K^H : M_H \to M_K$ be the map induced by $m \mapsto \sum_{h\in[K\backslash H]} h{\cdot}m$. Prove that Q_M is a Mackey functor. More generally prove that the homology functor $H_n(-,M)$ is a Mackey functor.

(53.3) Let $R_{\mathbb{C}}$ be the character ring functor (Example 53.5) and, for every $H \in \mathcal{S}(G)$, let $I(H)$ be the ideal of characters of dimension zero.
(a) Prove that I is a functorial ideal of $R_{\mathbb{C}}$.
(b) Let $\mathbb{Z}$ be the ring of integers, endowed with the trivial action of G, and let $F_{\mathbb{Z}}$ be the corresponding Green functor for G (Example 53.2). Prove that $R_{\mathbb{C}}/I \cong F_{\mathbb{Z}}$.

(53.4) Consider the ring R, endowed with the trivial action of G, and let F_R be the corresponding Green functor for G, so that $F_R(H) = R$ for every $H \in \mathcal{S}(G)$. Let A be a Green functor for G over R and, for every $H \in \mathcal{S}(G)$, let $f(H) : R \to A(H)$ be the structural homomorphism defining the R-algebra structure of $A(H)$ (that is, $\lambda \mapsto \lambda{\cdot}1_{A(H)}$).
(a) Prove that $f : F_R \to A$ is a homomorphism of Green functors if and only if A is cohomological.
(b) If A is cohomological, prove that f is the unique unitary homomorphism of Green functors $F_R \to A$, so that F_R is universal in the category of cohomological Green functors.

(53.5) For every $H \in \mathcal{S}(G)$, let $B(H)$ be the Burnside ring of H (Example 53.7).
(a) Prove that the transitive H-sets H/S form a $\mathbb{Z}$-basis of $B(H)$, where S runs over the subgroups of H up to H-conjugation.
(b) If $K \leq H$, define induction by $\mathrm{Ind}_K^H(X) = H \times_K X$ for every K-set X. Prove that the corresponding map $t_K^H : B(K) \to B(H)$ satisfies $t_K^H(K/S) = H/S$ and in particular $H/K = t_K^H(1_{B(K)})$.
(c) Prove that B is a Green functor.
(d) Prove that B is universal in the category of Green functors, by showing that, for every Green functor A, there exists a unique unitary homomorphism of Green functors $f : B \to A$. [Hint: In view of (b), $f(H) : B(H) \to A(H)$ must be defined by $f(H)(H/K) = t_K^H(1_{A(K)})$.]

Notes on Section 53

The concepts of Mackey functor and Green functor were introduced by Dress [1973] and Green [1971], as a convenient tool for dealing with the general theory of induction and transfer. In particular they proved some general induction theorems for Mackey functors. The theory has been used since in a variety of situations, suggested by the examples of this section.

§ 54 THE BRAUER HOMOMORPHISM FOR MACKEY FUNCTORS

The notion of Brauer homomorphism can be defined for arbitrary Mackey functors, in analogy with the case of G-algebras considered in Section 11 and the case of G-modules mentioned in Section 27. In this section, we generalize previous results and prove a general theorem concerning the kernel of a homomorphism constructed from various Brauer homomorphisms. We continue with a finite group G and a commutative base ring R.

Let M be a Mackey functor for G over R. For every subgroup P of G, we define the *Brauer quotient*

$$\overline{M}(P) = M(P) / \sum_{X<P} t_X^P(M(X))$$

and we write $br_P^M : M(P) \to \overline{M}(P)$ for the canonical surjection. The map br_P^M is called the *Brauer homomorphism* (corresponding to the subgroup P). The R-submodule $\sum_{X<P} t_X^P(M(X))$ is invariant under conjugation by $N_G(P)$, because ${}^g(t_X^P(M(X))) = t_{{}^gX}^P(M({}^gX))$ if $g \in N_G(P)$ by axiom (v) in the definition of a Mackey functor. Thus br_P^M is a homomorphism of $R\overline{N}_G(P)$-modules. When the context is clear, we often write simply br_P instead of br_P^M.

If A is a Green functor for G over R, then $t_X^P(A(X))$ is an ideal of $A(P)$ (by the Frobenius axiom), and therefore $\sum_{X<P} t_X^P(A(X))$ is an ideal. It follows that $\overline{A}(P)$ is an R-algebra and that the Brauer homomorphism $br_P^A : A(P) \to \overline{A}(P)$ is a homomorphism of R-algebras. Since br_P^A is also a homomorphism of $\overline{N}_G(P)$-modules, it is in fact a homomorphism of $\overline{N}_G(P)$-algebras.

(54.1) REMARK. In the special case of a G-algebra A over $\mathcal{O}$, the definition of $\overline{A}(P)$ given in Section 11 does not coincide with the present definition. Indeed it was convenient in this specific context to quotient further the $\mathcal{O}$-algebra $B = A^P / \sum_{X<P} t_X^P(A^X)$ by the ideal $\mathfrak{p}B$, as observed in Remark 11.8. However, this does not change the points of B because $\mathfrak{p}B \subseteq J(B)$. Thus as long as one deals with points or maximal ideals (and this is our main purpose for the defect theory), one can pass without difficulty from one definition to the other.

Let M be a Mackey functor for G. A subgroup P is called *primordial* for M if $\overline{M}(P) \neq 0$. For a G-algebra A over $\mathcal{O}$ (as in Chapter 2), the algebra $\overline{A}(P)$ can be non-zero only if P is a p-group (Lemma 11.7), but no such restriction occurs for Mackey and Green functors (Exercises 54.2 and 54.3).

Our first result is a fundamental property of the Brauer homomorphism which connects the transfer map in a Mackey functor M with the relative trace map in the $R\overline{N}_G(P)$-module $\overline{M}(P)$.

(54.2) PROPOSITION. *Let M be a Mackey functor for G over R, let P be a primordial subgroup for M, and let H be a subgroup of G containing P. Then for every $a \in M(P)$, we have*

$$br_P\, r_P^H\, t_P^H(a) = t_1^{\overline{N}_H(P)}\, br_P(a)\,,$$

where $t_1^{\overline{N}_H(P)} : \overline{M}(P) \to \overline{M}(P)^{\overline{N}_H(P)}$ is the relative trace map in the $R\overline{N}_G(P)$-module $\overline{M}(P)$.

Proof. The proof is identical with that of Proposition 11.9. □

The question of the surjectivity of transfer maps is the central problem of the defect theory. In this respect, the next result shows the crucial role of primordial subgroups.

(54.3) PROPOSITION. *Let M be a Mackey functor for G and let* $\mathrm{Prim}(M)$ *be the set of primordial subgroups for M. For every subgroup H of G, we have*

$$M(H) = \sum_{P \in \mathrm{Prim}(M) \cap \mathcal{S}(H)} t_P^H(M(P))\,,$$

where $\mathcal{S}(H)$ is the set of all subgroups of H.

Proof. Let $\mathcal{X}$ be a family of subgroups of H for which we have $M(H) = \sum_{P\in\mathcal{X}} t_P^H(M(P))$. If some maximal member Q of $\mathcal{X}$ is not primordial, then $M(Q) = \sum_{X<Q} t_X^Q(M(X))$ and therefore

$$M(H) = \sum_{P\in\mathcal{X}} t_P^H(M(P)) = \sum_{P\in\mathcal{X}-\{Q\}} t_P^H(M(P)) + \sum_{X<Q} t_Q^H t_X^Q(M(X))$$
$$= \sum_{P\in\mathcal{X}'} t_P^H(M(P)),$$

where $\mathcal{X}'$ is the union of $\mathcal{X} - \{Q\}$ with the set of proper subgroups of Q. Starting from $\mathcal{X} = \mathcal{S}(H)$ and suppressing one at a time every non-primordial subgroup in decreasing order, we easily obtain the result by induction. □

In fact a more precise result holds: $M(H) = \sum_{P\in\mathcal{M}} t_P^H(M(P))$, where $\mathcal{M}$ is the set of maximal elements of $\mathrm{Prim}(M) \cap \mathcal{S}(H)$ (Exercise 54.4).

Let M be a Mackey functor for G and let H be a subgroup of G. Combining all Brauer homomorphisms br_P for $P \leq H$, one obtains a homomorphism

$$\beta_H : M(H) \longrightarrow \prod_{P\leq H} \overline{M}(P),$$

defined to be the product of all homomorphisms $br_P\, r_P^H : M(H) \to \overline{M}(P)$. For a Green functor, β_H is a ring homomorphism because r_P^H and br_P are both ring homomorphisms. We write $\beta_H^M = \beta_H$ when we want to emphasize the dependence on the Mackey functor M.

In the case of a Mackey functor associated with a G-module M (and in particular for G-algebras), β_H is always injective because the component corresponding to $P = 1$ is injective. Indeed $br_1\, r_1^H = r_1^H$ is just the inclusion map $M^H \to M$. However, r_1^H is in general not injective for arbitrary Mackey functors. For a Green functor, we have the following result on the kernel of β_H.

(54.4) PROPOSITION. *Let A be a Green functor for G, let H be a subgroup of G, and let $\beta_H : A(H) \to \prod_{P\leq H} \overline{A}(P)$ be the algebra homomorphism defined above. Then* $\mathrm{Ker}(\beta_H)$ *is a nilpotent ideal of $A(H)$.*

Proof. It is clear that the homomorphism β_H^A coincides with the homomorphism $\beta_H^{\mathrm{Res}_H^G(A)}$ for the H-functor $\mathrm{Res}_H^G(A)$. Changing notation (that is, replacing the H-functor $\mathrm{Res}_H^G(A)$ by the G-functor A), it suffices to prove the result for β_G.

Let $\mathrm{Prim}(A)$ be the set of primordial subgroups for A. We define $\mathcal{P}_1 = \mathrm{Prim}(A)$, $\mathcal{P}_2 = \mathcal{P}_1 - \mathcal{M}_1$ where $\mathcal{M}_1$ is the set of maximal elements of $\mathcal{P}_1$, and inductively $\mathcal{P}_{i+1} = \mathcal{P}_i - \mathcal{M}_i$ where $\mathcal{M}_i$ is the set of maximal elements of $\mathcal{P}_i$. Then we have

$$\mathrm{Prim}(A) = \mathcal{P}_1 \supset \mathcal{P}_2 \supset \ldots \supset \mathcal{P}_{m-1} \supset \mathcal{P}_m = \emptyset$$

for some integer m. We claim that, for $1 \leq i \leq m-1$, we have

$$\text{(54.5)} \qquad \mathrm{Ker}(\beta_G) \cdot \big(\sum_{S \in \mathcal{P}_i} t_S^G(A(S)) \big) \subseteq \sum_{S \in \mathcal{P}_{i+1}} t_S^G(A(S)) \,.$$

In case $i+1 = m$, the sum over the empty set has to be interpreted as the zero submodule of $A(G)$. Postponing the proof of this claim, we deduce that $\mathrm{Ker}(\beta_G)^{m-1} = 0$. Indeed let $a_1, \ldots, a_{m-1} \in \mathrm{Ker}(\beta_G)$. Since $A(G) = \sum_{S \in \mathcal{P}_1} t_S^G(A(S))$ by Proposition 54.3, we have by 54.5

$$a_1 = a_1 \cdot 1_{A(G)} \in \sum_{S \in \mathcal{P}_2} t_S^G(A(S)) \,,$$

and inductively $a_i a_{i-1} \ldots a_1 \in \sum_{S \in \mathcal{P}_{i+1}} t_S^G(A(S))$ for $1 \leq i \leq m-1$. For $i = m-1$, this yields $a_{m-1} a_{m-2} \ldots a_1 = 0$, proving the nilpotency of $\mathrm{Ker}(\beta_G)$.

We are left with the proof of the claim 54.5. Let $a \in \mathrm{Ker}(\beta_G)$ and let $b \in \sum_{S \in \mathcal{P}_i} t_S^G(A(S))$. We have $\sum_{S \in \mathcal{P}_i} t_S^G(A(S)) = \sum_{S \in \mathcal{M}_i} t_S^G(A(S))$ by Exercise 54.4. Thus we can write $b = \sum_{S \in \mathcal{M}_i} t_S^G(b_S)$ for some $b_S \in A(S)$, and we deduce

$$ab = \sum_{S \in \mathcal{M}_i} t_S^G(r_S^G(a) b_S)$$

by the Frobenius axiom. Since $a \in \mathrm{Ker}(\beta_G)$, we have $br_S \, r_S^G(a) = 0$, that is, $r_S^G(a) \in \sum_{T < S} t_T^S(A(T))$. By Proposition 54.3 applied to each subgroup T, it follows that

$$r_S^G(a) \in \sum_{\substack{P \in \mathrm{Prim}(A) \\ P < S}} t_P^S(A(P)) \,.$$

Since $S \in \mathcal{M}_i$ and $P \in \mathrm{Prim}(A)$, the relation $P < S$ implies that $P \in \mathcal{P}_{i+1}$. Therefore we can write $r_S^G(a) = \sum_{P \in \mathcal{P}_{i+1}} t_P^S(a_{P,S})$ for some $a_{P,S} \in A(P)$. By the Frobenius axiom again, we obtain

$$\begin{aligned} ab &= \sum_{S \in \mathcal{M}_i} t_S^G \big(\sum_{P \in \mathcal{P}_{i+1}} t_P^S(a_{P,S}) b_S \big) \\ &= \sum_{S \in \mathcal{M}_i} \sum_{P \in \mathcal{P}_{i+1}} t_P^G(a_{P,S} \, r_P^S(b_S)) \in \sum_{P \in \mathcal{P}_{i+1}} t_P^G(A(P)) \,, \end{aligned}$$

as was to be shown. □

In the case of a commutative Green functor, the proposition has the following consequence about the nilradical. Recall that the *nilradical* of a commutative ring is the set of all nilpotent elements. This is an ideal because the ring is commutative.

(54.6) COROLLARY. *Let A be a Green functor for G. For every subgroup H of G, assume that $A(H)$ is commutative and let $J(H)$ be the nilradical of $A(H)$. Then J is a functorial ideal of A.*

Proof. Since the restriction and conjugation maps are ring homomorphisms, it is clear that J is invariant under restriction and conjugation. Let K be a proper subgroup of H. In order to prove that $t_K^H(J(K)) \subseteq J(H)$, we use induction on $|H|$. There is nothing to prove when $H = 1$. Let X be a proper subgroup of H. By the Mackey axiom and the fact that J is invariant under restriction and conjugation, we have

$$r_X^H \, t_K^H(J(K)) \subseteq \sum_{Y \leq X} t_Y^X(J(Y)) \, .$$

Since $X < H$, we have $t_Y^X(J(Y)) \subseteq J(X)$ by induction, and therefore

$$r_X^H \, t_K^H(J(K)) \subseteq J(X) \qquad \text{for every } X < H \, .$$

Now let $a \in t_K^H(J(K))$. We claim that $\beta_H(a)$ is nilpotent. By the definition of β_H, we have to prove that $br_X \, r_X^H(a)$ is nilpotent for every $X \leq H$. If $X = H$, then $br_H(a) = 0$ by the choice of a (because $K < H$). If $X < H$, then $r_X^H(a)$ is nilpotent by the proof above, and so $br_X \, r_X^H(a)$ is nilpotent. It follows that there exists an integer n such that $\beta_H(a^n) = \beta_H(a)^n = 0$. Thus $a^n \in \mathrm{Ker}(\beta_H)$ and since $\mathrm{Ker}(\beta_H)$ is nilpotent by Proposition 54.4, $a^{nm} = 0$ for some m. Therefore $a \in J(H)$. This proves that $t_K^H(J(K)) \subseteq J(H)$. □

Every maximal ideal of a commutative ring contains the nilradical (see Lemma 55.1). Therefore one can always pass to the quotient by the nilradical when working with maximal ideals. Corollary 54.6 above shows that one can do this uniformly in a commutative Green functor A and work in the quotient functor A/J, for which the nilradical of $(A/J)(H)$ is zero for every H.

There is no similar result in the non-commutative case. If one works with the Jacobson radical $J(A(H))$ of $A(H)$, then we know that it is in general not invariant under restriction and transfer (Exercise 11.3).

(54.7) REMARK. For an arbitrary Mackey functor M, one can prove more about the homomorphism β_H. First note that H acts by conjugation on $\prod_{P\leq H}\overline{M}(P)$. Since H acts trivially on $M(H)$ (by axiom (iv) of the definition) and since β_H commutes with the action of H (Exercise 54.1), the image of β_H is actually contained in the set of H-fixed elements $\big(\prod_{P\leq H}\overline{M}(P)\big)^H$. Viewing now β_H as the homomorphism

$$\beta_H : M(H) \longrightarrow \big(\prod_{P\leq H}\overline{M}(P)\big)^H ,$$

one can prove that both $\mathrm{Ker}(\beta_H)$ and $\mathrm{Coker}(\beta_H)$ are annihilated by the integer $\prod |N_H(P):P|$, where P runs over all primordial subgroups of H up to conjugation. This implies for instance that β_H is injective if there is no torsion in the abelian group $M(H)$. Also, if $|G|$ is invertible in the base ring R, then β_H is always an isomorphism.

Exercises

(54.1) Let M be a Mackey functor for G and let H be a subgroup of G. Prove that the homomorphism $\beta_H : M(H) \longrightarrow \prod_{P\leq H}\overline{M}(P)$ commutes with the action of H and has therefore an image contained in the H-fixed elements $\big(\prod_{P\leq H}\overline{M}(P)\big)^H$.

(54.2) Let B be the Burnside functor (Example 53.7 and Exercise 53.5).

(a) For every subgroup H of G, prove that $\overline{B}(H)\cong\mathbb{Z}$ and that the Brauer homomorphism $br_H : B(H)\to\mathbb{Z}$ maps an H-set X to the cardinality of the set X^H of H-fixed elements in X. [Hint: Show that the transitive H-sets H/K form a $\mathbb{Z}$-basis of $B(H)$ when K runs over all subgroups of H up to conjugation. Moreover show that $H/K = t_K^H(1_{B(K)}) \in \mathrm{Ker}(br_H)$ if $K<H$.]

(b) Prove that the set of primordial subgroups for B is the set of all subgroups of G.

(c) Prove that the homomorphism

$$\beta_H : B(H) \longrightarrow \big(\prod_{P\in\mathcal{S}(H)}\overline{B}(P)\big)^H \cong \prod_{P\in\mathcal{S}(H)/H}\mathbb{Z}$$

is injective and that it is an isomorphism after extending scalars to $\mathbb{Q}$. [Hint: Prove that, with respect to the canonical bases, the matrix of β_H is triangular with coefficients $|N_H(P):P|$ on the main diagonal.]

(54.3) Let $R_{\mathbb{C}}$ be the character ring functor (Example 53.5). Extending scalars to the field $\mathbb{Q}$ of rational numbers, define the functor $\mathbb{Q}R_{\mathbb{C}}$ by $\mathbb{Q}R_{\mathbb{C}}(H) = \mathbb{Q} \otimes_{\mathbb{Z}} R_{\mathbb{C}}(H)$ for every subgroup H of G.

(a) Prove that if H is not cyclic, then H is not a primordial subgroup for $\mathbb{Q}R_{\mathbb{C}}$. [Hint: This is a restatement of Artin's induction theorem, whose proof can be found in many textbooks, for instance in Curtis–Reiner [1981].]

(b) Prove that if H is cyclic of order n, then $\overline{R}_{\mathbb{C}}(H) \cong \mathbb{Z}[\zeta]$, where ζ is a primitive n-th root of unity. [Hint: Show that $R_{\mathbb{C}}(H) \cong \mathbb{Z}[t]/(t^n - 1)$ and that the sum of the images of induction from proper subgroups is the ideal generated by $\Phi_n(t)$, where $\Phi_n(t)$ denotes the cyclotomic polynomial, that is, the minimal polynomial of ζ.]

(c) Deduce from (b) that $\overline{\mathbb{Q}R_{\mathbb{C}}}(H) \cong \mathbb{Q}[\zeta]$.

(d) Prove that the set $\mathcal{C}$ of primordial subgroups for $\mathbb{Q}R_{\mathbb{C}}$ is the set of all cyclic subgroups of G.

(d) Prove that the homomorphism

$$\beta_G : \mathbb{Q}R_{\mathbb{C}}(G) \longrightarrow \Big(\prod_{H \in \mathcal{C}} \mathbb{Q}[\zeta_{|H|}]\Big)^G \cong \prod_{H \in \mathcal{C}/G} \mathbb{Q}[\zeta_{|H|}]^{N_G(H)}$$

is an isomorphism, where $\zeta_{|H|}$ denotes a primitive $|H|$-th root of unity. [Hint: For the injectivity, prove that $R_{\mathbb{C}}(G)$ has no non-zero nilpotent element. For the surjectivity, either apply the results of Remark 54.7 or compute dimensions, using the fact that $\dim(\mathbb{Q}R_{\mathbb{C}}(G))$ is the number of conjugacy classes of G.]

(54.4) Let M be a Mackey functor for G and let H be a subgroup of G.

(a) Prove that if $\mathcal{X}$ is a family of subgroups of H and if $\mathcal{M}$ is the set of maximal elements of $\mathcal{X}$, then $\sum_{S \in \mathcal{X}} t_S^H(M(S)) = \sum_{S \in \mathcal{M}} t_S^H(M(S))$.

(b) Let $\mathrm{Prim}(M)$ be the set of primordial subgroups for M. Prove that $M(H) = \sum_{S \in \mathcal{M}} t_S^H(M(S))$, where $\mathcal{M}$ is the set of maximal elements of $\mathrm{Prim}(M) \cap \mathcal{S}(H)$.

Notes on Section 54

The constructions and results of this section appear in Thévenaz [1988c], where one can also find the results mentioned in Remark 54.7. Corollary 54.6 is due to Thévenaz [1991].

§ 55 MAXIMAL IDEALS AND POINTED GROUPS

In this section, we consider pointed groups on arbitrary Green functors, using maximal ideals rather than idempotents. We define two partial order relations between pointed groups and we introduce the crucial notion of primordial pointed group. We start the section with some basic results about maximal ideals.

Let F be a ring (always with a unity element). Recall that an ideal of F is always understood to be two-sided. We denote by $\mathrm{Max}(F)$ the set of all maximal ideals of F . By Zorn's lemma, every ideal of F is contained in a maximal ideal (thanks to the fact that the unity element is never contained in a proper ideal). If $\mathfrak{m} \in \mathrm{Max}(F)$, we usually denote by $\pi_{\mathfrak{m}} : F \to F/\mathfrak{m}$ the canonical surjection. We review some basic facts about maximal ideals.

(55.1) LEMMA. *Let $\mathfrak{n}$ be a nilpotent ideal of a ring F . Then $\mathfrak{n}$ is contained in every maximal ideal of F .*

Proof. Let $\mathfrak{m} \in \mathrm{Max}(F)$ and suppose that $\mathfrak{m}$ does not contain $\mathfrak{n}$. Then $\mathfrak{m}+\mathfrak{n} = F$ by maximality of $\mathfrak{m}$, so that every element of $F/\mathfrak{m}$ is the image of some element of $\mathfrak{n}$ via the canonical surjection $F \to F/\mathfrak{m}$. Thus every element of $F/\mathfrak{m}$ is nilpotent and in particular $1_{F/\mathfrak{m}}$ is nilpotent. But this is clearly impossible in the non-zero ring $F/\mathfrak{m}$. □

Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of F are called *coprime* if $\mathfrak{a} + \mathfrak{b} = F$. Clearly $\mathfrak{a}$ and $\mathfrak{b}$ are coprime if and only if there exist $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ such that $a + b = 1_F$. If $\mathfrak{m} \in \mathrm{Max}(F)$, then $\mathfrak{a} + \mathfrak{m}$ is equal to $\mathfrak{m}$ if $\mathfrak{a} \subseteq \mathfrak{m}$ and to F otherwise (by maximality of $\mathfrak{m}$). Thus $\mathfrak{a}$ and $\mathfrak{m}$ are coprime if and only if $\mathfrak{m}$ does not contain $\mathfrak{a}$.

(55.2) LEMMA. *Let $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ and $\mathfrak{b}$ be ideals of a ring F . If $\mathfrak{a}_i$ and $\mathfrak{b}$ are coprime for every $i \in \{1, \ldots, n\}$, then $\bigcap_{i=1}^n \mathfrak{a}_i$ and $\mathfrak{b}$ are coprime.*

Proof. By assumption, there exist $a_i \in \mathfrak{a}_i$ and $b_i \in \mathfrak{b}$ such that $a_i + b_i = 1_F$. Then

$$1_F = 1_F^n = (a_1 + b_1) \ldots (a_n + b_n) = a_1 \ldots a_n + b$$

where b is a sum of products containing at least one term b_i . Thus $b \in \mathfrak{b}$. Since $a_1 \ldots a_n \in \bigcap_{i=1}^n \mathfrak{a}_i$, the result follows. □

(55.3) COROLLARY. *Let* $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ *be ideals of a ring* F *and let* $\mathfrak{m} \in \mathrm{Max}(F)$. *If* $\mathfrak{m} \supseteq \bigcap_{i=1}^n \mathfrak{a}_i$, *there exists* i *such that* $\mathfrak{m} \supseteq \mathfrak{a}_i$.

Proof. If $\mathfrak{m}$ does not contain $\mathfrak{a}_i$ for every i, then $\mathfrak{a}_i$ and $\mathfrak{m}$ are coprime for every i, by maximality of $\mathfrak{m}$. By Lemma 55.2, $\mathfrak{m}$ and $\bigcap_{i=1}^n \mathfrak{a}_i$ are coprime, so that $\mathfrak{m}$ does not contain $\bigcap_{i=1}^n \mathfrak{a}_i$. □

(55.4) LEMMA. *Let* $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ *be ideals of a ring* F. *If* $\mathfrak{a}_i$ *and* $\mathfrak{a}_j$ *are coprime whenever* $i \neq j$, *there is an isomorphism*

$$F\Big/\bigcap_{i=1}^n \mathfrak{a}_i \cong \prod_{i=1}^n F/\mathfrak{a}_i ,$$

induced by the product of the surjections $\pi_i : F \to F/\mathfrak{a}_i$.

Proof. The product of the surjections π_i induces a ring homomorphism

$$\pi : F \to \prod_{i=1}^n F/\mathfrak{a}_i$$

with kernel $\bigcap_{i=1}^n \mathfrak{a}_i$. Thus we only have to prove the surjectivity of π. For a fixed i, the assumption implies that $\mathfrak{a}_i$ and $\bigcap_{j\neq i} \mathfrak{a}_j$ are coprime (Lemma 55.2). Thus there exist $a_i \in \mathfrak{a}_i$ and $b_i \in \bigcap_{j\neq i} \mathfrak{a}_j$ such that $a_i + b_i = 1_F$. Let $(\overline{x}_1, \ldots, \overline{x}_n) \in \prod_{i=1}^n F/\mathfrak{a}_i$ and let $x_i \in F$ such that $\pi_i(x_i) = \overline{x}_i$. Consider the element

$$x = \sum_{i=1}^n b_i x_i .$$

We claim that $\pi(x) = (\overline{x}_1, \ldots, \overline{x}_n)$, proving the surjectivity of π. We have to show that $\pi_i(x) = \overline{x}_i$ for every i. But since $b_j \in \mathfrak{a}_i$ if $i \neq j$, $\pi_i(b_j) = 0$. Therefore $\pi_i(x) = \pi_i(b_i)\pi_i(x_i) = \pi_i(b_i)\overline{x}_i$ and it suffices to prove that $\pi_i(b_i) = 1_{F/\mathfrak{a}_i}$. But this is clear since $a_i + b_i = 1_F$ and $a_i \in \mathfrak{a}_i$. □

Let A be a Green functor for G over R. We define a *pointed group* on A to be a pair $(H,\mathfrak{m})$, always written $H_{\mathfrak{m}}$, where $H \in \mathcal{S}(G)$ and $\mathfrak{m} \in \mathrm{Max}(A(H))$. Here the word "point" has to be understood as referring to a maximal ideal (a terminology originating from algebraic geometry). In the case of a G-algebra A over $\mathcal{O}$ (as in Chapter 2), the set of points $\mathcal{P}(A^H)$ is in bijection with $\mathrm{Max}(A^H)$ (Theorem 4.3). Thus, up to an obvious passage from points to maximal ideals, the notion of pointed group on A defined in Chapter 2 coincides with the concept of pointed group on the corresponding G-functor F_A.

The group G acts by conjugation on the set of pointed groups on a Green functor A. If $g \in G$ and $H_{\mathfrak{m}}$ is a pointed group on A, then ${}^g(H_{\mathfrak{m}}) = ({}^gH)_{{}^g\mathfrak{m}}$, where ${}^gH = gHg^{-1}$ and where ${}^g\mathfrak{m} = c_{g,H}(\mathfrak{m})$ is the conjugate of $\mathfrak{m}$ (using the conjugation map which is part of the definition of a G-functor). The stabilizer of $H_{\mathfrak{m}}$ is written $N_G(H_{\mathfrak{m}})$. We have $H \leq N_G(H_{\mathfrak{m}}) \leq N_G(H)$ because H acts trivially on $A(H)$ (axiom (iv) in the definition). In particular the quotient group $\overline{N}_G(H_{\mathfrak{m}}) = N_G(H_{\mathfrak{m}})/H$ acts on the simple algebra $A(H)/\mathfrak{m}$, so that $A(H)/\mathfrak{m}$ is an $\overline{N}_G(H_{\mathfrak{m}})$-algebra.

We define the following containment relation between pointed groups. If $H_{\mathfrak{m}}$ and $K_{\mathfrak{n}}$ are pointed groups on A, we say that $K_{\mathfrak{n}}$ is *contained in* $H_{\mathfrak{m}}$ and we write $K_{\mathfrak{n}} \leq H_{\mathfrak{m}}$ if $K \leq H$ and $(r^H_K)^{-1}(\mathfrak{n}) \subseteq \mathfrak{m}$. It is clear that this relation is a partial order relation on the set of all pointed groups on A. For the transitivity, if $P_{\mathfrak{p}} \leq K_{\mathfrak{n}}$ and $K_{\mathfrak{n}} \leq H_{\mathfrak{m}}$, then

$$(r^H_P)^{-1}(\mathfrak{p}) \;=\; (r^H_K)^{-1}(r^K_P)^{-1}(\mathfrak{p}) \;\subseteq\; (r^H_K)^{-1}(\mathfrak{n}) \;\subseteq\; \mathfrak{m}\,.$$

In the case of a G-algebra A over $\mathcal{O}$ considered in Chapter 2, the relation $K_\beta \leq H_\alpha$ between two pointed groups on A is equivalent to the containment relation $K_{\mathfrak{m}_\beta} \leq H_{\mathfrak{m}_\alpha}$ between the corresponding pointed groups on the G-functor F_A (see Lemma 13.3).

For the definition of relative projectivity, we need the following notation. If M is an R-submodule of an R-algebra, then M° denotes the unique largest ideal contained in M. In other words M° is the sum of all ideals contained in M (this sum is still contained in M because M is an R-submodule). If $H_{\mathfrak{m}}$ and $K_{\mathfrak{n}}$ are pointed groups on A, we say that $H_{\mathfrak{m}}$ is *projective relative to* $K_{\mathfrak{n}}$, and we write $H_{\mathfrak{m}}\,pr\,K_{\mathfrak{n}}$, if $K \leq H$ and $(t^H_K)^{-1}(\mathfrak{m})^\circ \subseteq \mathfrak{n}$. Another way of seeing this is provided by the following lemma.

(55.5) LEMMA. *Let* A *be a Green functor for* G *and let* $H_{\mathfrak{m}}$ *and* $K_{\mathfrak{n}}$ *be pointed groups on* A *. Assume that* $K \leq H$ *. The following conditions are equivalent.*

(a) $(t_K^H)^{-1}(\mathfrak{m})^\circ \subseteq \mathfrak{n}$ *(that is,* $H_{\mathfrak{m}}\, pr\, K_{\mathfrak{n}}$ *).*

(b) Every ideal $\mathfrak{a}$ *of* $A(K)$ *such that* $\mathfrak{a} \not\subseteq \mathfrak{n}$ *satisfies* $t_K^H(\mathfrak{a}) \not\subseteq \mathfrak{m}$ *.*

(c) If an ideal $\mathfrak{a}$ *of* $A(K)$ *is coprime to* $\mathfrak{n}$ *, then the ideal* $t_K^H(\mathfrak{a})$ *is coprime to* $\mathfrak{m}$ *.*

Proof. It is clear that (b) and (c) are equivalent. Let $\mathfrak{a}$ be any ideal of $A(K)$. Then $\mathfrak{a} \subseteq (t_K^H)^{-1}(\mathfrak{m})^\circ$ if and only if $\mathfrak{a} \subseteq (t_K^H)^{-1}(\mathfrak{m})$, that is, $t_K^H(\mathfrak{a}) \subseteq \mathfrak{m}$. Therefore the inclusion $(t_K^H)^{-1}(\mathfrak{m})^\circ \subseteq \mathfrak{n}$ holds if and only if every ideal $\mathfrak{a}$ of $A(K)$ such that $t_K^H(\mathfrak{a}) \subseteq \mathfrak{m}$ satisfies $\mathfrak{a} \subseteq \mathfrak{n}$. This condition is equivalent to (b). □

(55.6) COROLLARY. *The relation* pr *is transitive.*

Proof. Let $P_{\mathfrak{p}}$, $K_{\mathfrak{n}}$, and $H_{\mathfrak{m}}$ be pointed groups on A such that $H_{\mathfrak{m}}\, pr\, K_{\mathfrak{n}}$ and $K_{\mathfrak{n}}\, pr\, P_{\mathfrak{p}}$. Let $\mathfrak{a}$ be an ideal of $A(P)$ coprime to $\mathfrak{p}$. Then $t_P^K(\mathfrak{a})$ is coprime to $\mathfrak{n}$ and in turn $t_K^H(t_P^K(\mathfrak{a})) = t_P^H(\mathfrak{a})$ is coprime to $\mathfrak{m}$, so that $H_{\mathfrak{m}}\, pr\, P_{\mathfrak{p}}$. □

Another consequence of Lemma 55.5 is that, in the case of G-algebras over $\mathcal{O}$, the relation pr coincides with the relation defined in Chapter 2. Indeed let H_α and K_β be two pointed groups on a G-algebra A over $\mathcal{O}$ (as in Chapter 2), and let $\mathfrak{m}_\alpha$ and $\mathfrak{m}_\beta$ be the corresponding maximal ideals. There is a unique minimal ideal $\mathfrak{a}$ satisfying $\mathfrak{a} \not\subseteq \mathfrak{m}_\beta$, namely the ideal $\mathfrak{a} = A^K \beta A^K$ (Lemma 4.13). If this ideal satisfies the property $t_K^H(A^K \beta A^K) \not\subseteq \mathfrak{m}_\alpha$, then any larger ideal $\mathfrak{a}'$ of A^K also satisfies $t_K^H(\mathfrak{a}') \not\subseteq \mathfrak{m}_\alpha$. Therefore condition (b) in Lemma 55.5 is equivalent to the single requirement $t_K^H(A^K \beta A^K) \not\subseteq \mathfrak{m}_\alpha$. But this in turn is equivalent to the condition $\alpha \subseteq t_K^H(A^K \beta A^K)$ (Corollary 4.10), and this is the definition of the relation $H_\alpha\, pr\, K_\beta$.

We shall often use the following easy observation. Let $H_{\mathfrak{m}}$ and $K_{\mathfrak{n}}$ be two pointed groups on A such that either $H_{\mathfrak{m}} \geq K_{\mathfrak{n}}$ or $H_{\mathfrak{m}}\, pr\, K_{\mathfrak{n}}$. If $H = K$, then $H_{\mathfrak{m}} = K_{\mathfrak{n}}$. The proof is left to the reader (Exercise 55.2).

A pointed group $H_{\mathfrak{m}}$ on A is called *projective relative to* a subgroup K of H if $H_{\mathfrak{m}}\, pr\, K_{\mathfrak{n}}$ for some $\mathfrak{n} \in \mathrm{Max}(A(K))$. Also $H_{\mathfrak{m}}$ is called *projective* if it is projective relative to the trivial subgroup 1.

(55.7) LEMMA. *Let A be a Green functor for G, let $H_{\mathfrak{m}}$ be a pointed group on A, and let K be a subgroup of H. The following conditions are equivalent.*
(a) $H_{\mathfrak{m}}$ *is projective relative to* K.
(b) $t_K^H(A(K))$ *and* $\mathfrak{m}$ *are coprime.*
(c) $(t_K^H)^{-1}(\mathfrak{m})^\circ$ *is a proper ideal of* $A(K)$.

Proof. We have $t_K^H(A(K)) \not\subseteq \mathfrak{m}$ (that is, $t_K^H(A(K))$ and $\mathfrak{m}$ are coprime) if and only if $(t_K^H)^{-1}(\mathfrak{m})$ is a proper R-submodule of $A(K)$, and this holds if and only if $(t_K^H)^{-1}(\mathfrak{m})^\circ$ is a proper ideal of $A(K)$. Now an ideal is proper if and only if it is contained in some maximal ideal $\mathfrak{n}$, and the inclusion $(t_K^H)^{-1}(\mathfrak{m})^\circ \subseteq \mathfrak{n}$ means that $H_{\mathfrak{m}}\,pr\,K_{\mathfrak{n}}$. □

Let A be a Green functor for G, let I be a functorial ideal of A, and consider the quotient functor A/I. The surjection $A(H) \to (A/I)(H)$ induces an injective map $\mathrm{Max}((A/I)(H)) \to \mathrm{Max}(A(H))$, defined by taking inverse images. If $\mathfrak{m} \in \mathrm{Max}(A(H))$ is the inverse image of a maximal ideal $\overline{\mathfrak{m}} \in \mathrm{Max}((A/I)(H))$, we shall say that the pointed group $H_{\mathfrak{m}}$ on A *comes* from the pointed group $H_{\overline{\mathfrak{m}}}$ on A/I. In other words $H_{\mathfrak{m}}$ comes from A/I if and only if $\mathfrak{m} \supseteq I(H)$, in which case $\overline{\mathfrak{m}} = \mathfrak{m}/I(H)$. This injection from the set of pointed groups on A/I into the set of pointed groups on A behaves very well with respect to the relations of containment and relative projectivity (Exercise 55.3).

We now turn to the extreme case where a pointed group is not projective relative to a proper subgroup.

(55.8) LEMMA. *Let A be a Green functor for G and let $P_{\mathfrak{p}}$ be a pointed group on A. The following conditions are equivalent.*
(a) $P_{\mathfrak{p}}$ *is minimal with respect to the relation* pr.
(b) $P_{\mathfrak{p}}$ *is not projective relative to a proper subgroup of* P.
(c) $\mathrm{Ker}(br_P) \subseteq \mathfrak{p}$.
(d) $\mathfrak{p}$ *is the inverse image under* $br_P : A(P) \to \overline{A}(P)$ *of some maximal ideal of* $\overline{A}(P)$.

Proof. The equivalence of (a) and (b) is clear. Now (b) holds if and only if $\mathfrak{p}$ contains $t_Q^P(A(Q))$ for every $Q < P$ (Lemma 55.7), and this means that $\mathfrak{p}$ contains $\sum_{Q<P} t_Q^P(A(Q)) = \mathrm{Ker}(br_P)$. Thus (b) and (c) are equivalent. Finally it is clear that (c) and (d) are equivalent. □

A pointed group $P_{\mathfrak{p}}$ on A is called *primordial* if it satisfies the equivalent conditions of the lemma. We also say that the maximal ideal $\mathfrak{p}$ of $A(P)$ is *primordial* if $P_{\mathfrak{p}}$ is primordial. More generally an arbitrary ideal $\mathfrak{a}$ of $A(P)$ is called *primordial* if it is a proper ideal of $A(P)$ and if $\operatorname{Ker}(br_P) \subseteq \mathfrak{a}$. This implies that the subgroup P is primordial because $\operatorname{Ker}(br_P)$ is then a proper ideal. Conversely if P is a primordial subgroup, then the proper ideal $\operatorname{Ker}(br_P)$ is contained in some maximal ideal $\mathfrak{p}$ and so $P_{\mathfrak{p}}$ is primordial.

(55.9) COROLLARY. *Let A be a Green functor for G and let P be a primordial subgroup for A. Then $br_P : A(P) \to \overline{A}(P)$ induces a bijection between $\operatorname{Max}(\overline{A}(P))$ and the set of primordial maximal ideals of $A(P)$.*

In the special case of a G-algebra A over $\mathcal{O}$, a pointed group P_γ on A is local if and only if, on the corresponding G-functor F_A, the pointed group $P_{\mathfrak{m}_\gamma}$ is primordial. We avoid the word "local" in the general case because this terminology is usually associated with p-subgroups of G, whereas primordial subgroups may be arbitrary.

The following crucial property of primordial pointed groups has already been proved in the case of local pointed groups on a G-algebra (Proposition 14.7) and is analogous to a result proved for the Brauer homomorphism (Proposition 54.2). Recall that if $P_{\mathfrak{p}}$ is a pointed group on a G-functor A, the simple algebra $A(P)/\mathfrak{p}$ is an $\overline{N}_G(P_{\mathfrak{p}})$-algebra, for the action of $\overline{N}_G(P_{\mathfrak{p}})$ induced by conjugation.

(55.10) PROPOSITION. *Let A be a Green functor for G, let $P_{\mathfrak{p}}$ be a primordial pointed group on A, let $\pi_{\mathfrak{p}} : A(P) \to A(P)/\mathfrak{p}$ be the canonical surjection, and let H be a subgroup of G containing P. If $a \in A(P)$ satisfies $a \in {}^h\mathfrak{p}$ for every $h \in N_H(P) - N_H(P_{\mathfrak{p}})$, then*

$$\pi_{\mathfrak{p}}\, r^H_P\, t^H_P(a) = t_1^{\overline{N}_H(P_{\mathfrak{p}})}\, \pi_{\mathfrak{p}}(a)\,,$$

where $t_1^{\overline{N}_H(P_{\mathfrak{p}})} : A(P)/\mathfrak{p} \to (A(P)/\mathfrak{p})^{\overline{N}_H(P_{\mathfrak{p}})}$ denotes the relative trace map in the $\overline{N}_G(P_{\mathfrak{p}})$-algebra $A(P)/\mathfrak{p}$.

Proof. The proof is the same as that of Proposition 14.7. Since $\mathfrak{p}$ is primordial, we have

$$t^P_Q(A(Q)) \subseteq \operatorname{Ker}(br_P) \subseteq \mathfrak{p} = \operatorname{Ker}(\pi_{\mathfrak{p}})$$

if $Q < P$. Using the Mackey axiom, it follows that

$$\pi_{\mathfrak{p}}\, r^H_P\, t^H_P(a) = \sum_{h\in[P\backslash H/P]} \pi_{\mathfrak{p}}\, t^P_{P\cap {}^hP}\, r^{{}^hP}_{P\cap {}^hP}({}^h a) = \sum_{h\in[N_H(P)/P]} \pi_{\mathfrak{p}}({}^h a)\,.$$

But ${}^h a \in \mathfrak{p}$ if $h \notin N_H(P_\mathfrak{p})$ (because $a \in {}^{h^{-1}}\mathfrak{p}$ by assumption), and therefore $\pi_\mathfrak{p}({}^h a) = 0$. Thus we are left with a sum over $[N_H(P_\mathfrak{p})/P]$ and since $\pi_\mathfrak{p}$ commutes with the action of $N_H(P_\mathfrak{p})$ (by definition of the action of $N_H(P_\mathfrak{p})$ on $A(P)/\mathfrak{p}$), we obtain

$$\begin{aligned}\pi_\mathfrak{p}\, r_P^H\, t_P^H(a) &= \sum_{h\in[N_H(P_\mathfrak{p})/P]} \pi_\mathfrak{p}({}^h a) = \sum_{h\in[N_H(P_\mathfrak{p})/P]} {}^h(\pi_\mathfrak{p}(a)) \\ &= t_1^{\overline{N}_H(P_\mathfrak{p})}\, \pi_\mathfrak{p}(a)\,,\end{aligned}$$

as required. □

For $P \leq K \leq H$, a slightly more general result holds, connecting t_K^H and the relative trace map $t_{\overline{N}_K(P_\mathfrak{p})}^{\overline{N}_H(P_\mathfrak{p})}$ (Exercise 55.6).

We end this section with the observation that the relation pr implies the relation $\geq$ in the commutative case.

(55.11) PROPOSITION. *Let A be a Green functor for G, let $H_\mathfrak{m}$ and $K_\mathfrak{n}$ be two pointed groups on A such that $H_\mathfrak{m}\, pr\, K_\mathfrak{n}$, and assume that $A(K)$ is a commutative ring. Then $(r_K^H)^{-1}(\mathfrak{n}) = \mathfrak{m}$, and in particular $H_\mathfrak{m} \geq K_\mathfrak{n}$.*

Proof. By the Frobenius axiom,

$$t_K^H\big(A(K)\cdot r_K^H(\mathfrak{m})\big) = t_K^H(A(K))\cdot \mathfrak{m} \subseteq \mathfrak{m}\,,$$

and therefore $A(K)\cdot r_K^H(\mathfrak{m}) \subseteq (t_K^H)^{-1}(\mathfrak{m})$. Since $A(K)\cdot r_K^H(\mathfrak{m})$ is an ideal by the commutativity assumption, we obtain

$$A(K)\cdot r_K^H(\mathfrak{m}) \subseteq (t_K^H)^{-1}(\mathfrak{m})^\circ \subseteq \mathfrak{n}\,,$$

using the definition of the relation pr. It follows that $\mathfrak{m} \subseteq (r_K^H)^{-1}(\mathfrak{n})$. By maximality of $\mathfrak{m}$, we deduce that $\mathfrak{m} = (r_K^H)^{-1}(\mathfrak{n})$, because we have $1_{A(H)} \notin (r_K^H)^{-1}(\mathfrak{n})$. In particular we obtain $H_\mathfrak{m} \geq K_\mathfrak{n}$. □

(55.12) REMARK. There is another situation where much more can be said about the relations pr and $\geq$, namely when the base ring R is an algebraically closed field in which $|G|$ is invertible. Let A be a Green functor for G over R and assume that, for every primordial pointed group $P_\mathfrak{p}$, the simple ring $A(P)/\mathfrak{p}$ is finite dimensional over R. It can be shown in this case that the relations pr and $\geq$ are equivalent.

Exercises

(55.1) Let A be a Green functor for G, let $H_{\mathfrak{m}}$ and $K_{\mathfrak{n}}$ be pointed groups on A, and let $g \in G$.
(a) Prove that if $H_{\mathfrak{m}} \geq K_{\mathfrak{n}}$, then ${}^g(H_{\mathfrak{m}}) \geq {}^g(K_{\mathfrak{n}})$.
(b) Prove that if $H_{\mathfrak{m}} \, pr \, K_{\mathfrak{n}}$, then ${}^g(H_{\mathfrak{m}}) \, pr \, {}^g(K_{\mathfrak{n}})$.
(c) Prove that if $H_{\mathfrak{m}}$ is primordial, then ${}^g(H_{\mathfrak{m}})$ is primordial.

(55.2) Let A be a Green functor for G and let $H_{\mathfrak{m}}$ and $H_{\mathfrak{n}}$ be pointed groups on A.
(a) Prove that if $H_{\mathfrak{m}} \geq H_{\mathfrak{n}}$, then $H_{\mathfrak{m}} = H_{\mathfrak{n}}$.
(b) Prove that if $H_{\mathfrak{m}} \, pr \, H_{\mathfrak{n}}$, then $H_{\mathfrak{m}} = H_{\mathfrak{n}}$.

(55.3) Let A be a Green functor for G and let I be a functorial ideal of A. Let $H_{\mathfrak{m}}$ and $K_{\mathfrak{n}}$ be pointed groups on A coming from pointed groups $H_{\overline{\mathfrak{m}}}$ and $K_{\overline{\mathfrak{n}}}$ on A/I.
(a) Prove that $H_{\mathfrak{m}} \geq K_{\mathfrak{n}}$ if and only if $H_{\overline{\mathfrak{m}}} \geq K_{\overline{\mathfrak{n}}}$.
(b) Prove that $H_{\mathfrak{m}} \, pr \, K_{\mathfrak{n}}$ if and only if $H_{\overline{\mathfrak{m}}} \, pr \, K_{\overline{\mathfrak{n}}}$.
(c) Prove that $H_{\mathfrak{m}}$ is projective relative to K if and only if $H_{\overline{\mathfrak{m}}}$ is projective relative to K.
(d) Prove that $H_{\mathfrak{m}}$ is primordial for A if and only if $H_{\overline{\mathfrak{m}}}$ is primordial for A/I.

(55.4) Let A be a Green functor for G, let $H_{\mathfrak{m}}$ be a pointed group on A, and let K be a subgroup of G.
(a) If $K \geq H$, prove that there exists $\mathfrak{n} \in \mathrm{Max}(A(K))$ with $K_{\mathfrak{n}} \geq H_{\mathfrak{m}}$.
(b) Assume that both $A(K)$ and $A(H)$ are finite dimensional algebras over a field (or more generally $\mathcal{O}$-algebras which are finitely generated as $\mathcal{O}$-modules, where $\mathcal{O}$ is a complete local ring, as in Chapter 1). If $K \leq H$ and $\mathrm{Ker}(r^H_K) \subseteq \mathfrak{m}$, prove that there exists $\mathfrak{n} \in \mathrm{Max}(A(K))$ such that $K_{\mathfrak{n}} \leq H_{\mathfrak{m}}$. [Hint: The assumption allows us to use idempotents and points instead of maximal ideals. Then proceed as in part (a) of Exercise 13.5. The next exercise shows that the result may not hold without the assumption. Note also that the condition $\mathrm{Ker}(r^H_K) \subseteq \mathfrak{m}$ is always an obvious necessary condition for the existence of $\mathfrak{n}$.]

(55.5) Let G be a cyclic group of prime order p, let k be a field of characteristic p, let $A(G) = k[t]$ be the ring of polynomials in one variable t, and let $A(1) = k[[t]]$ be the ring of formal power series in t. Let $r^G_1 : A(G) \to A(1)$ be the inclusion map, let $t^G_1 = 0$, and let G act trivially on $A(1)$.
(a) Prove that A is a Green functor for G over k.

(b) Let $a \in k$ and consider the maximal ideal $(t-a)$ of $k[t]$ generated by $t-a$. If $a=0$, prove that $G_{(t)} \geq 1_{(t)}$. If $a \neq 0$, prove that the pointed group $G_{(t-a)}$ is minimal (with respect to $\geq$).
(c) Prove that every pointed group on A is primordial.
(d) Prove that $1_{(t)}$ is maximal with respect to the relation pr.

(55.6) Let A be a Green functor for G, let $P_{\mathfrak{p}}$ be a primordial pointed group on A with corresponding surjection $\pi_{\mathfrak{p}} : A(P) \to A(P)/\mathfrak{p}$, and let $P \leq K \leq H \leq G$. Prove that if $a \in A(K)$ has the form $a = t_P^K(b)$ for some $b \in A(P)$ satisfying $b \in {}^h\mathfrak{p}$ for every $h \in N_H(P) - N_H(P_{\mathfrak{p}})$, then

$$\pi_{\mathfrak{p}}\, r_P^H\, t_K^H(a) = t_{\overline{N}_K(P_{\mathfrak{p}})}^{\overline{N}_H(P_{\mathfrak{p}})}\, \pi_{\mathfrak{p}}\, r_P^K(a)\,,$$

where $t_{\overline{N}_K(P_{\mathfrak{p}})}^{\overline{N}_H(P_{\mathfrak{p}})}$ is the relative trace map in the $\overline{N}_G(P_{\mathfrak{p}})$-algebra $A(P)/\mathfrak{p}$. [Hint: See Corollary 14.8.]

Notes on Section 55

The generalization to Green functors of the notions of pointed group, containment and relative projectivity appears in Thévenaz [1991], but the consideration of maximal ideals in various specific examples has been widely used before (in particular in the case of representation rings, cohomology rings, or rings of algebraic integers of Galois extensions). The proof of the result mentioned in Remark 55.12 can be found in Thévenaz [1991].

§ 56 DEFECT THEORY FOR MAXIMAL IDEALS

In this section, we extend the defect theory of pointed groups to the case of Green functors. We first introduce defect groups and then defect pointed groups. We prove the existence of defect pointed groups under a very mild assumption which is always satisfied in current examples.

We start with the crucial lemma.

(56.1) LEMMA. *Let A be a Green functor for G, let P be a subgroup of G, let $\mathfrak{q}$ be a primordial ideal of $A(P)$, and let $H_{\mathfrak{m}}$ and $K_{\mathfrak{n}}$ be two pointed groups on A satisfying the following two conditions:*
(a) $H_{\mathfrak{m}}\, pr\, K_{\mathfrak{n}}$,
(b) $P \leq H$ and $(r_P^H)^{-1}(\mathfrak{q}) \subseteq \mathfrak{m}$.
Then there exists $h \in H$ such that ${}^hP \leq K$ and $(r_{{}^hP}^K)^{-1}({}^h\mathfrak{q}) \subseteq \mathfrak{n}$.

Proof. Let $X = \{ h \in H \mid {}^hP \leq K \}$ and consider the ideal of $A(K)$

$$\mathfrak{a} = \bigcap_{h \in X} (r^K_{{}^hP})^{-1}({}^h\mathfrak{q}).$$

We shall prove below that $\mathfrak{a}$ is a proper ideal, so that X is non-empty. By the Mackey axiom, we have

$$\begin{aligned} r^H_P\, t^H_K(\mathfrak{a}) &= \sum_{h \in [P\backslash H/K]} t^P_{P\cap {}^hK}\, r^{{}^hK}_{P\cap {}^hK}({}^h\mathfrak{a}) \\ &\subseteq \sum_{Q<P} t^P_Q(A(Q)) + \sum_{h^{-1}\in X} r^{{}^hK}_P({}^h\mathfrak{a}) . \end{aligned}$$

We have $\sum_{Q<P} t^P_Q(A(Q)) = \mathrm{Ker}(br_P) \subseteq \mathfrak{q}$ since $\mathfrak{q}$ is primordial. The second sum is also contained in $\mathfrak{q}$ because $r^K_{{}^xP}(\mathfrak{a}) \subseteq {}^x\mathfrak{q}$ if $h^{-1} = x \in X$, by definition of $\mathfrak{a}$. Therefore $r^H_P\, t^H_K(\mathfrak{a}) \subseteq \mathfrak{q}$, and so $t^H_K(\mathfrak{a}) \subseteq (r^H_P)^{-1}(\mathfrak{q})$. By assumption (b), it follows that $t^H_K(\mathfrak{a}) \subseteq \mathfrak{m}$, that is, $\mathfrak{a} \subseteq (t^H_K)^{-1}(\mathfrak{m})$, and this implies $\mathfrak{a} \subseteq (t^H_K)^{-1}(\mathfrak{m})^\circ$. Since $H_\mathfrak{m}\, pr\, K_\mathfrak{n}$, it follows that $\mathfrak{a} \subseteq \mathfrak{n}$. By Corollary 55.3 and the definition of $\mathfrak{a}$, there exists $h \in X$ such that $(r^K_{{}^hP})^{-1}({}^h\mathfrak{q}) \subseteq \mathfrak{n}$. □

Our first application of the lemma has to do with subgroups and will be used for the main result on defect groups.

(56.2) COROLLARY. *Let A be a Green functor for G, let P and K be subgroups of G, and let $H_\mathfrak{m}$ be a pointed group on A satisfying the following two conditions:*
(a) $H_\mathfrak{m}$ is projective relative to K,
(b) $P \leq H$ and $\mathrm{Ker}(br_P\, r^H_P) \subseteq \mathfrak{m}$.
Then there exists $h \in H$ such that ${}^hP \leq K$.

Proof. We apply Lemma 56.1 with $\mathfrak{q} = \mathrm{Ker}(br_P)$. Since $\mathrm{Ker}(br_P\, r^H_P)$ is a proper ideal by (b), the ideal $\mathrm{Ker}(br_P)$ is proper, hence primordial. By (a), we have $H_\mathfrak{m}\, pr\, K_\mathfrak{n}$ for some $\mathfrak{n} \in \mathrm{Max}(A(K))$. On the other hand (b) asserts that $(r^H_P)^{-1}(\mathrm{Ker}(br_P)) \subseteq \mathfrak{m}$. Therefore both conditions of Lemma 56.1 are satisfied and the first conclusion of the lemma yields the result. □

Our second application of Lemma 56.1 has to do with pointed groups and has already been proved for pointed groups on a G-algebra over $\mathcal{O}$ (see Lemma 18.2). The result will be used for the main theorem on defect pointed groups.

(56.3) COROLLARY. *Let A be a Green functor for G and let $H_{\mathfrak{m}}$, $K_{\mathfrak{n}}$, and $P_{\mathfrak{p}}$ be pointed groups on A satisfying the following two conditions:*
(a) $H_{\mathfrak{m}} \, pr \, K_{\mathfrak{n}}$,
(b) $P_{\mathfrak{p}}$ *is primordial and* $H_{\mathfrak{m}} \geq P_{\mathfrak{p}}$.
Then there exists $h \in H$ such that $K_{\mathfrak{n}} \geq {}^h(P_{\mathfrak{p}})$.

Proof. We apply Lemma 56.1 with $\mathfrak{q} = \mathfrak{p}$, which is primordial by assumption (b). Since (b) also implies that $P \leq H$ and $(r^H_P)^{-1}(\mathfrak{p}) \subseteq \mathfrak{m}$, the conditions of Lemma 56.1 are satisfied. The conclusion of the lemma yields precisely the result. □

A third application of Lemma 56.1 will be given in the next section.

Let $H_{\mathfrak{m}}$ be a pointed group on a Green functor A for G. Since the homomorphism β_H of Proposition 54.4 has nilpotent kernel, we have

$$\mathfrak{m} \supseteq \mathrm{Ker}(\beta_H) = \bigcap_{P \leq H} \mathrm{Ker}(br_P \, r^H_P),$$

by Lemma 55.1 and the definition of β_H. By Corollary 55.3, it follows that there exists a subgroup P such that $\mathfrak{m} \supseteq \mathrm{Ker}(br_P \, r^H_P)$. On the other hand it is clear that there exists a subgroup Q such that $H_{\mathfrak{m}}$ is projective relative to Q (for instance $Q = H$). We now show in a direct way that there exists in fact a subgroup satisfying both properties.

We define a *defect group* of $H_{\mathfrak{m}}$ to be a subgroup P of H such that $H_{\mathfrak{m}}$ is projective relative to P and such that $\mathfrak{m} \supseteq \mathrm{Ker}(br_P \, r^H_P)$.

(56.4) LEMMA. *Let A be a Green functor for G and let $H_{\mathfrak{m}}$ be a pointed group on A. Then a defect group of $H_{\mathfrak{m}}$ exists.*

Proof. Let P be a minimal subgroup such that $H_{\mathfrak{m}}$ is projective relative to P and let $\mathfrak{a} = (t^H_P)^{-1}(\mathfrak{m})^\circ$. We claim that the following two properties hold.
(a) $\mathfrak{a}$ is a primordial ideal, that is, $\mathrm{Ker}(br_P) \subseteq \mathfrak{a} \neq A(P)$.
(b) $(r^H_P)^{-1}(\mathfrak{a}) \subseteq \mathfrak{m}$.
The result follows from this because

$$\mathrm{Ker}(br_P \, r^H_P) = (r^H_P)^{-1}(\mathrm{Ker}(br_P)) \subseteq (r^H_P)^{-1}(\mathfrak{a}) \subseteq \mathfrak{m}.$$

First note that $\mathfrak{a}$ is a proper ideal by definition of relative projectivity (Lemma 55.7). By minimality of P, we have $(t^H_Q)^{-1}(\mathfrak{m}) = A(Q)$ if $Q < P$. Therefore $t^P_Q(A(Q)) \subseteq (t^H_P)^{-1}(\mathfrak{m})$ (because $t^H_Q = t^H_P \, t^P_Q$), so that $t^P_Q(A(Q)) \subseteq \mathfrak{a}$ (because $t^P_Q(A(Q))$ is an ideal). Summing over all proper subgroups of P, we deduce that $\mathrm{Ker}(br_P) \subseteq \mathfrak{a}$, proving (a).

For the proof of (b), suppose that $(r_P^H)^{-1}(\mathfrak{a}) \not\subseteq \mathfrak{m}$, so that there exists $a \in (r_P^H)^{-1}(\mathfrak{a})$ and $b \in \mathfrak{m}$ such that $a + b = 1_{A(H)}$. Then we have

$$\begin{aligned} t_P^H(A(P)) &= t_P^H(A(P))\,(a+b) = t_P^H(A(P)\,r_P^H(a)) + t_P^H(A(P))\,b \\ &\subseteq t_P^H(\mathfrak{a}) + \mathfrak{m} \subseteq \mathfrak{m}, \end{aligned}$$

because $t_P^H(\mathfrak{a}) \subseteq \mathfrak{m}$ by definition of $\mathfrak{a}$. This contradicts the assumption that $H_\mathfrak{m}$ is projective relative to P (Lemma 55.7). □

We can now state the main theorem on defect groups, which extends the result for a pointed group on a G-algebra over $\mathcal{O}$ (Proposition 18.5).

(56.5) THEOREM. *Let A be a Green functor for G and let $H_\mathfrak{m}$ be a pointed group on A.*

(a) All defect groups of $H_\mathfrak{m}$ are conjugate under H.

(b) The following conditions on a subgroup P are equivalent.

(i) P is a defect group of $H_\mathfrak{m}$.

(ii) P is a minimal subgroup such that $H_\mathfrak{m}$ is projective relative to P.

(iii) P is a maximal subgroup such that $P \leq H$ and $\mathrm{Ker}(br_P\, r_P^H) \subseteq \mathfrak{m}$.

Proof. We first prove (b). Let Q be a defect group of $H_\mathfrak{m}$, which exists by Lemma 56.4.

(i) ⇒ (ii). Let R be a subgroup such that $H_\mathfrak{m}$ is projective relative to R and $P \geq R$. By Corollary 56.2, there exists $h \in H$ such that ${}^hP \leq R$. This forces the equality $P = R$, proving the minimality condition on P.

(ii) ⇒ (iii). Since $H_\mathfrak{m}$ is projective relative to P, there exists $h \in H$ such that ${}^hQ \leq P$ (Corollary 56.2). By minimality of P, it follows that ${}^hQ = P$. In particular $P \leq H$ and $\mathrm{Ker}(br_P\, r_P^H) \subseteq \mathfrak{m}$ (because the same property holds for Q and is invariant under H-conjugation). Let R be a subgroup such that $P \leq R \leq H$ and $\mathrm{Ker}(br_R\, r_R^H) \subseteq \mathfrak{m}$. By Corollary 56.2, there exists $h' \in H$ such that ${}^{h'}R \leq P$. This forces the equality $P = R$, proving the maximality condition on P.

(iii) ⇒ (i). Since $P \leq H$ and $\mathrm{Ker}(br_P\, r_P^H) \subseteq \mathfrak{m}$, there exists $h \in H$ such that ${}^hP \leq Q$ (Corollary 56.2). By maximality of P, it follows that ${}^hP = Q$. In particular $H_\mathfrak{m}$ is projective relative to P (because the same property holds for Q and is invariant under H-conjugation). Thus P is a defect group of $H_\mathfrak{m}$.

We have seen in the proof that any subgroup satisfying either (ii) or (iii) is H-conjugate to Q. This shows that all subgroups satisfying the equivalent conditions are conjugate under H, proving (a). □

For later use, we state the following result, which was established in the proof of Lemma 56.4.

(56.6) LEMMA. *Let* A *be a Green functor for* G *, let* $H_{\mathfrak{m}}$ *be a pointed group on* A *, let* P *be a defect group of* $H_{\mathfrak{m}}$ *, and let* $\mathfrak{a} = (t_P^H)^{-1}(\mathfrak{m})^\circ$ *. Then the following two properties hold.*
(a) $\mathfrak{a}$ *is a primordial ideal, that is,* $\mathrm{Ker}(br_P) \subseteq \mathfrak{a} \neq A(P)$ *.*
(b) $(r_P^H)^{-1}(\mathfrak{a}) \subseteq \mathfrak{m}$ *.*

Now we turn to the definition and properties of defect pointed groups. The treatment is almost identical with that of defect groups, except for the question of existence, which is more difficult. In fact we shall prove the existence of defect pointed groups under some additional mild assumption. Moreover we shall actually use a result on defect groups for one of the equivalent characterizations of defect pointed groups.

Let $H_{\mathfrak{m}}$ be a pointed group on a Green functor A for G . A pointed group $P_{\mathfrak{p}}$ on A is called a *defect pointed group* of $H_{\mathfrak{m}}$, or simply a *defect* of $H_{\mathfrak{m}}$, if $H_{\mathfrak{m}} \geq P_{\mathfrak{p}}$, $H_{\mathfrak{m}}\, pr\, P_{\mathfrak{p}}$, and $P_{\mathfrak{p}}$ is primordial. If $P_{\mathfrak{p}}$ is a defect of $H_{\mathfrak{m}}$, then the maximal ideal $\mathfrak{p}$ is called a *source* of $H_{\mathfrak{m}}$. We first relax slightly one of the conditions in the definition.

(56.7) LEMMA. *Let* $H_{\mathfrak{m}}$ *and* $P_{\mathfrak{p}}$ *be two pointed groups on a Green functor* A *for* G *. If* $P_{\mathfrak{p}}$ *is primordial,* $H_{\mathfrak{m}} \geq P_{\mathfrak{p}}$ *, and* $H_{\mathfrak{m}}$ *is projective relative to* P *, then* $P_{\mathfrak{p}}$ *is a defect pointed group of* $H_{\mathfrak{m}}$ *.*

Proof. There exists $\mathfrak{q} \in \mathrm{Max}(A(P))$ such that $H_{\mathfrak{m}}\, pr\, P_{\mathfrak{q}}$ because $H_{\mathfrak{m}}$ is projective relative to P . By Corollary 56.3, there exists $h \in H$ such that $P_{\mathfrak{q}} \geq {}^h(P_{\mathfrak{p}})$ so that $h \in N_H(P)$ and $P_{\mathfrak{q}} = {}^h(P_{\mathfrak{p}})$. Conjugating by h^{-1} the relation $H_{\mathfrak{m}}\, pr\, P_{\mathfrak{q}}$, we obtain $H_{\mathfrak{m}}\, pr\, P_{\mathfrak{p}}$ by Exercise 55.1, as was to be shown. □

Next we establish the expected connection with defect groups.

(56.8) LEMMA. *Let* $H_{\mathfrak{m}}$ *be a pointed group on a Green functor* A *for* G *. If* $P_{\mathfrak{p}}$ *is a defect pointed group of* $H_{\mathfrak{m}}$ *, then* P *is a defect group of* $H_{\mathfrak{m}}$ *.*

Proof. The property $H_{\mathfrak{m}}\, pr\, P_{\mathfrak{p}}$ implies that $H_{\mathfrak{m}}$ is projective relative to P . Moreover since $\mathfrak{p}$ is primordial, we have $\mathrm{Ker}(br_P) \subseteq \mathfrak{p}$, and since $H_{\mathfrak{m}} \geq P_{\mathfrak{p}}$, we have $(r_P^H)^{-1}(\mathfrak{p}) \subseteq \mathfrak{m}$. Therefore

$$\mathrm{Ker}(br_P\, r_P^H) \;=\; (r_P^H)^{-1}(\mathrm{Ker}(br_P)) \;\subseteq\; (r_P^H)^{-1}(\mathfrak{p}) \;\subseteq\; \mathfrak{m}\,,$$

as required. □

Postponing the question of existence of defects, we state the main result of defect theory, which is an extension of Theorem 18.3. The words *minimal* and *maximal* always refer to the containment relation $\geq$ between pointed groups.

(56.9) THEOREM. *Let $H_{\mathfrak{m}}$ be a pointed group on a Green functor A for G. Assume that a defect pointed group of $H_{\mathfrak{m}}$ exists.*
(a) All defect pointed groups of $H_{\mathfrak{m}}$ are conjugate under H.
(b) The following conditions on a pointed group $P_{\mathfrak{p}}$ on A are equivalent.
(i) $P_{\mathfrak{p}}$ is a defect of $H_{\mathfrak{m}}$.
(ii) $P_{\mathfrak{p}}$ is a minimal pointed group such that $H_{\mathfrak{m}}\, pr\, P_{\mathfrak{p}}$.
(iii) $P_{\mathfrak{p}}$ is a maximal pointed group such that $P_{\mathfrak{p}}$ is primordial and $H_{\mathfrak{m}} \geq P_{\mathfrak{p}}$.
(iv) $H_{\mathfrak{m}}\, pr\, P_{\mathfrak{p}}$ and $\mathrm{Ker}(br_P\, r^H_P) \subseteq \mathfrak{m}$.

Proof. Let $Q_{\mathfrak{q}}$ be a defect of $H_{\mathfrak{m}}$, which exists by assumption. Many steps of the proof are identical with the corresponding arguments in Theorem 18.3 (the use of Lemma 18.2 being of course replaced by the use of the corresponding Corollary 56.3). This remark applies to the proof of the implications (i) $\Rightarrow$ (ii) and (ii) $\Rightarrow$ (iii), and also to the proof of (a). Condition (iv) is stated slightly differently, because we had $br_P\, r^H_P(\alpha) \neq 0$ in Theorem 18.3, but this is equivalent to $\mathrm{Ker}(br_P\, r^H_P) \subseteq \mathfrak{m}_\alpha$ by Corollary 4.10. The additional condition (v) in Theorem 18.3 corresponds to Lemma 56.7 here, but the proof of the implication (iv) $\Rightarrow$ (v) in Theorem 18.3 does not apply in our general situation. Thus we give a complete proof of the implications involving (iv).

(iii) $\Rightarrow$ (iv). By Corollary 56.3 (applied to $H_{\mathfrak{m}}$, $Q_{\mathfrak{q}}$ and $P_{\mathfrak{p}}$), we have ${}^h(Q_{\mathfrak{q}}) \geq P_{\mathfrak{p}}$ for some $h \in H$, and by maximality of $P_{\mathfrak{p}}$ it follows that $P_{\mathfrak{p}} = {}^h(Q_{\mathfrak{q}})$. In particular $H_{\mathfrak{m}}\, pr\, P_{\mathfrak{p}}$, proving the first statement. Moreover, as in the proof of Lemma 56.8, we have

$$\mathrm{Ker}(br_P\, r^H_P) \;=\; (r^H_P)^{-1}(\mathrm{Ker}(br_P)) \;\subseteq\; (r^H_P)^{-1}(\mathfrak{p}) \;\subseteq\; \mathfrak{m}\,,$$

because $\mathfrak{p}$ is primordial and $H_{\mathfrak{m}} \geq P_{\mathfrak{p}}$.

(iv) $\Rightarrow$ (i). By Corollary 56.3 (applied to $H_{\mathfrak{m}}$, $P_{\mathfrak{p}}$ and $Q_{\mathfrak{q}}$), we have $P_{\mathfrak{p}} \geq {}^h(Q_{\mathfrak{q}})$ for some $h \in H$. By Lemma 56.8, Q is a defect group of $H_{\mathfrak{m}}$. On the other hand condition (iv) implies immediately that P is a defect group of $H_{\mathfrak{m}}$. By Theorem 56.5, P and Q are conjugate (or simply P is contained in a conjugate of Q by Corollary 56.2). Together with the above containment relation $P_{\mathfrak{p}} \geq {}^h(Q_{\mathfrak{q}})$, this implies that $P_{\mathfrak{p}} = {}^h(Q_{\mathfrak{q}})$. Therefore $P_{\mathfrak{p}}$ is primordial and is contained in $H_{\mathfrak{m}}$, because these properties hold for $Q_{\mathfrak{q}}$ and are invariant under H-conjugation. This proves that $P_{\mathfrak{p}}$ satisfies the conditions of Lemma 56.7, proving (i). □

We are left with the question of the existence of defect pointed groups. There is an easy direct proof for pointed groups containing a *maximal* primordial pointed group (Exercise 56.2). In the general case, we prove the existence of defects under the following assumption.

(56.10) ASSUMPTION. Let A be a Green functor for G. For every subgroup H of G, assume that every maximal left ideal of $A(H)$ contains a maximal two-sided ideal.

In other words if M is a maximal left ideal of $A(H)$, the two-sided ideal M° is assumed to be maximal. We shall discuss this assumption after the proof of the theorem.

Here is the crucial result. The method is an extension to the non-commutative case of the arguments used in Proposition 55.11.

(56.11) THEOREM. *Let A be a Green functor for G over R satisfying Assumption 56.10. Let $H_{\mathfrak{m}}$ be a pointed group on A and let K be a subgroup of G such that $H_{\mathfrak{m}}$ is projective relative to K. Then there exists $\mathfrak{n} \in \mathrm{Max}(A(K))$ such that $H_{\mathfrak{m}} \geq K_{\mathfrak{n}}$ and $H_{\mathfrak{m}}\, pr\, K_{\mathfrak{n}}$.*

Proof. Let $M = (t_K^H)^{-1}(\mathfrak{m})$, an R-submodule of $A(K)$, and let $M^\vee$ be the unique largest left ideal contained in M, that is, the sum of all left ideals contained in M. Similarly let M° be the unique largest two-sided ideal contained in M, so that $M^\circ \subseteq M^\vee \subseteq M$. By the Frobenius axiom, we have

$$t_K^H\big(A(K) \cdot r_K^H(\mathfrak{m})\big) = t_K^H(A(K)) \cdot \mathfrak{m} \subseteq \mathfrak{m},$$

and therefore $A(K) \cdot r_K^H(\mathfrak{m}) \subseteq M$, hence $A(K) \cdot r_K^H(\mathfrak{m}) \subseteq M^\vee$. Let N be a maximal left ideal containing $M^\vee$, which exists by Zorn's lemma (and the fact that the unity element never belongs to a proper left ideal), and consider the two-sided ideal $\mathfrak{n} = N^\circ$. Then $\mathfrak{n}$ is a maximal ideal of $A(K)$ by Assumption 56.10. The inclusion $N \supseteq M^\vee$ implies $\mathfrak{n} \supseteq M^\circ$, and this means precisely that $H_{\mathfrak{m}}\, pr\, K_{\mathfrak{n}}$.

Since $r_K^H(\mathfrak{m}) \subseteq M^\vee \subseteq N$, we have $\mathfrak{m} \subseteq (r_K^H)^{-1}(N)$ and therefore $\mathfrak{m} \subseteq (r_K^H)^{-1}(N)^\circ$. By maximality of $\mathfrak{m}$, we obtain $\mathfrak{m} = (r_K^H)^{-1}(N)^\circ$, because $1_{A(H)} \notin (r_K^H)^{-1}(N)$. Now the inclusion $\mathfrak{n} \subseteq N$ implies that

$$(r_K^H)^{-1}(\mathfrak{n}) \subseteq (r_K^H)^{-1}(N)^\circ = \mathfrak{m}$$

because $(r_K^H)^{-1}(\mathfrak{n})$ is a two-sided ideal. This means that $H_{\mathfrak{m}} \geq K_{\mathfrak{n}}$. □

(56.12) COROLLARY. *Let A be a Green functor for G satisfying Assumption 56.10 and let $H_{\mathfrak{m}}$ be a pointed group on A. Then a defect pointed group of $H_{\mathfrak{m}}$ exists.*

Proof. Let P be a minimal subgroup such that $H_{\mathfrak{m}}$ is projective relative to P (that is, a defect group of $H_{\mathfrak{m}}$ by Theorem 56.5). By Theorem 56.11, there exists $\mathfrak{p} \in \mathrm{Max}(A(P))$ such that $H_{\mathfrak{m}} \, pr \, P_{\mathfrak{p}}$ and $H_{\mathfrak{m}} \geq P_{\mathfrak{p}}$. Finally $P_{\mathfrak{p}}$ is primordial by the minimal choice of P. Indeed if $P_{\mathfrak{p}} \, pr \, Q_{\mathfrak{q}}$, then $H_{\mathfrak{m}} \, pr \, Q_{\mathfrak{q}}$ and $H_{\mathfrak{m}}$ is projective relative to Q, so that $Q = P$ and $Q_{\mathfrak{q}} = P_{\mathfrak{p}}$. □

Theorem 56.11 also has the following consequence on the poset of pointed groups.

(56.13) COROLLARY. *Let A be a Green functor for G satisfying Assumption 56.10. Then every minimal pointed group on A is primordial.*

Proof. Let $H_{\mathfrak{m}}$ be a minimal pointed group on A and let $P_{\mathfrak{p}}$ be a defect of $H_{\mathfrak{m}}$ (which exists by Corollary 56.12). The relation $H_{\mathfrak{m}} \geq P_{\mathfrak{p}}$ implies that $H_{\mathfrak{m}} = P_{\mathfrak{p}}$ by minimality. Therefore $H_{\mathfrak{m}}$ is primordial. □

The proof of Theorem 56.11 uses an analysis of the discrepancy between one-sided and two-sided ideals. In the commutative case, the same method was used in Proposition 55.11 and yielded the much stronger fact that the relation pr implies the relation $\geq$. In particular we deduce the following result.

(56.14) COROLLARY. *Let A be a Green functor for G and assume that $A(H)$ is commutative for every subgroup H of G. Let $H_{\mathfrak{m}}$ and $P_{\mathfrak{p}}$ be two pointed groups on A. If the condition $H_{\mathfrak{m}} \, pr \, P_{\mathfrak{p}}$ holds and if, with respect to the relation pr, $P_{\mathfrak{p}}$ is minimal such that this condition holds, then $P_{\mathfrak{p}}$ is a defect of $H_{\mathfrak{m}}$.*

Proof. The proof is easy and is left to the reader. □

Finally we discuss Assumption 56.10 and indicate why it holds in all current examples of Green functors. It is obvious that the assumption is satisfied in the commutative case. In fact the existence of defect pointed groups in that case is provided by the much more precise result above.

Note first that every maximal left ideal M of a ring F defines a simple left F-module F/M, and conversely every simple F-module arises in this way up to isomorphism (because it is generated by a single element). Moreover if M is a maximal left ideal, then it is not difficult to prove that the annihilator of the simple module F/M is the two-sided ideal M°. By construction F/M° acts faithfully on F/M, and this is the definition of a primitive ring (this has nothing to do with the notion of primitivity defined earlier for G-algebras). Thus, for a Green functor A for G, Assumption 56.10 can be rephrased as follows: for every subgroup H of G, the annihilator of every simple $A(H)$-module is a maximal (two-sided) ideal. In other words the assumption means that all primitive quotient rings $A(H)/M^\circ$ are simple rings. In Section 58, we shall only work with simple rings which are finite dimensional algebras over a field (in which case Wedderburn's theorem applies), but we do not need this restriction here.

Suppose that R is a field, or more generally a complete local commutative ring (as in Chapter 1). If A is a Green functor for G over R such that every $A(H)$ is finitely generated as an R-module, then Assumption 56.10 holds. Indeed we have seen in Theorem 1.10 and Theorem 4.3 that the annihilator of a simple module is a maximal ideal. It follows that Theorem 56.11 above holds in that case, but alternatively one can also use idempotents to prove the result directly (Exercise 56.4).

The above observations show that Assumption 56.10 holds in most examples mentioned in Section 53. However, the case of cohomology rings is not covered by the discussion so far. This is our next example.

(56.15) EXAMPLE. Let R be an algebraically closed field of prime characteristic p, let N be a finitely generated RG-module, and let A be the Green functor for G defined in Example 53.4, namely

$$A(H) = \mathrm{Ext}^*_{RH}(N,N) \cong H^*(H, \mathrm{End}_R(N)) .$$

Then it can be proved that A satisfies Assumption 56.10. In fact every simple $A(H)$-module $A(H)/M$ and every simple algebra $A(H)/\mathfrak{m}$ are finite dimensional over R (where M is a maximal left ideal and $\mathfrak{m}$ is a maximal two-sided ideal).

Exercises

(56.1) Let A be a Green functor for G and let I be a functorial ideal of A. Let $H_{\mathfrak{m}}$ and $P_{\mathfrak{p}}$ be pointed groups on A coming from pointed groups $H_{\overline{\mathfrak{m}}}$ and $P_{\overline{\mathfrak{p}}}$ on A/I. Prove that $P_{\mathfrak{p}}$ is a defect of $H_{\mathfrak{m}}$ if and only if $P_{\overline{\mathfrak{p}}}$ is a defect of $H_{\overline{\mathfrak{m}}}$.

(56.2) Let A be a Green functor for G and let $P_{\mathfrak{p}}$ be a maximal primordial pointed group on A. Prove that $P_{\mathfrak{p}}$ is a defect pointed group of any pointed group $H_{\mathfrak{m}}$ containing $P_{\mathfrak{p}}$. [Hint: Show that if Q is a defect group of $H_{\mathfrak{m}}$, then $H_{\mathfrak{m}}\, pr\, Q_{\mathfrak{q}}$ for some primordial maximal ideal $\mathfrak{q}$. Then use Corollary 56.3 to show that $P_{\mathfrak{p}}$ and $Q_{\mathfrak{q}}$ are H-conjugate.]

(56.3) Prove Corollary 56.14.

(56.4) Suppose that R is a field, or more generally a complete local commutative ring, and let A be a Green functor for G over R such that every $A(H)$ is finitely generated as an R-module. Prove Theorem 56.11 directly using idempotents. [Hint: Use the method of Lemma 18.1.]

Notes on Section 56

In the special case of G-algebras (over an arbitrary base ring R), the existence of defect groups for maximal ideals was first observed by Dade [1973]. The extension of the theory to the case of maximal ideals in Green functors (and in particular the introduction of sources, or in other words defect pointed groups) is due to Thévenaz [1991]. More details about the theory as well as examples can be found in Thévenaz [1990, 1991]. The facts mentioned in Example 56.15 are due to Carlson [1985].

§ 57 FUNCTORIAL IDEALS AND DEFECT THEORY

In this section, we associate a functorial ideal with every pointed group on a Green functor and we give a detailed description of these functorial ideals. Furthermore we show that the defect theory can in fact be entirely described in terms of functorial ideals and this shed some new light on this theory even in the case of G-algebras considered in Chapter 3.

Let A be a Green functor for G and let $\{I_j \mid j \in J\}$ be a family of functorial ideals of A. Define the subfunctor $\sum_{j\in J} I_j$ of A by $(\sum_{j\in J} I_j)(H) = \sum_{j\in J} I_j(H)$ for every subgroup H of G. It is straightforward to check that $\sum_{j\in J} I_j$ is again a functorial ideal of A.

Let $H_{\mathfrak{m}}$ be a pointed group on A. The sum of all functorial ideals I of A satisfying $I(H) \subseteq \mathfrak{m}$ is a functorial ideal and is the unique largest functorial ideal of A with this property. It is called the functorial ideal *associated with* $H_{\mathfrak{m}}$, and is written $I_{H_{\mathfrak{m}}}$. It is easy to prove that, for every $g \in G$, we have $I_{{}^g(H_{\mathfrak{m}})} = I_{H_{\mathfrak{m}}}$ (Exercise 57.1).

If I and J are two functorial ideals, then the inclusion $J \subseteq I$ means by definition that $J(K) \subseteq I(K)$ for every subgroup K of G. If $I_{H_{\mathfrak{m}}}$ is the functorial ideal associated with a pointed group $H_{\mathfrak{m}}$ and if J is an arbitrary functorial ideal, then $J \subseteq I_{H_{\mathfrak{m}}}$ if and only if $J(H) \subseteq \mathfrak{m}$. This in turn is equivalent to the condition that $H_{\mathfrak{m}}$ comes from A/J. Thus $J \subseteq I_{H_{\mathfrak{m}}}$ if and only if $H_{\mathfrak{m}}$ comes from A/J.

Here is a first description of $I_{H_{\mathfrak{m}}}$. More precise information will be given later in Corollary 57.6.

(57.1) PROPOSITION. *Let A be a Green functor for G.*

(a) Let $H_{\mathfrak{m}}$ be a pointed group on A, let $I_{H_{\mathfrak{m}}}$ be its associated functorial ideal, let P be a defect group of $H_{\mathfrak{m}}$, and let $\mathfrak{a} = (t_P^H)^{-1}(\mathfrak{m})^\circ$. Then, for every subgroup K of G, we have

$$I_{H_{\mathfrak{m}}}(K) = \bigcap_{\substack{g\in G \\ {}^gP\le K}} (r^K_{{}^gP})^{-1}({}^g\mathfrak{a})\,.$$

In particular $I_{H_{\mathfrak{m}}}(K) = A(K)$ if K does not contain a G-conjugate of P.

(b) Let $P_{\mathfrak{p}}$ be a primordial pointed group on A and let $I_{P_{\mathfrak{p}}}$ be its associated functorial ideal. Then, for every subgroup K of G, we have

$$I_{P_{\mathfrak{p}}}(K) = \bigcap_{\substack{g\in G \\ {}^gP\le K}} (r^K_{{}^gP})^{-1}({}^g\mathfrak{p})\,.$$

In particular $I_{P_{\mathfrak{p}}}(K) = A(K)$ if K does not contain a G-conjugate of P.

Proof. First note that (b) is a special case of (a), because a primordial pointed group $P_{\mathfrak{p}}$ is its own defect and the ideal $\mathfrak{a}$ is equal to $\mathfrak{p}$ in that case. We now prove (a). For every $K \leq G$, consider the ideal

$$I(K) = \bigcap_{\substack{g \in G \\ {}^gP \leq K}} (r^K_{{}^gP})^{-1}({}^g\mathfrak{a}) .$$

We claim that I is a functorial ideal of A. It is easy to check that I is invariant under conjugation and restriction (Exercise 57.2). In order to deal with transfer, let $K \leq L \leq G$. By definition of $I(L)$, the inclusion $t^L_K(I(K)) \subseteq I(L)$ will follow if we prove that $r^L_{{}^gP}\, t^L_K(I(K)) \subseteq {}^g\mathfrak{a}$ for every $g \in G$ such that ${}^gP \leq L$. Applying the Mackey axiom, it suffices to show that, for every $x \in L$, we have

$$t^{\,{}^gP}_{{}^gP \cap {}^xK}\, r^{\,{}^xK}_{{}^gP \cap {}^xK}(I({}^xK)) \subseteq {}^g\mathfrak{a} .$$

By Lemma 56.6, the ideal $\mathfrak{a}$ is primordial and therefore so is ${}^g\mathfrak{a}$. If ${}^gP \cap {}^xK < {}^gP$, it follows that the image of $t^{\,{}^gP}_{{}^gP \cap {}^xK}$ is contained in ${}^g\mathfrak{a}$, as required. If now ${}^gP \cap {}^xK = {}^gP$, then $r^{\,{}^xK}_{{}^gP}(I({}^xK)) \subseteq {}^g\mathfrak{a}$ by definition of $I({}^xK)$. This completes the proof that I is a functorial ideal.

By the second statement of Lemma 56.6, we have $(r^H_P)^{-1}(\mathfrak{a}) \subseteq \mathfrak{m}$, and therefore $I(H) \subseteq \mathfrak{m}$. Thus, in order to prove that $I = I_{H_\mathfrak{m}}$, it suffices to show that any functorial ideal J of A such that $J(H) \subseteq \mathfrak{m}$ is contained in I. Since $t^H_P(J(P)) \subseteq J(H)$, we have

$$J(P) \subseteq (t^H_P)^{-1}(J(H))^\circ \subseteq (t^H_P)^{-1}(\mathfrak{m})^\circ = \mathfrak{a} .$$

Therefore $J({}^gP) = {}^g(J(P)) \subseteq {}^g\mathfrak{a}$ for every $g \in G$. If g is such that ${}^gP \leq K$, it follows that

$$r^K_{{}^gP}(J(K)) \subseteq J({}^gP) \subseteq {}^g\mathfrak{a} ,$$

proving that $J(K) \subseteq I(K)$. □

Proposition 57.1 has a number of consequences. The first is the following characterization of defect groups in terms of minimal subgroups of the quotient functor $A/I_{H_\mathfrak{m}}$. Define a *minimal subgroup* of a Green functor B to be a minimal subgroup P such that $B(P) \neq 0$.

(57.2) COROLLARY. *Let A be a Green functor for G, let $H_{\mathfrak{m}}$ be a pointed group on A, let $I_{H_{\mathfrak{m}}}$ be its associated functorial ideal, and let P be a subgroup of G. The following conditions are equivalent.*
(a) Some G-conjugate of P is a defect group of $H_{\mathfrak{m}}$.
(b) P is a minimal subgroup of $A/I_{H_{\mathfrak{m}}}$.
In particular all minimal subgroups of $A/I_{H_{\mathfrak{m}}}$ are G-conjugate.

Proof. Let P be a defect group of $H_{\mathfrak{m}}$ and let $\mathfrak{a} = (t_P^H)^{-1}(\mathfrak{m})^\circ$, which is a proper ideal of $A(P)$ by definition of relative projectivity. If K does not contain a G-conjugate of P, then $I_{H_{\mathfrak{m}}}(K) = A(K)$ by Proposition 57.1 and therefore $(A/I_{H_{\mathfrak{m}}})(K) = 0$. If now $K = {}^gP$ for some $g \in G$, then

$$I_{H_{\mathfrak{m}}}({}^gP) \subseteq {}^g\mathfrak{a} \neq A(K),$$

and therefore $(A/I_{H_{\mathfrak{m}}})({}^gP) \neq 0$. This shows that the set of G-conjugates of P is exactly the set of minimal subgroups of $A/I_{H_{\mathfrak{m}}}$. The result follows. □

Corollary 57.2 takes a simpler form when $H = G$, because a G-conjugate of a defect group is again a defect group in that case. Thus P is a defect group of $G_{\mathfrak{m}}$ if and only if P is a minimal subgroup of $A/I_{G_{\mathfrak{m}}}$. For a given pointed group $H_{\mathfrak{m}}$, this situation can always be achieved, for it suffices to replace the G-functor A by the H-functor $\mathrm{Res}_H^G(A)$. This procedure does not change the pointed group and subgroup which we consider, but it has the effect of enlarging the associated functorial ideal $I_{H_{\mathfrak{m}}}$, because it is now only required to be invariant under H-conjugation. This can be seen explicitly from the description of Proposition 57.1, where the intersection is now only running over elements of H.

The second application of Proposition 57.1 is the following.

(57.3) COROLLARY. *Let A be a Green functor for G, let $H_{\mathfrak{m}}$ and $P_{\mathfrak{p}}$ be two pointed groups on A, let $I_{H_{\mathfrak{m}}}$ and $I_{P_{\mathfrak{p}}}$ be their associated functorial ideals, and assume that $P_{\mathfrak{p}}$ is primordial. The following conditions are equivalent.*
(a) $H_{\mathfrak{m}}$ comes from $A/I_{P_{\mathfrak{p}}}$.
(b) $I_{H_{\mathfrak{m}}} \supseteq I_{P_{\mathfrak{p}}}$.
(c) $H_{\mathfrak{m}}$ contains a G-conjugate of $P_{\mathfrak{p}}$.

Proof. It is clear that (a) and (b) are equivalent, because they are both equivalent to the inclusion $I_{P_{\mathfrak{p}}}(H) \subseteq \mathfrak{m}$. By Proposition 57.1 above and by Corollary 55.3, $I_{P_{\mathfrak{p}}}(H) \subseteq \mathfrak{m}$ if and only if there exists $g \in G$ such that ${}^gP \leq H$ and $(r_{{}^gP}^H)^{-1}({}^g\mathfrak{p}) \subseteq \mathfrak{m}$. But this condition means precisely that $H_{\mathfrak{m}} \geq {}^g(P_{\mathfrak{p}})$. □

In our next application of Proposition 57.1, we establish a link between associated functorial ideals and the other relation pr. The proof uses again the key lemma of defect theory (Lemma 56.1).

(57.4) COROLLARY. *Let A be a Green functor for G, let $H_{\mathfrak{m}}$ and $K_{\mathfrak{n}}$ be pointed groups on A, and let $I_{H_{\mathfrak{m}}}$ and $I_{K_{\mathfrak{n}}}$ be their associated functorial ideals. If $H_{\mathfrak{m}}\, pr\, K_{\mathfrak{n}}$, then $K_{\mathfrak{n}}$ comes from $A/I_{H_{\mathfrak{m}}}$, or equivalently, $I_{H_{\mathfrak{m}}} \subseteq I_{K_{\mathfrak{n}}}$.*

Proof. Let P be a defect group of $H_{\mathfrak{m}}$ and let $\mathfrak{a} = (t_P^H)^{-1}(\mathfrak{m})^\circ$. By Lemma 56.6, $\mathfrak{a}$ is a primordial ideal and $(r_P^H)^{-1}(\mathfrak{a}) \subseteq \mathfrak{m}$. Therefore the assumptions of Lemma 56.1 are satisfied and it follows that there exists $h \in H$ such that ${}^hP \leq K$ and $(r_{{}^hP}^K)^{-1}({}^h\mathfrak{a}) \subseteq \mathfrak{n}$. In particular, by the description of $I_{H_{\mathfrak{m}}}(K)$ given in Proposition 57.1, we have $I_{H_{\mathfrak{m}}}(K) \subseteq \mathfrak{n}$, as was to be shown. □

We can now prove that defect pointed groups are characterized in terms of associated functorial ideals.

(57.5) THEOREM. *Let A be a Green functor for G, let $H_{\mathfrak{m}}$ and $P_{\mathfrak{p}}$ be pointed groups on A, let $I_{H_{\mathfrak{m}}}$ and $I_{P_{\mathfrak{p}}}$ be their associated functorial ideals, and assume that $P_{\mathfrak{p}}$ is primordial. The following two conditions are equivalent.*

(a) Some G-conjugate of $P_{\mathfrak{p}}$ is a defect pointed group of $H_{\mathfrak{m}}$.

(b) $I_{H_{\mathfrak{m}}} = I_{P_{\mathfrak{p}}}$.

If in particular $H = G$, then $P_{\mathfrak{p}}$ is a defect pointed group of $G_{\mathfrak{m}}$ if and only if $I_{G_{\mathfrak{m}}} = I_{P_{\mathfrak{p}}}$.

Proof. (a) ⇒ (b). Replacing $P_{\mathfrak{p}}$ by a G-conjugate does not change the associated functorial ideal $I_{P_{\mathfrak{p}}}$ (Exercise 57.1). Thus we can assume that $P_{\mathfrak{p}}$ is a defect of $H_{\mathfrak{m}}$. The relation $H_{\mathfrak{m}} \geq P_{\mathfrak{p}}$ implies $I_{H_{\mathfrak{m}}} \supseteq I_{P_{\mathfrak{p}}}$ by Corollary 57.3, while the relation $H_{\mathfrak{m}}\, pr\, P_{\mathfrak{p}}$ implies $I_{H_{\mathfrak{m}}} \subseteq I_{P_{\mathfrak{p}}}$ by Corollary 57.4.

(b) ⇒ (a). By Proposition 57.1, $I_{P_{\mathfrak{p}}}(K) = A(K)$ if $K < P$, so that P is a minimal subgroup of $A/I_{P_{\mathfrak{p}}}$. Thus (b) implies that P is a minimal subgroup of $A/I_{H_{\mathfrak{m}}}$, so that some G-conjugate of P is a defect group of $H_{\mathfrak{m}}$ (Corollary 57.2). Therefore all defect groups of $H_{\mathfrak{m}}$ are G-conjugate to P (because they are H-conjugate).

Now by Corollary 57.3, the relation $I_{H_{\mathfrak{m}}} \supseteq I_{P_{\mathfrak{p}}}$ implies the existence of $g \in G$ such that $H_{\mathfrak{m}} \geq {}^g(P_{\mathfrak{p}})$. In particular, since ${}^g\mathfrak{p}$ is primordial,

$$\mathrm{Ker}(br_{{}^gP}\, r_{{}^gP}^H) \;=\; (r_{{}^gP}^H)^{-1}(\mathrm{Ker}(br_{{}^gP})) \;\subseteq\; (r_{{}^gP}^H)^{-1}({}^g\mathfrak{p}) \;\subseteq\; \mathfrak{m}\,.$$

By the maximality criterion for defect groups (Theorem 56.5), it follows that ${}^gP$ is contained in a defect group of $H_{\mathfrak{m}}$, hence in a G-conjugate of P by the above argument. Therefore ${}^gP$ is a defect group of $H_{\mathfrak{m}}$, and in particular $H_{\mathfrak{m}}$ is projective relative to ${}^gP$. Now Lemma 56.7 implies that ${}^g(P_{\mathfrak{p}})$ is a defect pointed group of $H_{\mathfrak{m}}$, because ${}^g(P_{\mathfrak{p}})$ is primordial, $H_{\mathfrak{m}} \geq {}^g(P_{\mathfrak{p}})$, and $H_{\mathfrak{m}}$ is projective relative to ${}^gP$. This proves (a).

The special case $H = G$ follows immediately, because a G-conjugate of a defect pointed group is again a defect pointed group. □

As in the case of Corollary 57.2, the above result takes a simpler form when $H = G$. But for an arbitrary pointed group $H_{\mathfrak{m}}$, this situation can be achieved if one replaces the G-functor A by the H-functor $\mathrm{Res}^G_H(A)$ (this has the effect of enlarging the associated functorial ideal $I_{H_{\mathfrak{m}}}$). Theorem 57.5 can also be viewed as a criterion for the existence of defect pointed groups (Exercise 57.3).

The description of $I_{H_{\mathfrak{m}}}$ given in Proposition 57.1 is quite explicit in case $H_{\mathfrak{m}}$ is primordial, but in the general case it depends on the ideal $\mathfrak{a} = (t^H_P)^{-1}(\mathfrak{m})^\circ$, which looks rather mysterious. But if a defect pointed group $P_{\mathfrak{p}}$ exists, the equality $I_{H_{\mathfrak{m}}} = I_{P_{\mathfrak{p}}}$ in Theorem 57.5 allows us to describe $\mathfrak{a}$ explicitly. We also obtain an expression of the ideal $I_{H_{\mathfrak{m}}}(P)$ as an intersection of maximal ideals.

(57.6) COROLLARY. *Let A be a Green functor for G, let $H_{\mathfrak{m}}$ be a pointed group on A, and assume that a defect pointed group $P_{\mathfrak{p}}$ of $H_{\mathfrak{m}}$ exists.*

(a) The ideal $\mathfrak{a} = (t^H_P)^{-1}(\mathfrak{m})^\circ$ (appearing in Proposition 57.1) is equal to

$$\mathfrak{a} = \bigcap_{h \in [N_H(P)/N_H(P_{\mathfrak{p}})]} {}^h\mathfrak{p}\,.$$

(b) The associated functorial ideal $I_{H_{\mathfrak{m}}}$ satisfies

$$I_{H_{\mathfrak{m}}}(P) = \bigcap_{g \in [N_G(P)/N_H(P)]} {}^g\mathfrak{a} = \bigcap_{g \in [N_G(P)/N_H(P_{\mathfrak{p}})]} {}^g\mathfrak{p}\,.$$

Proof. (a) We work with the H-functor $\mathrm{Res}^G_H(A)$. This does not change the ideal $\mathfrak{a}$, but the functorial ideal of $\mathrm{Res}^G_H(A)$ associated with $H_{\mathfrak{m}}$ may be larger (on subgroups of H). We write $I^H_{H_{\mathfrak{m}}}$ for this functorial ideal of $\mathrm{Res}^G_H(A)$, and similarly $I^H_{P_{\mathfrak{p}}}$ for the functorial ideal of $\mathrm{Res}^G_H(A)$ associated with $P_{\mathfrak{p}}$. By Proposition 57.1, we have

$$I^H_{H_{\mathfrak{m}}}(P) = \bigcap_{h \in N_H(P)} {}^h\mathfrak{a} = \mathfrak{a}\,,$$

because the definition of $\mathfrak{a}$ shows that it is H-invariant. Now $I^H_{H_\mathfrak{m}} = I^H_{P_\mathfrak{p}}$ by Theorem 57.5, and the description of $I^H_{P_\mathfrak{p}}$ given in Proposition 57.1 yields

$$I^H_{H_\mathfrak{m}}(P) = I^H_{P_\mathfrak{p}}(P) = \bigcap_{h \in N_H(P)} {}^h\mathfrak{p} = \bigcap_{h \in [N_H(P)/N_H(P_\mathfrak{p})]} {}^h\mathfrak{p} .$$

The result follows.

(b) By Proposition 57.1, we have

$$I_{H_\mathfrak{m}}(P) = \bigcap_{g \in N_G(P)} {}^g\mathfrak{a} = \bigcap_{g \in [N_G(P)/N_H(P)]} {}^g\mathfrak{a} ,$$

because $\mathfrak{a}$ is H-invariant. The second equality in the statement follows from (a). □

We know that a defect group of $H_\mathfrak{m}$ is a minimal subgroup of $A/I_{H_\mathfrak{m}}$ (Corollary 57.2). We can now also characterize a source using the quotient functor $A/I_{H_\mathfrak{m}}$. For simplicity we assume that $H = G$. Otherwise it is always possible to work with the H-functor $\mathrm{Res}^G_H(A)$. Recall that defect pointed groups and hence sources exist under Assumption 56.10 (see Corollary 56.12). However, we do not need this assumption here and in fact we include new conditions for the existence of defect pointed groups.

(57.7) PROPOSITION. *Let A be a Green functor for G, let $G_\mathfrak{m}$ be a pointed group on A, let $I_{G_\mathfrak{m}}$ be its associated functorial ideal, let $B = A/I_{G_\mathfrak{m}}$, and let P be a defect group of $H_\mathfrak{m}$.*

(a) The following conditions are equivalent.

(i) A defect pointed group $P_\mathfrak{p}$ of $G_\mathfrak{m}$ exists.

(ii) The ideal $I_{G_\mathfrak{m}}(P) = (t^G_P)^{-1}(\mathfrak{m})^\circ$ is a finite intersection of maximal ideals.

(iii) $B(P)$ is a finite direct product of simple rings.

(b) Assume that the equivalent conditions of (a) are satisfied, let $\overline{\mathfrak{p}}$ be any maximal ideal of $B(P)$, and let $\mathfrak{p}$ be its inverse image in $A(P)$. Then $\mathfrak{p}$ is a source of $H_\mathfrak{m}$. Moreover every maximal ideal of $B(P)$ is an $N_G(P)$-conjugate of $\overline{\mathfrak{p}}$ and we have

$$B(P) \cong \prod_{g \in [N_G(P)/N_G(P_\mathfrak{p})]} B(P)/{}^g\overline{\mathfrak{p}} .$$

Proof. First note that $I_{G_\mathfrak{m}}(P) = (t^G_P)^{-1}(\mathfrak{m})^\circ$ by Proposition 57.1 (with $H = G$). Thus (ii) makes sense. Assume that a defect pointed group $P_\mathfrak{p}$ of $G_\mathfrak{m}$ exists. By Corollary 57.6, we have

$$I_{G_\mathfrak{m}}(P) = \bigcap_{g \in [N_G(P)/N_G(P_\mathfrak{p})]} {}^g\mathfrak{p} ,$$

and this proves that (i) implies (ii). Moreover, by Lemma 55.4, we obtain

$$B(P) = A(P)/I_{G_{\mathfrak{m}}}(P) \cong \prod_{g\in[N_G(P)/N_G(P_{\mathfrak{p}})]} B(P)/{}^g\overline{\mathfrak{p}}\,,$$

proving (b). Indeed any maximal ideal of $B(P)$ is an $N_G(P)$-conjugate of $\overline{\mathfrak{p}}$, and therefore gives rise to a source of $H_{\mathfrak{m}}$.

It is clear that (ii) and (iii) are equivalent: the proof of (ii) $\Rightarrow$ (iii) follows again from Lemma 55.4, and the converse uses the easy fact that, in a finite direct product of simple rings, there are finitely many maximal ideals and their intersection is zero.

We are left with the proof that (ii) implies (i). By (ii), we can write

$$\mathfrak{a} = (t_P^G)^{-1}(\mathfrak{m})^\circ = \bigcap_{i=1}^n \mathfrak{p}_i\,,$$

where each $\mathfrak{p}_i$ is a maximal ideal of $A(P)$. Consider the inverse image $(r_P^G)^{-1}(\mathfrak{a}) = \bigcap_{i=1}^n (r_P^G)^{-1}(\mathfrak{p}_i)$. By Lemma 56.6, $\mathfrak{a}$ is primordial and $(r_P^G)^{-1}(\mathfrak{a}) \subseteq \mathfrak{m}$. The first assertion implies that every $\mathfrak{p}_i$ is primordial. The second implies that $(r_P^G)^{-1}(\mathfrak{p}_i) \subseteq \mathfrak{m}$ for some i, by Corollary 55.3. This means that $G_{\mathfrak{m}} \geq P_{\mathfrak{p}_i}$. On the other hand the inclusion $(t_P^G)^{-1}(\mathfrak{m})^\circ \subseteq \mathfrak{p}_i$ means that $G_{\mathfrak{m}}\, pr\, P_{\mathfrak{p}_i}$. Therefore $P_{\mathfrak{p}_i}$ is a defect pointed group of $G_{\mathfrak{m}}$, proving (i). □

Proposition 57.7 shows that the whole defect theory of $G_{\mathfrak{m}}$ takes place in the quotient functor $A/I_{G_{\mathfrak{m}}}$. Moreover $I_{G_{\mathfrak{m}}} = I_{P_{\mathfrak{p}}}$ if $P_{\mathfrak{p}}$ is a defect pointed group of $G_{\mathfrak{m}}$ (Theorem 57.5), so that the relevant quotient functors have the form $A/I_{P_{\mathfrak{p}}}$, where $P_{\mathfrak{p}}$ is primordial. When $P_{\mathfrak{p}}$ is maximal primordial, this quotient functor turns out to be simple, as we now show. Here we define a *simple* Green functor to be a Green functor without nonzero proper functorial ideal.

(57.8) PROPOSITION. *Let A be a Green functor for G.*
(a) *Let J be a maximal functorial ideal of A. Then there exists a primordial pointed group $P_{\mathfrak{p}}$ on A such that $J = I_{P_{\mathfrak{p}}}$.*
(b) *Let $P_{\mathfrak{p}}$ be a primordial pointed group on A. The associated functorial ideal $I_{P_{\mathfrak{p}}}$ is maximal if and only if $P_{\mathfrak{p}}$ is maximal primordial.*

Proof. (a) Let P be a minimal subgroup such that $J(P) \neq A(P)$ and let $\mathfrak{p} \in \mathrm{Max}(A(P))$ be such that $J(P) \subseteq \mathfrak{p}$. Since $J(Q) = A(Q)$ if $Q < P$, we have $t_Q^P(A(Q)) \subseteq J(P) \subseteq \mathfrak{p}$. Therefore $P_{\mathfrak{p}}$ is a primordial pointed group. By definition of $I_{P_{\mathfrak{p}}}$, we have $J \subseteq I_{P_{\mathfrak{p}}}$ and so $J = I_{P_{\mathfrak{p}}}$ by maximality of J.

(b) If $I_{P_\mathfrak{p}}$ is maximal and if we have $P_\mathfrak{p} \leq Q_\mathfrak{q}$ with $Q_\mathfrak{q}$ primordial, then $I_{P_\mathfrak{p}} \subseteq I_{Q_\mathfrak{q}}$ by Corollary 57.3, and so $I_{P_\mathfrak{p}} = I_{Q_\mathfrak{q}}$ by maximality. By Corollary 57.3 again, $P_\mathfrak{p}$ and $Q_\mathfrak{q}$ must be G-conjugate, forcing $P_\mathfrak{p} = Q_\mathfrak{q}$. Conversely if $P_\mathfrak{p}$ is maximal primordial, let J be a maximal functorial ideal containing $I_{P_\mathfrak{p}}$. By part (a), $J = I_{Q_\mathfrak{q}}$ for some primordial pointed group $Q_\mathfrak{q}$, and therefore $P_\mathfrak{p} \leq {}^g(Q_\mathfrak{q})$ by Corollary 57.3. It follows that $P_\mathfrak{p} = {}^g(Q_\mathfrak{q})$ by maximality and so, by Exercise 57.1, $I_{P_\mathfrak{p}} = I_{^g(Q_\mathfrak{q})} = I_{Q_\mathfrak{q}}$ is maximal. □

(57.9) COROLLARY. *Let A be a Green functor for G. The simple quotient functors of A are precisely the G-functors $A/I_{P_\mathfrak{p}}$, where $P_\mathfrak{p}$ is a maximal primordial pointed group on A.*

One can deduce from this the following result on the structure of simple Green functors.

(57.10) COROLLARY. *Let A be a simple Green functor, let P be a minimal subgroup of A, and let $\mathfrak{p} \in \mathrm{Max}(A(P))$.*

(a) $P_\mathfrak{p}$ is primordial and the G-conjugacy class of $P_\mathfrak{p}$ is the unique conjugacy class of primordial pointed groups on A. In particular $P_\mathfrak{p}$ is maximal primordial. Moreover $I_{P_\mathfrak{p}} = 0$.

(b) The G-conjugacy class of P is the unique conjugacy class of primordial subgroups for A.

(c) Any pointed group $H_\mathfrak{m}$ on A has a defect pointed group which is some G-conjugate of $P_\mathfrak{p}$.

Proof. This is left to the reader (Exercise 57.4). □

(57.11) REMARK. Much more can be said about simple Green functors. If A is a simple Green functor, then a (maximal) primordial pointed group $P_\mathfrak{p}$ on A defines a simple algebra $A(P)/\mathfrak{p}$, endowed with an $\overline{N}_G(P_\mathfrak{p})$-algebra structure. Since $P_\mathfrak{p}$ is unique up to G-conjugation, so is $A(P)/\mathfrak{p}$. Moreover, by Exercise 58.1, $A(P)/\mathfrak{p}$ is a projective $\overline{N}_G(P_\mathfrak{p})$-algebra (that is, the relative trace map $t_1^{\overline{N}_G(P_\mathfrak{p})}$ is surjective). One can show that the projective $\overline{N}_G(P_\mathfrak{p})$-algebra $A(P)/\mathfrak{p}$ determines uniquely the simple Green functor A. In fact A can be reconstructed from $A(P)/\mathfrak{p}$ by an induction procedure. This provides a classification of simple Green functors in terms of conjugacy classes of triples (H, P, S), where H is a subgroup of G, P is a normal subgroup of H, and S is a projective H/P-algebra which is simple.

Exercises

(57.1) Let A be a Green functor for G, let $H_{\mathfrak{m}}$ be a pointed group on A, let $I_{H_{\mathfrak{m}}}$ be its associated functorial ideal, and let $g \in G$. Prove that $I_{{}^g(H_{\mathfrak{m}})} = I_{H_{\mathfrak{m}}}$.

(57.2) Prove that the family of ideals $I(K)$ defined at the beginning of the proof of Proposition 57.1 is invariant under conjugation and restriction.

(57.3) Let A be a Green functor for G, let $H_{\mathfrak{m}}$ be a pointed group on A, and let $I_{H_{\mathfrak{m}}}$ be its associated functorial ideal. Prove that a defect pointed group of $H_{\mathfrak{m}}$ exists if and only if $I_{H_{\mathfrak{m}}}$ is equal to the functorial ideal associated with some primordial pointed group on A.

(57.4) Prove Corollary 57.10. [Hint: For (a), use Corollary 57.9 and Corollary 57.3. For (c), show that $H_{\mathfrak{m}}$ contains a conjugate ${}^g(P_{\mathfrak{p}})$ of $P_{\mathfrak{p}}$ (Corollary 57.3). Then either use Exercise 56.2 or show that ${}^gP$ is a defect group of $H_{\mathfrak{m}}$ and use Lemma 56.7 to conclude.]

Notes on Section 57

The results of this section are due to Thévenaz [1991]. The classification of simple Green functors mentioned in Remark 57.11 also appears in that paper.

§ 58 THE PUIG AND GREEN CORRESPONDENCES FOR MAXIMAL IDEALS

In this section we show that the Puig correspondence also works for maximal ideals in Green functors and we deduce the Green correspondence.

Let A be a Green functor for G over R, let $P_{\mathfrak{p}}$ be a primordial pointed group on A, let $S = A(P)/\mathfrak{p}$, and let $\pi_{\mathfrak{p}} : A(P) \to S$ be the quotient map. The ring S is simple and has an $\overline{N}_G(P_{\mathfrak{p}})$-algebra structure. For the Puig correspondence, we need the following assumption on S.

(58.1) ASSUMPTION. The simple ring $S = A(P)/\mathfrak{p}$ is a finite dimensional k-algebra for some field k, and the action of $\overline{N}_G(P_{\mathfrak{p}})$ is k-linear.

(58.2) REMARK. One can view this assumption slightly differently by merely requiring that S be finite dimensional over its centre. It is not difficult to show that the centre $Z(S)$ of a simple ring S is a field. Clearly $\overline{N}_G(P_\mathfrak{p})$ acts on $Z(S)$, so that $Z(S)$ is a finite Galois extension of the field $k = Z(S)^{\overline{N}_G(P_\mathfrak{p})}$ (with Galois group $\overline{N}_G(P_\mathfrak{p})/X$ where X is the kernel of the action on $Z(S)$). It follows that, if S is finite dimensional over $Z(S)$, then S is a finite dimensional k-algebra and the action of $\overline{N}_G(P_\mathfrak{p})$ is k-linear.

Given a subgroup H of G, we are going to establish a bijective correspondence between pointed groups on A with defect pointed group $P_\mathfrak{p}$ and projective pointed groups on the $\overline{N}_H(P_\mathfrak{p})$-algebra S (or equivalently on the corresponding $\overline{N}_H(P_\mathfrak{p})$-functor F_S defined in Example 53.2). We shall use the ring homomorphism $\pi_\mathfrak{p}\, r^H_P$, which has an image contained in the $N_H(P_\mathfrak{p})$-fixed elements because H acts trivially on $A(H)$ and $\pi_\mathfrak{p}\, r^H_P$ commutes with the action of $N_H(P_\mathfrak{p})$. Thus we view this map as a ring homomorphism

$$\pi_\mathfrak{p}\, r^H_P : A(H) \longrightarrow S^{\overline{N}_H(P_\mathfrak{p})}.$$

We shall often need to consider elements mapping to zero in every simple quotient $A(P)/{}^h\mathfrak{p}$ such that ${}^h\mathfrak{p} \neq \mathfrak{p}$ (but not necessarily to zero in $A(P)/\mathfrak{p} = S$). For this reason we shall use the ideal

$$\mathfrak{q} = \bigcap_{h\in[N_H(P)-N_H(P_\mathfrak{p})]} {}^h\mathfrak{p}.$$

By construction $\mathfrak{q}$ and $\mathfrak{p}$ are coprime. Note that we have $\mathfrak{q} = A(P)$ if $N_H(P) = N_H(P_\mathfrak{p})$.

We need two preliminary lemmas. The first is a characterization of defect pointed groups.

(58.3) LEMMA. *Let A be a Green functor for G, let $P_\mathfrak{p}$ be a primordial pointed group on A, let $H_\mathfrak{m}$ be a pointed group on A containing $P_\mathfrak{p}$, and let $\mathfrak{q}$ be an ideal of $A(P)$ such that $\mathfrak{q}$ and $\mathfrak{p}$ are coprime. Then $P_\mathfrak{p}$ is a defect of $H_\mathfrak{m}$ if and only if $t^H_P(\mathfrak{q}) \not\subseteq \mathfrak{m}$.*

Proof. If $P_\mathfrak{p}$ is a defect of $H_\mathfrak{m}$, then $H_\mathfrak{m}\, pr\, P_\mathfrak{p}$. Therefore, since $\mathfrak{q} \not\subseteq \mathfrak{p}$, we have $t^H_P(\mathfrak{q}) \not\subseteq \mathfrak{m}$ (Lemma 55.5). Conversely assume that we have $t^H_P(\mathfrak{q}) \not\subseteq \mathfrak{m}$. By Lemma 56.7, we only have to show that $H_\mathfrak{m}$ is projective relative to P. But this is clear since $t^H_P(A(P)) \not\subseteq \mathfrak{m}$. □

The second tool for the Puig correspondence is the following result about finite dimensional algebras over a field.

(58.4) LEMMA. *Let F be a finite dimensional algebra over a field, let T be a subring of F, and let $\mathfrak{a}$ be an ideal of F which is contained in T.*
(a) The inclusion $j : T \to F$ induces a bijection

$$j^* : \{\mathfrak{m} \in \mathrm{Max}(F) \mid \mathfrak{m} \not\supseteq \mathfrak{a}\} \xrightarrow{\sim} \{\mathfrak{n} \in \mathrm{Max}(T) \mid \mathfrak{n} \not\supseteq \mathfrak{a}\},$$

given by $j^*(\mathfrak{m}) = \mathfrak{m} \cap T$.
(b) If $\mathfrak{m} \in \mathrm{Max}(F)$ satisfies $\mathfrak{m} \not\supseteq \mathfrak{a}$, then j induces an isomorphism $T/j^*(\mathfrak{m}) \cong F/\mathfrak{m}$.

Proof. Since F is a finite dimensional algebra over a field, $\mathrm{Max}(F)$ is finite. Let

$$\mathfrak{b} = \bigcap_{\substack{\mathfrak{m} \in \mathrm{Max}(F) \\ \mathfrak{m} \not\supseteq \mathfrak{a}}} \mathfrak{m}.$$

By Corollary 55.3, a maximal ideal $\mathfrak{m} \in \mathrm{Max}(F)$ contains $\mathfrak{b}$ if and only if $\mathfrak{m}$ is one of the maximal ideals appearing in the intersection, and therefore

$$(58.5) \qquad \mathfrak{m} \supseteq \mathfrak{b} \quad \text{if and only if} \quad \mathfrak{m} \not\supseteq \mathfrak{a}.$$

In particular $\mathfrak{a}+\mathfrak{b}$ is not contained in any maximal ideal, so that $\mathfrak{a}+\mathfrak{b} = F$. Therefore $\mathfrak{a} + (\mathfrak{b} \cap T) = T$ because $\mathfrak{a} \subseteq T$.

Let $\mathfrak{n} \in \mathrm{Max}(T)$. If $\mathfrak{n} \supseteq \mathfrak{b} \cap T$, then we have $\mathfrak{n} \not\supseteq \mathfrak{a}$ because $\mathfrak{a} + (\mathfrak{b} \cap T) = T$. Conversely assume that $\mathfrak{n} \not\supseteq \mathfrak{a}$. Since a maximal ideal of F either contains $\mathfrak{a}$ or $\mathfrak{b}$, the intersection $\mathfrak{a} \cap \mathfrak{b}$ is contained in the Jacobson radical of F. Since F is a finite dimensional algebra over a field, $\mathfrak{a} \cap \mathfrak{b}$ is nilpotent (Theorem 1.13). Therefore $\mathfrak{a} \cap \mathfrak{b} \cap T$ is nilpotent and $\mathfrak{n} \supseteq \mathfrak{a} \cap \mathfrak{b} \cap T$ by Lemma 55.1. Since $\mathfrak{n} \not\supseteq \mathfrak{a}$, we have $\mathfrak{n} \supseteq \mathfrak{b} \cap T$ by Corollary 55.3. So we have proved that

$$(58.6) \qquad \mathfrak{n} \supseteq \mathfrak{b} \cap T \quad \text{if and only if} \quad \mathfrak{n} \not\supseteq \mathfrak{a}.$$

Now j induces an isomorphism $\overline{j} : T/(\mathfrak{b} \cap T) \xrightarrow{\sim} F/\mathfrak{b}$. First it is clear that $\overline{j}$ is injective. Moreover since $\mathfrak{a} + \mathfrak{b} = F$, any element of $F/\mathfrak{b}$ can be represented by an element of $\mathfrak{a}$, hence an element of T since $\mathfrak{a} \subseteq T$, and this proves the surjectivity of $\overline{j}$. By 58.5 and 58.6, it is now clear that we have a sequence of bijections

$$\begin{aligned}\{\mathfrak{m} \in \mathrm{Max}(F) \mid \mathfrak{m} \not\supseteq \mathfrak{a}\} &\cong \mathrm{Max}(F/\mathfrak{b}) \cong \mathrm{Max}(T/(\mathfrak{b} \cap T)) \\ &\cong \{\mathfrak{n} \in \mathrm{Max}(T) \mid \mathfrak{n} \not\supseteq \mathfrak{a}\},\end{aligned}$$

the second bijection being induced by the isomorphism $\overline{j}$. Moreover $\overline{j}$ necessarily induces an isomorphism $T/(\mathfrak{m} \cap T) \xrightarrow{\sim} F/\mathfrak{m}$ whenever $\mathfrak{m} \supseteq \mathfrak{b}$. □

Now we can state the Puig correspondence.

(58.7) THEOREM (Puig correspondence). *Let* A *be a Green functor for* G, *let* $P_{\mathfrak{p}}$ *be a primordial pointed group on* A, *let* $S = A(P)/\mathfrak{p}$, *and let* $\pi_{\mathfrak{p}} : A(P) \to S$ *be the quotient map. Assume that* S *satisfies Assumption 58.1. If* H *is a subgroup of* G *containing* P, *the ring homomorphism* $\pi_{\mathfrak{p}}\, r_P^H : A(H) \to S^{\overline{N}_H(P_{\mathfrak{p}})}$ *induces a bijection between the sets*

$$\{\, \mathfrak{m} \in \mathrm{Max}(A(H)) \mid P_{\mathfrak{p}} \textit{ is a defect of } H_{\mathfrak{m}} \,\} \qquad \textit{and}$$
$$\{\, \overline{\mathfrak{m}} \in \mathrm{Max}(S^{\overline{N}_H(P_{\mathfrak{p}})}) \mid \overline{N}_H(P_{\mathfrak{p}})_{\overline{\mathfrak{m}}} \textit{ is projective} \,\}$$

such that $(\pi_{\mathfrak{p}}\, r_P^H)^{-1}(\overline{\mathfrak{m}}) = \mathfrak{m}$ *if* $\overline{\mathfrak{m}}$ *corresponds to* $\mathfrak{m}$. *Moreover the homomorphism* $\pi_{\mathfrak{p}}\, r_P^H$ *induces an isomorphism between the simple quotients* $A(H)/\mathfrak{m} \cong S^{\overline{N}_H(P_{\mathfrak{p}})}/\overline{\mathfrak{m}}$.

Proof. Let T be the image of $\pi_{\mathfrak{p}}\, r_P^H$, a subalgebra of $S^{\overline{N}_H(P_{\mathfrak{p}})}$. Let

$$\mathfrak{q} = \bigcap_{h \in [N_H(P) - N_H(P_{\mathfrak{p}})]} {}^{h}\mathfrak{p}\,.$$

Since $\mathfrak{p}$ and $\mathfrak{q}$ are coprime, $\pi_{\mathfrak{p}}(\mathfrak{q}) = S$. Thus by Proposition 55.10, we have

$$\pi_{\mathfrak{p}}\, r_P^H(t_P^H(\mathfrak{q})) = t_1^{\overline{N}_H(P_{\mathfrak{p}})}(\pi_{\mathfrak{p}}(\mathfrak{q})) = t_1^{\overline{N}_H(P_{\mathfrak{p}})}(S) = S_1^{\overline{N}_H(P_{\mathfrak{p}})}\,,$$

the last equality being just the usual notation. It follows that we have $S_1^{\overline{N}_H(P_{\mathfrak{p}})} \subseteq T \subseteq S^{\overline{N}_H(P_{\mathfrak{p}})}$, and so $S_1^{\overline{N}_H(P_{\mathfrak{p}})}$ is an ideal of $S^{\overline{N}_H(P_{\mathfrak{p}})}$. Clearly $\pi_{\mathfrak{p}}\, r_P^H$ induces a bijection between $\mathrm{Max}(T)$ and the set

$$\{\, \mathfrak{m} \in \mathrm{Max}(A(H)) \mid \mathfrak{m} \supseteq \mathrm{Ker}(\pi_{\mathfrak{p}}\, r_P^H) \,\} = \{\, \mathfrak{m} \in \mathrm{Max}(A(H) \mid H_{\mathfrak{m}} \geq P_{\mathfrak{p}} \,\}$$

(the latter equality coming from the very definition of the containment relation). Let $\widetilde{\mathfrak{m}} \in \mathrm{Max}(T)$ and let $\mathfrak{m} = (\pi_{\mathfrak{p}}\, r_P^H)^{-1}(\widetilde{\mathfrak{m}})$ be the corresponding maximal ideal of $A(H)$. Since $H_{\mathfrak{m}} \geq P_{\mathfrak{p}}$, Lemma 58.3 implies that $P_{\mathfrak{p}}$ is a defect of $H_{\mathfrak{m}}$ if and only if $t_P^H(\mathfrak{q}) \not\subseteq \mathfrak{m}$. But this condition is equivalent to $S_1^{\overline{N}_H(P_{\mathfrak{p}})} \not\subseteq \widetilde{\mathfrak{m}}$, by merely applying $\pi_{\mathfrak{p}}\, r_P^H$. Therefore $\pi_{\mathfrak{p}}\, r_P^H$ induces a bijection between

$$\{\, \widetilde{\mathfrak{m}} \in \mathrm{Max}(T) \mid S_1^{\overline{N}_H(P_{\mathfrak{p}})} \not\subseteq \widetilde{\mathfrak{m}} \,\} \qquad \text{and}$$
$$\{\, \mathfrak{m} \in \mathrm{Max}(A(H)) \mid P_{\mathfrak{p}} \text{ is a defect of } H_{\mathfrak{m}} \,\}.$$

Moreover it is clear that $T/\widetilde{\mathfrak{m}} \cong A(H)/\mathfrak{m}$ if $\mathfrak{m} = (\pi_{\mathfrak{p}}\, r_P^H)^{-1}(\widetilde{\mathfrak{m}})$.

It remains to pass from T to $S^{\overline{N}_H(P_\mathfrak{p})}$. We can apply Lemma 58.4 because, by Assumption 58.1, $S^{\overline{N}_H(P_\mathfrak{p})}$ is a finite dimensional algebra over a field. This lemma asserts that the inclusion $j : T \to S^{\overline{N}_H(P_\mathfrak{p})}$ induces a bijection

$$\{\,\overline{\mathfrak{m}} \in \mathrm{Max}(S^{\overline{N}_H(P_\mathfrak{p})}) \mid S_1^{\overline{N}_H(P_\mathfrak{p})} \not\subseteq \overline{\mathfrak{m}}\,\} \cong \{\,\widetilde{\mathfrak{m}} \in \mathrm{Max}(T) \mid S_1^{\overline{N}_H(P_\mathfrak{p})} \not\subseteq \widetilde{\mathfrak{m}}\,\}$$

given by $\widetilde{\mathfrak{m}} = \overline{\mathfrak{m}} \cap T$. Moreover we have $T/\widetilde{\mathfrak{m}} \cong S^{\overline{N}_H(P_\mathfrak{p})}/\overline{\mathfrak{m}}$. The composition of this bijection with the one induced by $\pi_\mathfrak{p}\, r_P^H$ yields the result. Indeed the condition $S_1^{\overline{N}_H(P_\mathfrak{p})} \not\subseteq \overline{\mathfrak{m}}$ is equivalent to the requirement that $\overline{N}_H(P_\mathfrak{p})_{\overline{\mathfrak{m}}}$ be projective. □

The bijection in Theorem 58.7 is called the *Puig correspondence*. Also, if $P_\mathfrak{p}$ is a defect of $H_\mathfrak{m}$, the image of $\mathfrak{m}$ under the Puig correspondence is called the *Puig correspondent* of $\mathfrak{m}$. In case $P_\mathfrak{p}$ is maximal primordial, the Puig correspondence takes a more precise form and has a simpler proof (Exercise 58.1).

Since S is simple, $\{0\}$ is the unique maximal ideal of S, and $1_{\{0\}}$ is the unique pointed group on S having the trivial subgroup 1 as first component. It follows that a pointed group $\overline{N}_H(P_\mathfrak{p})_{\overline{\mathfrak{m}}}$ on S is projective if and only $\overline{N}_H(P_\mathfrak{p})_{\overline{\mathfrak{m}}}\ pr\ 1_{\{0\}}$. In that case $1_{\{0\}}$ is a defect of $\overline{N}_H(P_\mathfrak{p})_{\overline{\mathfrak{m}}}$, because $1_{\{0\}}$ is clearly primordial and the relation $\overline{N}_H(P_\mathfrak{p})_{\overline{\mathfrak{m}}} \geq 1_{\{0\}}$ always holds (since $(r_1^X)^{-1}(\{0\}) = \{0\} \subseteq \mathfrak{m}$). Therefore $\overline{N}_H(P_\mathfrak{p})_{\overline{\mathfrak{m}}}$ is projective if and only if it has defect $1_{\{0\}}$. Thus the target of the Puig correspondence can also be viewed as the set of pointed groups $\overline{N}_H(P_\mathfrak{p})_{\overline{\mathfrak{m}}}$ with defect pointed group $1_{\{0\}}$.

As in Chapter 3, we now show that the Green correspondence is a consequence of the Puig correspondence. We include in the statement the analogue of the Burry–Carlson–Puig theorem (Theorem 20.4).

(58.8) THEOREM (Green correspondence). *Let A be a Green functor for G, let $P_\mathfrak{p}$ be a primordial pointed group on A, let $S = A(P)/\mathfrak{p}$, and let H be a subgroup of G containing $N_G(P_\mathfrak{p})$. Assume that S satisfies Assumption 58.1.*

(a) If $\mathfrak{m}$ is a maximal ideal of $A(G)$ such that $P_\mathfrak{p}$ is a defect of $G_\mathfrak{m}$, there exists a unique maximal ideal $\mathfrak{n}$ of $A(H)$ such that $G_\mathfrak{m} \geq H_\mathfrak{n} \geq P_\mathfrak{p}$.

(b) The correspondence defined by (a) is a bijection between the sets

$$\{\,\mathfrak{m} \in \mathrm{Max}(A(G)) \mid P_\mathfrak{p} \textit{ is a defect of } G_\mathfrak{m}\,\} \qquad \textit{and}$$
$$\{\,\mathfrak{n} \in \mathrm{Max}(A(H)) \mid P_\mathfrak{p} \textit{ is a defect of } H_\mathfrak{n}\,\}.$$

(c) The bijection of part (b) has the following properties. Let $\mathfrak{n}$ be the image of $\mathfrak{m}$ under this bijection. Then

(i) $\mathfrak{m} = (r^G_H)^{-1}(\mathfrak{n})$,
(ii) *The homomorphism* r^G_H *induces an isomorphism between the simple quotients* $A(G)/\mathfrak{m} \cong A(H)/\mathfrak{n}$,
(iii) $G_\mathfrak{m} \, pr \, H_\mathfrak{n}$.

(d) Let $\mathfrak{m} \in \mathrm{Max}(A(G))$ *and* $\mathfrak{n} \in \mathrm{Max}(A(H))$ *such that* $G_\mathfrak{m} \geq H_\mathfrak{n} \geq P_\mathfrak{p}$. *Then* $P_\mathfrak{p}$ *is a defect of* $G_\mathfrak{m}$ *if and only if* $P_\mathfrak{p}$ *is a defect of* $H_\mathfrak{n}$. *If these conditions are satisfied, then* $\mathfrak{n}$ *is the image of* $\mathfrak{m}$ *under the bijection of part (b).*

Proof. We construct a bijection as in (b) and we shall prove later that it is defined by the property (a). Since $H \geq N_G(P_\mathfrak{p})$ by assumption, we have $N_H(P_\mathfrak{p}) = N_G(P_\mathfrak{p})$ and we set

$$\overline{N} = \overline{N}_H(P_\mathfrak{p}) = \overline{N}_G(P_\mathfrak{p}) .$$

Consider the following sets:

$$X = \{ \mathfrak{m} \in \mathrm{Max}(A(G)) \mid P_\mathfrak{p} \text{ is a defect of } G_\mathfrak{m} \} ,$$
$$Y = \{ \mathfrak{n} \in \mathrm{Max}(A(H)) \mid P_\mathfrak{p} \text{ is a defect of } H_\mathfrak{n} \} ,$$
$$Z = \{ \mathfrak{b} \in \mathrm{Max}(S^{\overline{N}}) \mid \overline{N}_\mathfrak{b} \text{ is projective} \} .$$

Let $\pi_\mathfrak{p} : A(P) \to S$ be the quotient map. By the Puig correspondence (Theorem 58.7), X is in bijection with Z via $(\pi_\mathfrak{p} \, r^G_P)^{-1}$, and similarly Y is in bijection with Z via $(\pi_\mathfrak{p} \, r^H_P)^{-1}$. Thus it is clear that X is in bijection with Y via $(r^G_H)^{-1}$.

We now prove that the bijection we have just constructed has the properties stated in (c). Suppose that $\mathfrak{m} \in X$ corresponds to $\mathfrak{n} \in Y$ under the above bijection, and let $\mathfrak{b} \in Z$ be the Puig correspondent of both $\mathfrak{m}$ and $\mathfrak{n}$. Recall that $(\pi_\mathfrak{p} \, r^G_P)^{-1}(\mathfrak{b}) = \mathfrak{m}$ and $(\pi_\mathfrak{p} \, r^H_P)^{-1}(\mathfrak{b}) = \mathfrak{n}$. Then we have $(r^G_H)^{-1}(\mathfrak{n}) = \mathfrak{m}$ and in particular $G_\mathfrak{m} \geq H_\mathfrak{n}$. Moreover r^G_H induces an injective map $r^G_H : A(G)/\mathfrak{m} \to A(H)/\mathfrak{n}$. By Theorem 58.7, $\pi_\mathfrak{p} \, r^G_P$ and $\pi_\mathfrak{p} \, r^H_P$ induce isomorphisms $A(G)/\mathfrak{m} \cong S^{\overline{N}}/\mathfrak{b}$ and $A(H)/\mathfrak{n} \cong S^{\overline{N}}/\mathfrak{b}$ respectively. This forces the map $r^G_H : A(G)/\mathfrak{m} \to A(H)/\mathfrak{n}$ to be an isomorphism. In order to prove that $G_\mathfrak{m} \, pr \, H_\mathfrak{n}$, we let $\mathfrak{a} = (t^G_H)^{-1}(\mathfrak{m})^\circ$ and we have to show that $\mathfrak{a} \subseteq \mathfrak{n}$. Let $\mathfrak{q} = \bigcap_{h \in N_G(P) - N_G(P_\mathfrak{p})} {}^h\mathfrak{p}$. Since $H_\mathfrak{n} \, pr \, P_\mathfrak{p}$ and since $\mathfrak{q}$ and $\mathfrak{p}$ are coprime, we have $t^H_P(\mathfrak{q}) \not\subseteq \mathfrak{n}$. Therefore by Corollary 55.3, it suffices to show that $\mathfrak{n}$ contains the ideal $\mathfrak{a}' = \mathfrak{a} \cap t^H_P(\mathfrak{q})$. If $a \in \mathfrak{a}'$, then by Exercise 55.6

$$\pi_\mathfrak{p} \, r^G_P \, t^G_H(a) = t^{\overline{N}_G(P_\mathfrak{p})}_{\overline{N}_H(P_\mathfrak{p})} \, \pi_\mathfrak{p} \, r^H_P(a) = \pi_\mathfrak{p} \, r^H_P(a) .$$

Moreover since $a \in \mathfrak{a}$, we have $t_H^G(a) \in \mathfrak{m}$ and therefore

$$\pi_{\mathfrak{p}}\, r_P^H(a) \;=\; \pi_{\mathfrak{p}}\, r_P^G(t_H^G(a)) \;\in\; \pi_{\mathfrak{p}}\, r_P^G(\mathfrak{m}) \;\subseteq\; \mathfrak{b}\,.$$

This implies that $a \in \mathfrak{n}$ as required, because $\mathfrak{n} = (\pi_{\mathfrak{p}}\, r_P^H)^{-1}(\mathfrak{b})$.

We now prove (d). Consider again the ideal $\mathfrak{q} = \bigcap_{h\in N_G(P)-N_G(P_{\mathfrak{p}})} {}^h\mathfrak{p}$. By Proposition 55.10, we have

$$(\pi_{\mathfrak{p}}\, r_P^H)(r_H^G\, t_P^G(\mathfrak{q})) = S_1^{\overline{N}} \qquad \text{and} \qquad (\pi_{\mathfrak{p}}\, r_P^H)(t_P^H(\mathfrak{q})) = S_1^{\overline{N}}\,.$$

Therefore $r_H^G\, t_P^G(\mathfrak{q}) \subseteq t_P^H(\mathfrak{q}) + \mathrm{Ker}(\pi_{\mathfrak{p}}\, r_P^H)$. Note also that $\mathrm{Ker}(\pi_{\mathfrak{p}}\, r_P^H) \subseteq \mathfrak{n}$ because $H_{\mathfrak{n}} \geq P_{\mathfrak{p}}$. If $P_{\mathfrak{p}}$ is not a defect of $H_{\mathfrak{n}}$, then $t_P^H(\mathfrak{q}) \subseteq \mathfrak{n}$ by Lemma 58.3, and therefore $r_H^G\, t_P^G(\mathfrak{q}) \subseteq \mathfrak{n}$. It follows that we have inclusions $t_P^G(\mathfrak{q}) \subseteq (r_H^G)^{-1}(\mathfrak{n}) \subseteq \mathfrak{m}$ (using the relation $G_{\mathfrak{m}} \geq H_{\mathfrak{n}}$), and by Lemma 58.3 again, $P_{\mathfrak{p}}$ is not a defect of $G_{\mathfrak{m}}$.

Conversely assume that $P_{\mathfrak{p}}$ is a defect of $H_{\mathfrak{n}}$. If $\mathfrak{b} \in \mathrm{Max}(S^{\overline{N}})$ is the Puig correspondent of $\mathfrak{n}$, we have $\mathfrak{n} = (\pi_{\mathfrak{p}} r_P^H)^{-1}(\mathfrak{b})$. With respect to the Puig correspondence for G, the ideal $\mathfrak{b}$ is the Puig correspondent of $\mathfrak{m}' = (\pi_{\mathfrak{p}}\, r_P^G)^{-1}(\mathfrak{b}) \in \mathrm{Max}(A(G))$ and $P_{\mathfrak{p}}$ is a defect of $G_{\mathfrak{m}'}$. Then

$$\mathfrak{m}' \;=\; (r_H^G)^{-1}(\pi_{\mathfrak{p}}\, r_P^H)^{-1}(\mathfrak{b}) \;=\; (r_H^G)^{-1}(\mathfrak{n}) \;\subseteq\; \mathfrak{m}\,,$$

using the assumption $G_{\mathfrak{m}} \geq H_{\mathfrak{n}}$. By maximality of $\mathfrak{m}'$, it follows that $\mathfrak{m} = \mathfrak{m}'$. In particular $P_{\mathfrak{p}}$ is a defect of $G_{\mathfrak{m}}$. It is clear that $H_{\mathfrak{n}}$ is the image of $G_{\mathfrak{m}}$ under the bijection constructed at the beginning of the proof. This completes the proof of (d).

We are left with the proof of (a). Suppose that $G_{\mathfrak{m}}$ has defect $P_{\mathfrak{p}}$ and let $G_{\mathfrak{m}} \geq H_{\mathfrak{n}} \geq P_{\mathfrak{p}}$. By (d), $P_{\mathfrak{p}}$ is a defect of $H_{\mathfrak{n}}$ and $H_{\mathfrak{n}}$ is necessarily the image of $G_{\mathfrak{m}}$ under the bijection defined above. This proves the uniqueness of $H_{\mathfrak{n}}$ and shows also that the map defined by (a) coincides with the bijection defined above. □

Exercises

(58.1) Let A be a Green functor for G, let $P_{\mathfrak{p}}$ be a primordial pointed group on A, let $S = A(P)/\mathfrak{p}$, let $\pi_{\mathfrak{p}} : A(P) \to S$ be the quotient map, and let H be a subgroup of G containing P. Assume that $P_{\mathfrak{p}}$ is maximal primordial.

(a) Prove that $\pi_{\mathfrak{p}}\, r^H_P : A(H) \to S^{\overline{N}_H(P_{\mathfrak{p}})}$ is surjective and that we have $S_1^{\overline{N}_H(P_{\mathfrak{p}})} = S^{\overline{N}_H(P_{\mathfrak{p}})}$. [Hint: By Exercise 56.2, $P_{\mathfrak{p}}$ is a defect of any pointed group $H_{\mathfrak{m}}$ containing $P_{\mathfrak{p}}$. If $\mathfrak{q} = \bigcap_{h \in N_H(P) - N_H(P_{\mathfrak{p}})} {}^h\mathfrak{p}$, deduce that $\mathrm{Ker}(\pi_{\mathfrak{p}}\, r^H_P)$ and $t^H_P(\mathfrak{q})$ are coprime. Use Proposition 55.10 to show that the image of $\pi_{\mathfrak{p}}\, r^H_P$ is equal to $S_1^{\overline{N}_H(P_{\mathfrak{p}})}$. Conclude with the observation that this image contains 1_S.]

(b) Prove that every pointed group on the $\overline{N}_G(P_{\mathfrak{p}})$-algebra S is projective.

(c) Prove that the ring homomorphism $\pi_{\mathfrak{p}}\, r^H_P$ induces a bijection between the sets $\{\, \mathfrak{m} \in \mathrm{Max}(A(H)) \mid H_{\mathfrak{m}} \geq P_{\mathfrak{p}} \,\}$ and $\mathrm{Max}(S^{\overline{N}_H(P_{\mathfrak{p}})})$. [Note that this is a stronger form of the Puig correspondence and that Assumption 58.1 is not needed here.]

(58.2) For maximal ideals in Green functors, state and prove a result analogous to Corollary 20.6.

(58.3) Let A be a Green functor for G, let $P_{\mathfrak{p}}$ be a primordial pointed group on A satisfying Assumption 58.1, let $H_{\mathfrak{m}}$ and $K_{\mathfrak{n}}$ be two pointed groups on A with defect $P_{\mathfrak{p}}$, and let respectively $\overline{N}_H(P_{\mathfrak{p}})_{\overline{\mathfrak{m}}}$ and $\overline{N}_K(P_{\mathfrak{p}})_{\overline{\mathfrak{n}}}$ be their Puig correspondents (with respect to $P_{\mathfrak{p}}$). Prove that $H_{\mathfrak{m}} \geq K_{\mathfrak{n}}$ if and only if $\overline{N}_H(P_{\mathfrak{p}})_{\overline{\mathfrak{m}}} \geq \overline{N}_K(P_{\mathfrak{p}})_{\overline{\mathfrak{n}}}$. [Hint: Let $S = A(P)/\mathfrak{p}$, let T_H and T_K be the images of $\pi_{\mathfrak{p}}\, r^H_P$ and $\pi_{\mathfrak{p}}\, r^K_P$ respectively, let $\widetilde{\mathfrak{m}} = \overline{\mathfrak{m}} \cap T_H$ and $\widetilde{\mathfrak{n}} = \overline{\mathfrak{n}} \cap T_K$ (as in the proof of Theorem 58.7), and consider the following diagram.

$$\begin{array}{ccccc} A(H) & \xrightarrow{\pi_{\mathfrak{p}}\, r^H_P} & T_H & \longrightarrow & S^{\overline{N}_H(P_{\mathfrak{p}})} \\ \big\downarrow r^H_K & & \big\downarrow r^{\overline{N}_H(P_{\mathfrak{p}})}_{\overline{N}_K(P_{\mathfrak{p}})} & & \big\downarrow r^{\overline{N}_H(P_{\mathfrak{p}})}_{\overline{N}_K(P_{\mathfrak{p}})} \\ A(K) & \xrightarrow{\pi_{\mathfrak{p}}\, r^K_P} & T_K & \longrightarrow & S^{\overline{N}_K(P_{\mathfrak{p}})} \end{array}$$

The proof that $\overline{N}_H(P_{\mathfrak{p}})_{\overline{\mathfrak{m}}} \geq \overline{N}_K(P_{\mathfrak{p}})_{\overline{\mathfrak{n}}}$ implies $H_{\mathfrak{m}} \geq K_{\mathfrak{n}}$ is easy. If now $H_{\mathfrak{m}} \geq K_{\mathfrak{n}}$, prove first that $(r^{\overline{N}_H(P_{\mathfrak{p}})}_{\overline{N}_K(P_{\mathfrak{p}})})^{-1}(\widetilde{\mathfrak{n}}) \subseteq \widetilde{\mathfrak{m}}$. To prove that $(r^{\overline{N}_H(P_{\mathfrak{p}})}_{\overline{N}_K(P_{\mathfrak{p}})})^{-1}(\overline{\mathfrak{n}}) \subseteq \overline{\mathfrak{m}}$, it suffices by Corollary 55.3 to show that

$$(r^{\overline{N}_H(P_{\mathfrak{p}})}_{\overline{N}_K(P_{\mathfrak{p}})})^{-1}(\overline{\mathfrak{n}}) \cap S_1^{\overline{N}_H(P_{\mathfrak{p}})} \subseteq \overline{\mathfrak{m}} .$$

But this takes place in T_H and follows from the previous inclusion.]

Notes on Section 58

The extension of the Puig and Green correspondences to the case of maximal ideals in Green functors is due to Thévenaz [1991].

Bibliography

We only list references of books and papers cited in this text, or of papers focussing on G-algebras. For other references in modular representation theory, the interested reader can consult the books by Benson [1991], Curtis and Reiner [1981, 1987], Feit [1982], and Landrock [1983].

Alperin, J.L.

[1967] Sylow intersections and fusion, *J. Algebra* **6**, 222–241.

[1986] *Local representation theory*, Cambridge University Press.

Alperin, J.L., Broué, M.

[1979] Local methods in block theory, *Ann. of Math.* **110**, 143–157.

Aschbacher, M.

[1993] Simple connectivity of p-group complexes, Israel J. Math. **82**, 1–43.

Atiyah, M.

[1961] Characters and cohomology of finite groups, *Publ. Math. Inst. Hautes Etudes Sci.* **9**, 23–64.

Auslander, M.

[1977] Existence theorems for almost split sequences, in: Ring Theory II (Proceedings of the 2nd Oklahoma Ring Theory Conference), p. 1–44, M. Dekker, New York – Basel.

Auslander, M., Reiten, I.

[1975] Representation theory of Artin algebras III, *Comm. Algebra* **3**, 239–294.

Barker, L.

[1994a] Modules with simple multiplicity modules, *J. Algebra*, to appear.

[1994b] G-algebras, Clifford theory, and the Green correspondence, *J. Algebra*, to appear.

[1994c] Induction, restriction and G-algebras, *Comm. Algebra* **22**, 6349–6383.

Bass, H., Tate, J.

[1973] The Milnor ring of a global field, in: *Algebraic K-theory II*, Lecture Notes in Math. 342, Springer-Verlag, New York – Heidelberg – Berlin, p. 349–428.

Benson, D.

[1991] *Representations and cohomology*, Vol. I and II, Cambridge University Press.

Benson, D., Parker, R.

[1984] The Green ring of a finite group, *J. Algebra* **87**, 290–331.

Brauer, R.
[1956] Zur Darstellungstheorie der Gruppen endlicher Ordnung, *Math. Z.* **63**, 406–444.
[1959] Zur Darstellungstheorie der Gruppen endlicher Ordnung II, *Math. Z.* **72**, 25–46.
[1964] Some applications of the theory of blocks of characters of finite groups I, *J. Algebra* **1**, 152–167.
[1974] On the structure of blocks of characters of finite groups, in "Proc. Second Intern. Conf. on Theory of Groups", Lecture Notes in Math. 372, Springer-Verlag, New York – Heidelberg – Berlin, p. 103–130.

Brauer, R., Nesbitt, C.J.
[1941] On the modular characters of groups, *Ann. of Math.* **42**, 556–590.

Broué, M.
[1985] On Scott modules and p-permutation modules: an approach through the Brauer morphism, *Proc. Amer. Math. Soc.* **93**, 401–408.
[1986] Les ℓ-blocs des groupes $GL(n,q)$ et $U(n,q^2)$ et leurs structures locales, *Astérisque* **133–134**, 159–188.

Broué, M., Olsson, J.B.
[1986] Subpairs multiplicities in finite groups, *J. Reine Angew. Math. (Crelle)* **371**, 125–143.

Broué, M., Puig, L.
[1980a] Characters and local structure in G-algebras, *J. Algebra* **63**, 306–317.
[1980b] A Frobenius theorem for blocks, *Invent. Math.* **56**, 117–128.

Broué, M., Robinson, G.R.
[1986] Bilinear forms on G-algebras, *J. Algebra* **104**, 377–396.

Brown, K.S.
[1982] *Cohomology of groups*, Graduate Texts in Math. 87, Springer-Verlag, New York – Heidelberg – Berlin.

Burry, D., Carlson, J.F.
[1982] Restrictions of modules to local subgroups, *Proc. Amer. Math. Soc.* **84**, 181–184.

Cabanes, M.
[1987] Extensions of p-groups and construction of characters, *Comm. Algebra* **15**, 1297–1311.
[1988a] A note on extensions of p-blocks by p-groups and their characters, *J. Algebra* **115**, 445–449.
[1988b] Local structure of the p-blocks of $\widetilde{S}_n$, *Math. Z.* **198**, 519–543.

Cabanes, M., Enguehard, M.

[1992] On blocks and unipotent characters of reductive groups over a finite field II, *Rapport de recherche du LMENS* **92–13**.

[1993] On general blocks of finite reductive groups: ordinary characters and defect groups, *Rapport de recherche du LMENS* **93–13**.

Cabanes, M., Picaronny, C.

[1992] Types of blocks with dihedral or quaternion defect groups, *J. Fac. Sci. Univ. Tokyo* **39**, 141–161.

Carlson, J.F.

[1985] The cohomology ring of a module, *J. Pure Appl. Algebra* **36**, 105–121.

Clifford, A.H.

[1937] Representations induced in an invariant subgroup, *Ann. of Math.* **38**, 533–550.

Conlon, S.B.

[1968] Decompositions induced from the Burnside algebra, *J. Algebra* **10**, 102–122.

Curtis, C.W., Reiner, I.

[1962] *Representation theory of finite groups and associative algebras*, John Wiley & Sons, New York – London – Sydney.

[1981] *Methods of representation theory*, Vol. I, John Wiley & Sons, New York – London – Sydney.

[1987] *Methods of representation theory*, Vol. II, John Wiley & Sons, New York – London – Sydney.

Dade, E.C.

[1966] Blocks with cyclic defect groups, *Ann. of Math.* (2) **84**, 20–48.

[1973] Block extensions, *Illinois J. Math.* **17**, 198–272.

[1978a] Endo-permutation modules over p-groups, I, *Ann. of Math.* **107**, 459–494.

[1978b] Endo-permutation modules over p-groups, II, *Ann. of Math.* **108**, 317–346.

[1982] The Green correspondents of simple group modules, *J. Algebra* **78**, 357–371.

tom Dieck, T.

[1979] *Transformation groups and representation theory*, Lecture Notes in Math. 766, Springer-Verlag, New York – Heidelberg – Berlin.

[1987] *Transformation groups*, Studies in Math. 8, Walter de Gruyter, Berlin – New York.

Dress, A.W.M.

[1973] Contributions to the theory of induced representations, in: *Algebraic K-theory II*, Lecture Notes in Math. 342, Springer-Verlag, New York – Heidelberg – Berlin, p. 183–240.

[1975] Induction and structure theorems for orthogonal representations of finite groups, *Ann. of Math.* **102**, 291–325.

Erdmann, K.

[1990] Blocks of tame representation type and related algebras, Lecture Notes in Math. 1428, Springer-Verlag, New York – Heidelberg – Berlin.

Fan, Y.

[1994] The source algebras of nilpotent blocks over arbitrary groundfields, *J. Algebra* **165**, 606–632.

Feit, W.

[1980] Some consequences of the classification of finite simple groups, *Proc. Symp. Pure Math.* **37**, 175–181.

[1982] *The representation theory of finite groups*, North-Holland, Amsterdam – New York – Oxford.

Fong, P., Srinivasan, B.

[1989] The blocks of finite classical groups, *J. Reine Angew. Math. (Crelle)* **396**, 122–191.

Garotta, O.

[1994] Suites presque scindées d'algèbres intérieures, *Publ. Math. Univ. Paris VII* **34**, 137–237.

Gaschütz, W.

[1952] Über den Fundamentalsatz von Maschke zur Darstellungstheorie der endlichen Gruppen, *Math. Z.* **56**, 376–387.

Goldschmidt, D.M.

[1970] A conjugation family for finite groups, *J. Algebra* **16**, 138–142.

Gorenstein, D., Lyons, R.

[1983] The local structure of finite groups of characteristic 2 type, *Memoirs Amer. Math. Soc.* **276**.

Green, J.A.

[1959] On the indecomposable representations of a finite group, *Math. Z.* **70**, 430–445.

[1962] Blocks of modular representations, *Math. Z.* **79**, 100–115.

[1964] A transfer theorem for modular representations, *J. Algebra* **1**, 73–84.

[1968] Some remarks on defect groups, *Math. Z.* **107**, 133–150.

[1971] Axiomatic representation theory for finite groups, *J. Pure Appl. Algebra* **1**, 41–77.

[1985] Functors on categories of finite groups representations, *J. Pure Appl. Algebra* **37**, 265–298.

Hardy, G.H., Littlewood, J.E., Pólya, G.

[1952] *Inequalities*, Cambridge University Press, second edition.

Higman, D.G.

[1954] Indecomposable representations at characteristic p, *Duke Math. J.* **21**, 377–381.

Huppert, B.

[1967] *Endliche Gruppen I*, Springer-Verlag, New York – Heidelberg – Berlin.

Ikeda, T.

[1987] A characterization of blocks with vertices, *J. Algebra* **105**, 344–350.

[1990] On defect groups of interior G-algebras and vertices of modules, *Hokkaido Math. J.* **19**, 447–460.

Kato, K.

[1980] A generalization of local class field theory using K-groups, *J. Fac. Sci. Univ. Tokyo* **27**, 603–683.

Knörr, R.

[1979] On the vertices of irreducible modules, *Ann. of Math.* **110**, 487–499.

[1985] Auslander–Reiten sequences and a certain ideal in $\text{mod}-FG$, manuscript.

[1987] Projective homomorphisms of RG-lattices, manuscript.

Külshammer, B.

[1984] Bemerkungen über die Gruppenalgebra als symmetrische Algebra III, *J. Algebra* **88**, 279–291.

[1985] Crossed products and blocks with normal defect group, *Comm. Algebra* **13**, 147–168.

[1990] Blocks and source algebras: an invitation, *Bayreuth. Math. Schr.* **33**, 109–135.

[1991a] *Lectures on block theory*, London Mathematical Society Lecture Notes Series 161, Cambridge University Press.

[1991b] The principal block idempotent, *Arch. Math.* **56**, 313–319.

[1994] Central idempotents in p-adic group rings, *J. Austr. Math. Soc.* **56**, 278–289.

Külshammer, B., Puig, L.
[1990] Extensions of nilpotent blocks, *Invent. Math.* **102**, 17–71.

Landrock, P.
[1983] *Finite group algebras and their modules*, London Mathematical Society Lecture Notes Series 84, Cambridge University Press.

Linckelmann, M.
[1989] Modules in the sources of Green's exact sequences for cyclic blocks, *Invent. Math.* **97**, 129–140.
[1991] Derived equivalence for cyclic blocks over a p-adic ring, *Math. Z.* **207**, 293–304.
[1993] The isomorphism problem for cyclic blocks, preprint.
[1994] The source algebras of blocks with a Klein four defect group, *J. Algebra* **167**, 821–854.

Linckelmann, M., Puig, L.
[1987] Structure des p'-extensions des blocs nilpotents, *C.R. Acad. Sci. Paris* **304**, 181–184.

Mac Lane, S.
[1971] *Categories for the Working Mathematician*, Graduate Texts in Math. 5, Springer-Verlag, New York – Heidelberg – Berlin.

Okuyama, T., Uno, K.
[1990] On vertices of Auslander–Reiten sequences, *Bull. London Math. Soc.* **22**, 153–158.

Oliver, R.
[1988] *Whitehead groups of finite groups*, London Mathematical Society Lecture Notes Series 132, Cambridge University Press.

Picaronny, C.
[1987] Un théorème de Dade, *Publ. Math. Univ. Paris VII* **25**, 159–169.

Picaronny, C., Puig, L.
[1987] Quelques remarques sur un thème de Knörr, *J. Algebra* **109**, 69–73.

Puig, L.
[1976] Structure locale dans les groupes finis, *Bull. Soc. Math. France*, Mémoire **47**.
[1979] Sur un théorème de Green, *Math. Z.* **166**, 117–129.
[1980] Local block theory in p-solvable groups, *Proc. Symp. Pure Math.* **37**, 385–388.
[1981] Pointed groups and construction of characters, *Math. Z.* **176**, 209–216.
[1982] Une conjecture de finitude sur les blocs, unpublished manuscript.

[1984] *Introduction à la théorie des représentations modulaires des groupes finis*, cours de troisième cycle, Paris, handwritten lecture notes.

[1986] Local fusions in block source algebras, *J. Algebra* **104**, 358–369.

[1987a] The Nakayama conjectures and the Brauer pairs, *Publ. Math. Univ. Paris VII* **25**, 171–189.

[1987b] Local extensions in endo-permutation modules split: a proof of Dade's theorem, *Publ. Math. Univ. Paris VII* **25**, 199–205.

[1988a] Pointed groups and construction of modules, *J. Algebra* **116**, 7–129.

[1988b] Nilpotent blocks and their source algebras, *Invent. Math.* **93**, 77–116.

[1988c] Vortex et sources des foncteurs simples, *C.R. Acad. Sci. Paris* **306**, 223–226.

[1988d] Notes sur les algèbres de Dade, unpublished manuscript.

[1990a] Affirmative answer to a question of Feit, *J. Algebra* **131**, 513–526.

[1990b] Algèbres de source de certains blocs des groupes de Chevalley, *Astérisque* **181-182**, 221–236.

[1991] Une correspondance de modules pour les blocs à groupes de défaut abéliens, *Geom. Dedicata* **37**, 9–43.

[1994a] On Thévenaz' parametrization of interior G-algebras, *Math. Z.* **215**, 321–335.

[1994b] On Joanna Scopes' criterion of equivalence for blocks of symmetric groups, *Algebra Colloq.* **1**, 25–55.

Puig, L., Watanabe, A.

[1994] On blocks with one simple module in any Brauer correspondent, *J. Algebra* **163**, 135–138.

Quillen, D.

[1973] Higher algebraic K-theory, in: *Algebraic K-theory I*, Lecture Notes in Math. 341, Springer-Verlag, New York – Heidelberg – Berlin, p. 85–147.

Reiner, I.

[1975] *Maximal orders*, Academic Press, London – New York – San Francisco.

Ribenboim, P.

[1972] *Algebraic numbers*, John Wiley & Sons, New York – London – Sydney.

Robinson, G.R.

[1983] The number of blocks with a given defect group, *J. Algebra* **84**, 493–502.

Roggenkamp, K.W.
[1977] The construction of almost split sequences for integral group rings and orders, *Comm. Algebra* **5**, 1363–1373.

Roggenkamp, K.W., Schmidt, J.W.
[1976] Almost split sequences for integral group rings and orders, *Comm. Algebra* **4**, 893–917.

Scott, L.
[1973] Modular permutation representations, *Trans. Amer. Math. Soc.* **175**, 101–121.

Serre, J.P.
[1962] *Corps locaux*, Hermann, Paris.
(English translation: *Local fields*, Graduate Texts in Math. 67, Springer-Verlag, New York – Heidelberg – Berlin, 1979.)
[1971] *Représentations linéaires de groupes finis*, deuxième édition, Hermann, Paris.
(English translation: *Linear representations of finite groups*, Graduate Texts in Math. 42, Springer-Verlag, New York – Heidelberg – Berlin, 1977.)

Sibley, D.A.
[1990] Vertices, blocks, and virtual characters, *J. Algebra* **132**, 501–507.

Thévenaz, J.
[1983a] Extensions of group representations from a normal subgroup, *Comm. Algebra* **11**, 391–425.
[1983b] Lifting idempotents and Clifford theory, *Comment. Math. Helv.* **58**, 86–95.
[1988a] Duality in G-algebras, *Math. Z.* **200**, 47–85.
[1988b] G-algebras, Jacobson radical and almost split sequences, *Invent. Math.* **93**, 131–159.
[1988c] Some remarks on G-functors and the Brauer morphism, *J. Reine Angew. Math. (Crelle)* **384**, 24–56.
[1990] A visit to the kingdom of the Mackey functors, *Bayreuth. Math. Schr.* **33**, 215–241.
[1991] Defect theory for maximal ideals and simple functors, *J. Algebra* **140**, 426–483.
[1993] The parametrization of interior algebras, *Math. Z.* **212**, 411–454.

Uno, K.
[1988] Relative projectivity and extendibility of Auslander–Reiten sequences, *Osaka J. Math.* **25**, 499–518.

Watanabe, A.
[1994] On nilpotent blocks of finite groups, *J. Algebra* **163**, 128–134.

Webb, P.J.
[1982] The Auslander–Reiten quiver of a finite group, *Math. Z.* **179**, 97–121.

Notation Index

$\leq$, $\geq$	order relation between subgroups, order relation between pointed groups
A^*	group of invertible elements of the ring A
A^H	algebra of H-fixed elements in the G-algebra A
$\overline{A}(P)$	Brauer quotient of A^P
A_K^H	image of the relative trace map $t_K^H : A^K \to A^H$
A_α	localization of A with respect to the point α
A_γ	localization of A with respect to the point γ, source algebra
$\mathcal{B}_G(b)$	Brauer category of the block b
br_P^A , br_P	Brauer homomorphism
$\mathrm{Conj}(g)$	conjugation by g
$\mathcal{D}_H^G$	canonical embedding $A \to \mathrm{Res}_H^G \mathrm{Ind}_H^G(A)$ (for an interior H-algebra A)
$\mathcal{D}_\mathcal{O}(P)$	Dade group of P
$E_G(P_\gamma)$	quotient group $N_G(P_\gamma)/PC_G(P)$
F_A	Green functor associated with the G-algebra A
F_M	Mackey functor associated with the G-module M
$\mathcal{F}$	exomorphism containing a homomorphism f
$\mathcal{F}_\alpha$	embedding associated with the pointed group H_α
$\mathcal{F}_\beta^\alpha$	embedding corresponding to the relation $H_\alpha \geq K_\beta$
$\mathcal{F}(G)$	Frobenius category of G
G_α , H_β	pointed groups on a G-algebra
$G_\mathfrak{m}$, $H_\mathfrak{n}$	pointed groups on a Green functor
$[H/K]$	set of representatives of cosets hK where $h \in H$
$[L\backslash H/K]$	set of representatives of double cosets LhK where $h \in H$
$\overline{\mathrm{Hom}}_{\mathcal{O}H}(M,N)$	stable quotient of $\mathrm{Hom}_{\mathcal{O}H}(M,N)$
$I_{H_\mathfrak{m}}$	functorial ideal associated with the pointed group $H_\mathfrak{m}$ on a Green functor
$\mathrm{Ind}_H^G(A)$	induction of the interior H-algebra A
$\mathrm{Ind}_H^G(\mathcal{F})$	induction of the exomorphism $\mathcal{F}$
$\mathrm{Inj}(A)$	set of all isomorphism classes of indecomposable injective A-lattices
$\mathrm{Inn}(a)$	inner automorphism defined by a
$\mathrm{Irr}(A)$	set of all isomorphism classes of simple (or irreducible) A-modules
$J(A)$	Jacobson radical of A
k	algebraically closed field of characteristic p, residue field of $\mathcal{O}$
$k_\sharp \widehat{\overline{N}}_G(P_\gamma)$	twisted group algebra of the group $\overline{N}_G(P_\gamma)$

$L_M(H)$	socle of $\overline{\mathrm{Hom}}_{\mathcal{O}H}(M,TM)$, orthogonal of $J(\overline{\mathrm{End}}_{\mathcal{O}H}(M))$ with respect to the Auslander–Reiten duality
$L_M(H_\beta)$	orthogonal of the maximal ideal $\mathfrak{m}_\beta$ of $\overline{\mathrm{End}}_{\mathcal{O}H}(M)$ with respect to the Auslander–Reiten duality
$\mathcal{L}_G(A)$	Puig category of A
$\mathcal{L}_G(b)$	Puig category of the block b
$\mathcal{LP}(A^P)$	set of all local points of A^P
$\mathrm{Max}(A)$	set of all maximal ideals of the algebra A
$\mathfrak{m}_\alpha$	maximal ideal corresponding to the point α
$M_n(A)$	algebra of $(n \times n)$-matrices with coefficients in A
$\overline{N}_G(H)$	quotient group $N_G(H)/H$
$N_G(P_\gamma)$	normalizer of the pointed group P_γ
$\overline{N}_G(P_\gamma)$	quotient group $N_G(P_\gamma)/P$
$\widehat{N}_G(P_\gamma)$	central extension of the group $N_G(P_\gamma)$ by the central subgroup k^*
$\widehat{\overline{N}}_G(P_\gamma)$	central extension of the group $\overline{N}_G(P_\gamma)$ by the central subgroup k^*
$\mathcal{O}$	commutative complete local noetherian ring with maximal ideal $\mathfrak{p}$ and algebraically closed residue field $k = \mathcal{O}/\mathfrak{p}$ of prime characteristic p
$\mathcal{O}G$	group algebra of the group G
$\mathcal{O}Gb$	block algebra
$(\mathcal{O}Gb)_\gamma$	source algebra of a block algebra
$\mathcal{O}_\sharp\widehat{G}$	twisted group algebra of the group G
p	characteristic of the residue field k of $\mathcal{O}$, assumed to be non-zero.
$\mathfrak{p}$	maximal ideal of $\mathcal{O}$, with residue field $k = \mathcal{O}/\mathfrak{p}$
$\mathcal{P}(A)$	set of all points of the algebra A
$\mathcal{PG}(A)$	set of all pointed groups on the G-algebra A
$\mathrm{Prim}(M)$	set of all primordial subgroups of a Mackey functor M
$\mathrm{Proj}(A)$	set of all isomorphism classes of indecomposable projective A-modules
P_γ, Q_δ	local pointed groups on a G-algebra
$P_\mathfrak{p}$, $Q_\mathfrak{q}$	primordial pointed groups on a Green functor
(P,e), (Q,f)	Brauer pairs
pr	projective relative to
$\mathrm{Res}^G_H(A)$	restriction of the G-algebra A
$\mathrm{Res}^G_H(\mathcal{F})$	restriction of the exomorphism $\mathcal{F}$
r^H_K	inclusion of fixed points, restriction
$S(\alpha)$	multiplicity algebra of the point α
$\mathcal{S}(G)$	set of all subgroups of G
S_M	almost split sequence terminating in M

$\mathrm{Soc}(M)$	socle of the module M
t_K^H	relative trace map, transfer
TM	either the module $\Omega M \oplus Q$ if $\mathcal{O} = k$, or the module $M \oplus Q$ if $\mathcal{O}$ is a discrete valuation ring, where Q is projective
$\mathrm{tr}(a; V)$	trace of the endomorphism a acting on the vector space V
$V(\alpha)$	multiplicity module of the point α
$Z(G)$	centre of the group G
$Z(A)$, ZA	centre of the algebra A
π_γ	canonical map onto the multiplicity algebra of the point γ
$\phi_{M,L}^H$	Auslander–Reiten duality

Subject Index