



On an Example of Jacobson

B. Sury

The American Mathematical Monthly, Vol. 106, No. 7. (Aug. - Sep., 1999), pp. 675-676.

Stable URL:

<http://links.jstor.org/sici?sici=0002-9890%28199908%2F09%29106%3A7%3C675%3AOAEOJ%3E2.0.CO%3B2-J>

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.

On an Example of Jacobson

B. Sury

In Vol. III of Nathan Jacobson's celebrated book [2], there appears the following exercise on p. 49:

Let \mathbb{F}_p be the field with p elements, and $P = \mathbb{F}_p(x, y)$ where x, y are indeterminates. Let E be the subfield $\mathbb{F}_p(x^p - x, y^p - x)$. Show that $[P : E] = p^2$, that P/E is not separable, and that P/E contains no purely inseparable element.

Now, it is seen immediately that Jacobson's example is really a nonexample. Surprisingly, none of the other standard graduate texts seem to give an example, although one can be found in [1, Ex. 17, Ch. V]. Here is another:

Example. Let $P = \mathbb{F}_p(x, y)$ and let E be the subfield $\mathbb{F}_p(x^p - x, y^p x)$. Then

- (i) $[P : E] = p^2$,
- (ii) P/E is not separable, and
- (iii) P/E contains no purely inseparable element over E except those contained in E .

Recall that an element x in an algebraic closure \bar{K} of a field K is *separable* if its minimal polynomial $f(T)$ in $K[T]$ has all roots (in \bar{K}) simple.

It is said to be *purely inseparable* over K if it is fixed by all K -automorphisms of \bar{K} . More generally, an algebraic extension L of K is said to be *purely inseparable* if the only elements of L that are separable over K are the elements of K itself. Any algebraic extension L of K is built in two stages: $K \subset L_{sep} \subset L$, where L_{sep} is separable over K , and L is purely inseparable over L_{sep} .

One has as a consequence of this definition:

Let $x \in \bar{K}$, and let $f(T)$ be its minimal polynomial over K . Then, the following statements are equivalent:

- (i) x is not separable over K ;
- (ii) The derivative $f'(T)$ is the zero polynomial; and
- (iii) K is of characteristic $p > 0$, and $f(T) \in K[T^p]$.

Under any of these equivalent hypotheses, if n is the smallest integer such that $x^{p^n} \in K$, then the minimal polynomial over K is $f(T) = T^{p^n} - x^{p^n}$.

We return to our example now.

$P = \mathbb{F}_p(x, y) \supset E = \mathbb{F}_p(a, b)$ where $a = x^p - x$, $b = y^p x$. Then, over E , y satisfies the polynomial $g(T) = T^{p^2} + rT^{p(p-1)} - s$, where $r = b/a$ and $s = b^p/a$. Also, $P = E(y)$.

We note:

(a) x is separable over E and y is inseparable over E .

The separability of x follows from the preceding remarks by looking at the polynomial $T^p - T - (x^p - x)$. This is a polynomial over E satisfied by x . In fact, the Artin-Schreier Theorem [3, Ch. 8] shows that this polynomial is irreducible and is the minimal polynomial of x over E . However, we do not need this fact for the proof.

The inseparability of y is a consequence of the observation that $T^p - y^p$ is the minimal polynomial of y over the field $E(x)$.

(b) y is not purely inseparable over E .

As $y^p \notin E$, one has also $y^{p^2} \notin E$; otherwise, from $g(y) = 0$ one concludes $y^{p(p-1)} \in E$, which would lead to the erroneous conclusion $y^p \in E$.

(c) x is not a p -th power in P .

This is easy to check by a simple comparison of like powers of x in view of the algebraic independence of x and y over \mathbb{F}_p .

Suppose $t \in P \setminus E$ is purely inseparable over E . Then $t^p \in E$ (because if $t^{p^n} \in E$ for some $n \geq 2$, then since the degree of $P = E(y)$ over E is at most p^2 , $n \leq 2$. But, if $n \neq 1$, then P would be purely inseparable, a contradiction).

Look at $P \supset E(t) \supset E$. Now, the minimal polynomial of t over E is $T^p - t^p$, and $[E(t) : E] = p$. Note that $\alpha^p \in E$ for all $\alpha \in E(t)$.

Let $[P : E(t)] = l$, say. If the minimal polynomial of y over $E(t)$ is $f(T) = \sum_{i=0}^l a_i T^i$, then y satisfies the polynomial $f(T)^p = \sum_{i=0}^l a_i^p T^{ip}$. As this is the minimal polynomial of y over E , $f(T)^p$ divides $g(T)$. If $f(T)^p \sum u_i T^i = T^{p^2} + rT^{p(p-1)} - s$, one gets $u_i = 0$ if $i \not\equiv 0 \pmod p$. Renaming $u_{i/p}$ as v_i , the equation $\sum_{i=0}^l a_i^p T^{ip} \sum_{i=0}^{p-1} v_i T^{ip} = T^{p^2} + rT^{p(p-1)} - s$ gives inductively that $v_i = sb_i^p$ for some $b_i \in P$. Therefore, comparing the coefficients of $T^{p(p-1)}$ on both sides, we see $r = sv^p$ for some $v \in P$. This means that x is a p -th power in P , which is a contradiction.

Therefore, P has no purely inseparable elements outside of E .

Remarks. As a consequence of the proof, it is clear that $T^{p^2} + rT^{p(p-1)} - s$ is the minimal polynomial of y over E . The extension P of E is built up in two steps $P \supset E(x) \supset E$ with P purely inseparable of degree p over $E(x)$ and $E(x)$ separable of degree p over E .

REFERENCES

1. N. Bourbaki, *Algebre*, Actualites Scientifiques et Industrielles 1102, Hermann, Paris, 1950.
2. N. Jacobson, *Lectures in abstract algebra*, Vol. III, Van Nostrand, 1964.
3. S. Lang, *Algebra*, Addison-Wesley Publishing Company, Mass., 1965.

School of Mathematics, Tata Institute of Fundamental Research, Mumbai 400005, India.
sury@math.tifr.res.in