Field Theory: From Equations to Axiomatization

Israel Kleiner

The American Mathematical Monthly, Vol. 106, No. 7. (Aug. - Sep., 1999), pp. 677-684.

Stable URL:

http://links.jstor.org/sici?sici=0002-9890%28199908%2F09%29106%3A7%3C677%3AFTFETA%3E2.0.CO%3B2-8

The American Mathematical Monthly is currently published by Mathematical Association of America.

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at http://www.jstor.org/about/terms.html. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at http://www.jstor.org/journals/maa.html.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

The JSTOR Archive is a trusted digital repository providing for long-term preservation and access to leading academic journals and scholarly literature from around the world. The Archive is supported by libraries, scholarly societies, publishers, and foundations. It is an initiative of JSTOR, a not-for-profit organization with a mission to help the scholarly community take advantage of advances in technology. For more information regarding JSTOR, please contact support@jstor.org.

http://www.jstor.org
Sat Dec 22 05:33:33 2007

THE EVOLUTION OF...

Edited by **Abe Shenitzer**

Mathematics, York University, North York, Ontario M3J 1P3, Canada

Field Theory: From Equations to Axiomatization

Part I

Israel Kleiner

1. INTRODUCTION. The evolution of field theory spans a period of about 100 years, beginning in the early decades of the 19th century. This period also saw the development of the other major algebraic theories, namely group theory, ring theory, and linear algebra. The evolution of field theory was closely intertwined with that of the other three theories, as we shall see.

Abstract field theory emerged from three concrete theories—what came to be known as Galois theory, algebraic number theory, and algebraic geometry. These were founded, and began to flourish, in the 19th century. Of some influence in the rise of the abstract field concept were also the theory of congruences and (British) symbolical algebra. The 19th century's increased concern for rigor, generalization, and abstraction undoubtedly also had an impact on our story.

In this paper we discuss the sources of field theory as well as some of the main events in its evolution, culminating in Steinitz's abstract treatment of fields.

2. GALOIS THEORY. For three millennia (until the early 19th century) algebra meant solving polynomial equations, mainly of degrees up to 4. Field-theoretic ideas are implicit even here. For example, in solving the linear equation $ax + b = 0$, the four algebraic operations come into play and hence implicitly so does the notion of a field. In the case of the quadratic equation $ax^2 + bx + c = 0$, its solutions, $x = (-b \pm \sqrt{b^2 - 4ac})/2a$, require the adjunction of square roots to the field of coefficients of the equation. The concept of adjunction of an element to a field is fundamental in field theory.

Field-theoretic notions appear much more prominently, even if at first still implicitly, in the modern theory of solvability of polynomial equations. The groundwork was laid by Lagrange in 1770, but the field-theoretic elements of the subject were introduced by Abel and Galois in the early decades of the 19th century. Ruffini's 1799 proof of the insolvability of the quintic had a major gap because he lacked sufficient understanding of field-theoretic ideas [**16**].

Such ideas were starting points in Galois's 1831 "Mémoire sur les conditions de résolubilité des équations par radicaux" [**16**, p. 305]:

> One can agree to regard all rational functions of a certain number of determined quantities a priori. For example, one can choose a particular root

of a whole number and regard as rational every rational function of this radical. When we agree to regard certain quantities as known in this manner, we shall say that we adjoin them to the equation to be resolved. We shall say that these quantities are adjoined to the equation. With these conventions, we shall call rational any quantity which can be expressed as a rational function of the coefficients of the equation and of a certain number of adjoined quantities arbitrarily agreed upon:... One can see, moreover, that the properties and the difficulties of an equation can be altogether different, depending on what quantities are adjoined to it.

It is clear that Galois has a good insight into the fields that we would denote today by $F(u_1, u_2, \dots, u_n)$, obtained by adjoining the quantities $u_1, u_2, \dots, u_n$ to the (field of) coefficients of an equation. In the specific example mentioned, he has in mind a quadratic field, $Q(\sqrt{d})$.

Galois was the first to use the term "adjoin" in a technical sense. The notion of adjoining the roots of an equation to the field of coefficients is central in his work **[9]**, **[16]**.

One of the fundamental theorems of the subject proved by Galois is the Primitive Element Theorem. This says (in our terminology) that if E is the splitting field of a polynomial $f(x)$ over a field F, then $E = F(V)$ for some rational function V of the roots of $f(x)$. Galois used this result to determine the Galois group of the equation $f(x) = 0$ **[1]**, **[16]**. The Primitive Element Theorem was essential in all subsequent work in Galois theory until Artin bypassed it in the 1930s by reformulating Galois theory, for he felt that the theorem was not intrinsic to the subject **[9]**.

3. ALGEBRAIC NUMBER THEORY. The central field-theoretic notion here, due independently to Dedekind and Kronecker, is that of an algebraic number field $Q(a)$, where a is an algebraic number. How did it arise? Mainly from three major number-theoretic problems: Fermat's Last Theorem (FLT), reciprocity laws, and representation of integers by binary quadratic forms. Although all three problems have to do with the domain of (ordinary) integers, in order to deal with them effectively it was found necessary to embed them in domains of what came to be known as algebraic integers. The following examples illustrate the ideas involved.

(a) To prove FLT for (say) $n = 3$, that is, to show that $x^3 + y^3 = z^3$ has no nonzero integer solutions, one factors the left side to obtain the equation $(x + y)(x + yw)(x + yw^2) = z^3$, where w is a primitive cube root of unity, $w = (-1 + \sqrt{3}\,i)/2$. This is now an equation in the domain $D = \{a + bw : a, b \in Z\}$ of algebraic integers. This approach to FLT (for $n = 3$) was essentially used by Euler and later by Lamé and others **[5]**.

(b) Gauss's quadratic reciprocity law appeared in his *Disquisitiones Arithmeticae* of 1801. It says that $x^2 \equiv p \pmod{q}$ is solvable if and only if $x^2 \equiv q \pmod{p}$ is solvable, unless $p \equiv q \equiv 3 \pmod{4}$, in which case $x^2 \equiv p \pmod{q}$ is solvable if and only if $x^2 \equiv q \pmod{p}$ is not. Here p and q are odd primes **[8]**.

Gauss and others tried to extend this result to "higher" reciprocity laws. For example, for cubic reciprocity one asks about the relationship between the solvability of $x^3 \equiv p \pmod{q}$ and $x^3 \equiv q \pmod{p}$. These higher reciprocity-type problems are much more difficult to deal with than quadratic reciprocity. Gauss remarked that [**8**, p. 108]:

> The previously accepted laws of arithmetic are not sufficient for the foundations of a general theory [of higher reciprocity]... Such a theory demands that the domain of arithmetic be endlessly enlarged.

His comments were no idle speculation. In fact, he himself began to implement the above "programme" by formulating and proving a law of *biquadratic reciprocity*. To do that he extended the domain of arithmetic by introducing what came to be known as the *gaussian integers* $G = \{a + bi : a, b \in Z\}$. He could not even formulate such a law without introducing G [**8**].

(c) The problem of representing integers by binary quadratic forms, namely determining when $n = ax^2 + bxy + cy^2$ $(a, b, c \in Z)$, goes back to Fermat. In particular, Fermat asked and answered the question: which integers n are sums of two squares, $n = x^2 + y^2$? In the *Disquisitiones* Gauss studied the *general* problem very thoroughly, developing a comprehensive and beautiful, but very difficult, theory. To gain a deeper understanding of Gauss's theory of binary quadratic forms, Dedekind found that he, too, needed to extend the domain Z of integers. For example, even in the simple case of representing integers as sums of two squares, it is the equation $(x + yi)(x - yi) = z^2$ rather than $x^2 + y^2 = z^2$ that yields conceptual insight [**1**], [**10**].

Dedekind's ideas. The fundamental question in extending the domain of ordinary arithmetic to "higher" domains is whether such domains behave like the integers, namely whether they are unique factorization domains (UFDs). It is this property that facilitates the solution of problems (a)–(c). While the domains D and G introduced above are UFDs, most domains that arise in connection with the three number-theoretic problems we have described are not. For example, when we factor the left side of $x^n + y^n = z^n$ for $n > 23$, the resulting domains are never UFDs. To rescue unique factorization in such domains Dedekind introduced (in Supplement X (1871) to Dirichlet's *Vorlesungen über Zahlentheorie*) ideals and prime ideals, and showed that every ideal in these domains is a unique product of prime ideals [**10**].

But what *are* the domains with restored unique factorization? To answer that—one of the fundamental questions of his theory—Dedekind needed to introduce fields, in particular *algebraic number fields* $Q(a)$, where a is a root of a polynomial with integer coefficients. These were the natural habitats of his domains, just as the rationals are the natural habitat of the integers. The domains in question were then defined as "the integers of $Q(a)$," namely those elements of $Q(a)$ that are roots of *monic* polynomials with integer coefficients. Dedekind showed that they form a commutative ring with identity and without zero divisors whose field of quotients is $Q(a)$ [**3**], [**10**], [**13**].

Given Dedekind's predisposition for abstraction—a rather rare phenomenon in the 1870s, he placed his theory in a broader context by giving axiomatic definitions of rings, fields, and ideals. Here is his definition of a field [**1**, p. 117]:

> By a field we will mean every infinite system of real or complex numbers so closed in itself and perfect that addition, subtraction, multiplication, and division of any two of these numbers again yields a number of the system.

To Dedekind, then, fields were subsets of the complex numbers, which is, of course, all he needed for his theory of algebraic numbers. Still, an axiomatic definition in number theory/algebra, even in this restricted sense, is remarkable for that time. Also remarkable are Dedekind's use of infinite sets ("systems"), which predates Cantor's, and his "descriptive" rather than "constructive" definition of a mathematical object as a set of all elements of a certain kind satisfying a number of properties.

The field concept was a unifying mathematical notion for Dedekind. Before his definition of a field he says [**4**, p. 131]:

> In the following paragraphs I have attempted to introduce the reader into a higher domain, in which algebra and number theory interconnect in the most intimate manner.... I became convinced that studying the algebraic relationship of numbers is most conveniently based on a concept that is directly connected with the simplest arithmetic properties. I had originally used the term "rational domain," which I later changed to "field."

Hilbert remarked that Gauss, Dirichlet, and Jacobi had also expressed their amazement at the close connection between number theory and algebra, on the grounds that these subjects have common roots in (as Dedekind would put it) the theory of fields [**4**].

Dedekind produced several editions of his groundbreaking theory of ideal decomposition in algebraic number fields. In his mature 1894 version (4th edition of Dirichlet's *Zahlentheorie*) he included important concepts and results on fields—nowadays standard—such as [**9**, pp. 130–132]:

(i) If S is any subset of the complex numbers containing the rationals, the intersection of all fields containing S is a field; it is called "rational with respect to S."
(ii) He defines field isomorphism, calling it "permutation of the field," as a mapping of a field E onto a field F that preserves all four operations of the field. He observes that if F is nonzero, the mapping is one-one. He also notes that the mapping is the identity on Q.
(iii) If E is a subfield of K, he defines the *degree* of K over E as the dimension of K considered as a vector space over E. He shows that if the degree is finite then every element of K is algebraic over E.

Kronecker's ideas. Kronecker's work was broader but much more difficult than Dedekind's. He developed his ideas over several decades, beginning in the 1850s, trying to frame a general theory that would subsume algebraic number theory and algebraic geometry as special cases. In his great 1882 work *Grundzüge einer arithmetischen Theorie der algebraischen Grössen* he developed algebraic number theory using an approach entirely different from Dedekind's. One of his central concepts was also that of a field—he called it "domain of rationality," defined as follows [**9**, p. 127]:

> The domain of rationality $(R', R'', R''', \dots)$ contains every one of those quantities which are rational functions of the quantities $R', R'', R''', \dots$ with integer coefficients.

Note how different Kronecker's "definition" of a field is from Dedekind's! It is a constructive description, rather than the kind of definition that would be acceptable to us today. But it was dictated by Kronecker's views on the nature of mathematics.

Kronecker rejected irrational numbers as bona fide entities since they involve the mathematical infinite. For example, the algebraic number field $Q(\sqrt{2})$ was defined by Kronecker as the quotient field of the polynomial ring $Q[x]$ relative to the ideal generated by $x^2 - 2$, though he would have put it in terms of congruences rather than quotient rings. These ideas contain the germ of what came to be known as Kronecker's Theorem, namely that every polynomial over a field has a root in some extension field **[9]**, **[13]**.

It is interesting to compare this definition of $Q(\sqrt{2})$ with Cauchy's definition in the 1840s of the complex numbers as polynomials over the reals modulo $x^2 + 1$ (and compare the latter with Gauss's integers modulo p). Cauchy's rationale was to give an "algebraic" definition of complex numbers that would avoid the use of $\sqrt{-1}$.

Dedekind vs. Kronecker. Dedekind and Kronecker were great contemporary algebraists. Both published pathbreaking works on algebraic number theory. But their approaches to the subject were very different. Both were guided in their works by their "philosophies" of mathematics, and these too were very different **[13]**. Kronecker was perhaps the first preintuitionist, Dedekind likely the first preformalist (cf. Kronecker's "God made the [positive] integers, all the rest is the work of man" with Dedekind's "[The natural] numbers are a free creation of the human mind"). To Kronecker mathematics had to be constructive and finitary. Dedekind did not hesitate to use axiomatic notions and the infinite. While Kronecker made frequent pronouncements on these topics, Dedekind made few; his views became known mainly from his works—conceptual and abstract. Some examples:

(i) Since Kronecker's domains of rationality had to be generated by *finitely* many elements (the $R', R'', R''', \dots$), his definition would not admit the totality of algebraic numbers as a field. Dedekind had no problem in considering the set of all complex numbers that are roots of polynomial equations with integer coefficients (viz. the set of all algebraic numbers) as a bona fide mathematical object.

(ii) On the other hand, Kronecker put no restriction on the nature of the entities $R', R'', R''', \dots$—they could, for example, be indeterminates or roots of algebraic equations. So $Q(x)$ was a legitimate field to Kronecker. In fact, the adjunction of indeterminates to a field was a cornerstone of his approach to algebraic number theory. Dedekind, recall, defined his fields to be subsets of the complex numbers (but see Section 4).

(iii) Since Kronecker did not accept π (say) as a legitimate number, he identified $Q(\pi)$ with $Q(x)$ (x an indeterminate), thus claiming that transcendental numbers are indeterminate! To Dedekind $Q(\pi)$ was a perfectly legitimate entity not requiring any assistance from $Q(x)$.

4. ALGEBRAIC GEOMETRY. The examples of fields we have come across so far have been mainly fields of numbers. Here we encounter principally fields of functions, in particular, algebraic functions and rational functions. The ideas are due mainly to Kronecker and Dedekind-Weber.

Fields of algebraic functions. Algebraic geometry is the study of algebraic curves and their generalizations to higher dimensions, algebraic varieties. An *algebraic curve* is the set of roots of an algebraic function, that is, a function $y = f(x)$ defined implicitly by a polynomial equation $P(x, y) = 0$.

Several approaches were used in the study of algebraic curves, notably the analytic, the geometric-algebraic, and the algebraic-arithmetic. In the analytic approach, to which Riemann (in the 1850s) was the major contributor, the main objects of study were algebraic functions $f(w, z) = 0$ of a complex variable and their integrals, the so-called abelian integrals. It was in this connection that Riemann introduced the fundamental notion of a Riemann surface, on which algebraic functions become single-valued. Riemann's methods, however, were nonrigorous, relying heavily on the physically obvious but mathematically questionable Dirichlet Principle [**3**], [**11**].

Dedekind and Weber, in their important 1882 paper "Theorie der algebraischen Funktionen einer Veränderlichen," set for themselves the task of making Riemann's ideas rigorous, or, as they put it [**11**, p. 154]:

> The purpose of the[se] investigations... is to justify the theory of algebraic functions of a single variable, which is one of the main achievements of Riemann's creative work, from a simple as well as rigorous and completely general viewpoint.

To accomplish this, they carried over to algebraic functions the ideas that Dedekind had earlier introduced for algebraic numbers. Specifically, just as an algebraic number field is a finite extension $Q(a)$ of the field Q of rational numbers, so Dedekind and Weber defined an *algebraic function field* as a finite extension $K = C(z)(w)$ of the field $C(z)$ of rational functions (in the indeterminate z). That is, w is a root of a polynomial $p(t) = a_0 + a_1t + a_2t^2 + \cdots + a_nt^n$, where $a_i \in C(z)$ (we can take $a_i \in C[z]$). Thus $w = f(z)$ is an algebraic function defined implicitly by the polynomial equation $P(z, w) = a_0 + a_1w + a_2w^2 + \cdots + a_nw^n = 0$. In fact, all the elements of $K = C(z)(w) = C(z, w)$ are algebraic functions.

Now let A be "the integers of K"; that is, A consists of the elements of $K = C(z)(w)$ that are roots of monic polynomials over $C[z]$ (cf. "the integers of $Q(a)$," Section 3). By analogy with the case of algebraic numbers, here too A is an integral domain and every nonzero ideal of A is a unique product of prime ideals [**1**], [**3**]. Incidentally, the meromorphic functions on a Riemann surface form a field of algebraic functions, with the entire functions as their "integers."

Dedekind and Weber were now ready to give a rigorous, algebraic definition of a Riemann surface S of the algebraic function field K: It is (in our terminology) the set of nontrivial discrete valuations on K. The finite points of S correspond to the ideals of A; to deal with points at infinity of S, they introduced the notions of "place" and "divisor" [**3**]. They developed many of Riemann's ideas on algebraic functions algebraically and rigorously. In particular, they gave a rigorous algebraic proof of the important Riemann-Roch Theorem [**1**], [**3**], [**11**].

Dedekind and Weber were at heart algebraists. They felt that algebraic function theory is intrinsically an algebraic subject, hence it ought to be developed algebraically. As they put it: "In this way, a well-delimited and relatively comprehensive part of the theory of algebraic functions is treated solely by means belonging to its own domain" [**11**, p. 156].

Beyond their technical achievements in putting major parts of Riemann's algebraic function theory on solid ground, the conceptual breakthrough by Dedekind and Weber lay in pointing to the strong analogy between algebraic number fields and algebraic function fields, hence between algebraic number theory and algebraic geometry. This analogy proved most fruitful for both theories.

Another noteworthy aspect of their work was its generality, in particular its applicability to arbitrary fields; see [**6**], [**15**].

Fields of rational functions. As noted earlier, algebraic geometry is the study of algebraic varieties. An algebraic variety is the set of points in R^n (or C^n) satisfying a system of polynomial equations $f_i(x_1, x_2, \dots, x_n) = 0$, $i = 1, 2, \dots, k$; the Hilbert basis theorem implies that finitely many equations will do. The ideal structure of the ring $R[x_1, \dots, x_n]$ (or $C[x_1, \dots, x_n]$) to which the polynomials $f_i(x_1, x_2, \dots, x_n)$ belong is fundamental for the understanding of the algebraic variety, as is the "natural habitat" of that ring—its field of quotients $R(x_1, \dots, x_n)$ (or $C(x_1, \dots, x_n)$). These are the fields of (formally) *rational functions*. We have seen that such fields were also introduced by Kronecker in connection with his work in algebraic number theory [**6**], [**13**].

5. CONGRUENCES.

Gauss introduced the congruence notation in the *Disquisitiones Arithmeticae* of 1801 and showed (among other things) that one can add, subtract, multiply, and divide congruences modulo a prime p, in effect that the integers modulo p form a field—a *finite* field of p elements. Inspired by Gauss's work on congruences, Galois introduced finite fields with p^n elements in an 1830 paper entitled "Sur la theorie des nombres."

Galois's aim was to study the congruence $F(x) \equiv 0 \pmod{p}$ as a generalization of Gauss's quadratic congruences (cf. Gauss's quadratic reciprocity law). Here $F(x)$ is a polynomial of degree n that is irreducible mod p, i.e., $F(x)$ is irreducible over the field Z_p. Galois showed that $F(x)$ has no integral roots [mod p]. His conclusion was that [**7**, pp. 277–278]:

> One should therefore regard the roots of this congruence as some kind of imaginary symbols..., symbols whose employment in calculation will often prove as useful as that of the imaginary $\sqrt{-1}$ in ordinary analysis.

He continues:

> Let i [an arbitrary symbol, *not* the complex number i] denote one of the roots of the congruence $F(x) \equiv 0$, which can be supposed to have degree n. Consider the general expression
>
> $$a + a_1 i + a_2 i^2 + \cdots + a_{n-1} i^{n-1}, \qquad (**)$$
>
> where $a, a_1, a_2, \dots, a_{n-1}$ represent integers [mod p]. When these numbers are assigned all their possible values, expression (**) takes on p^n values, which possess, as I shall demonstrate, the same properties as the natural numbers in the *theory of residues of powers*.

Galois did, indeed, show that the expressions (**) form a field, now called a *Galois field*. He also showed that (in our terminology) the multiplicative group of that field is cyclic [**1**], [**7**], [**13**]. In an 1893 paper entitled "A doubly-infinite system of simple groups," E. H. Moore characterized the finite fields [**12**].

6. SYMBOLICAL ALGEBRA.

In the third and fourth decades of the 19th century British mathematicians, notably Peacock, Gregory, and De Morgan, created what came to be known as symbolical algebra. Their aim was to set algebra—to them this meant the laws of operation with numbers, negative numbers especially—on an equal footing with geometry by providing it with logical justification. They did this by distinguishing between *arithmetical algebra*—laws of operation with positive numbers, and *symbolical algebra*—a subject newly created by Peacock, which dealt with laws of operation with numbers in general.

Although the laws were carried over verbatim from those of arithmetical algebra, in accordance with the so-called Principle of Permanence of Equivalent Forms, the point of view was remarkably modern. Witness Peacock's definition of symbolical algebra, given in his *Treatise of Algebra* of 1830 [**14**, p. 35]:

> The science which treats of the combinations of arbitrary signs and symbols by means of defined though arbitrary laws.

Quite a statement for the early 19th century! Such sentiments were about a century ahead of their time. And of course one did have to wait about a century to have what Peacock had preached put fully into practice. Nevertheless, the creation of symbolical algebra was a significant development, even if not directly related to fields, signalling (according to some) the birth of abstract algebra [**2**].

REFERENCES

1. I. G. Bashmakova and E. I. Slavutin, Algebra and algebraic number theory, in *Mathematics of the 19th Century*, ed. by A. N. Kolmogorov and A. P. Yushkevich, Birkhäuser, 1992, pp. 35–135.
2. G. Birkhoff, Current trends in algebra, *Amer. Math. Monthly* **80** (1973) 760–782, and corrections in **81** (1974) 746.
3. N. Bourbaki, *Elements of the History of Mathematics*, Springer-Verlag, 1984.
4. L. Corry, *Modern Algebra and the Rise of Mathematical Structures*, Birkhäuser, 1996.
5. H. M. Edwards, *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*, Springer-Verlag, 1977.
6. D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, 1995.
7. E. Galois, Sur la theorie des nombres, English translation in S. Stahl, *Introductory Modern Algebra: A Historical Approach*, Wiley, 1997, pp. 277–284.
8. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer-Verlag, 1982.
9. B. M. Kiernan, The development of Galois theory from Lagrange to Artin, *Arch. Hist. Exact Sci.* **8** (1971/72) 40–54.
10. I. Kleiner, The roots of commutative algebra in algebraic number theory, *Math. Mag.* **68** (1995) 3–15.
11. D. Laugwitz, *Bernhard Riemann, 1826–1866*, Birkhäuser, 1999. Translated from the German by A. Shenitzer.
12. E. H. Moore, A doubly-infinite system of simple groups, *New York Math. Soc. Bull.* **3** (1893) 73–78.
13. W. Purkert, Zur Genesis des abstrakten Körperbegriffs I, II, *Naturwiss., Techn. u. Med.* **8** (1971) 23–37 and **10** (1973) 8–20. Unpublished English translation by A. Shenitzer.
14. H. M. Pycior, George Peacock and the British origins of symbolical algebra, *Historia Math.* **8** (1981) 23–45.
15. J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, 1992.
16. J.-P. Tignol, *Galois' Theory of Algebraic Equations*, Wiley, 1988.