A SIMPLE NEW PROOF OF THE PRIMITIVE ELEMENT THEOREM

Ilse Fischer

Institut für Mathematik der Universität Wien,
Strudlhofgasse 4, A-1090 Wien, Austria.

Abstract. In this note we give a new proof of the well-known Primitive Element Theorem in the theory of fields. The proof is based on a lemma which states that it is impossible to decompose a field set-theoretically into proper subfields.

Mathematics Subject Classification: 12F10
Keywords: field theory, finite separable extensions.

1. Introduction

The purpose of this note is to present a simple new proof of the following version of the Primitive Element Theorem:

Theorem (Primitive Element Theorem). *Let k be a field and K a finite separable extension of k. Then there exists $\alpha \in K$ (a so-called primitive element) such that $K = k[\alpha]$.*

The usual proofs (see e.g. [2, p.186] or [1, p.250]) distinguish two cases: If k is infinite, they reduce the theorem to $K = k[\beta, \gamma]$ and choose α as a linear combination $\alpha = \beta + c\gamma$ ($c \in k$). If k is finite, these proofs use the characterization of finite fields.

The present proof manages to explain the theorem without reduction to fields $K = k[\beta, \gamma]$. In addition the distinction beetween the cases $|k| = \infty$ and $|k| < \infty$ will not be necessary either.

Besides this new proof uses a quite interesting lemma, which is a generalization of the following popular exercise for algebra students: *Let K be a field and K_1, K_2 be proper subfields of K. Show that $K_1 \cup K_2 \neq K$.*

2. Preliminaries

Our proof of the Primitive Element Theorem chiefly involves the k-monomorphisms $\sigma : K \to C$ (where C denotes an algebraic closure of k). Therefore we use the following characterization of separability:

Theorem. *The field K is separable over k if and only if there exist precisely $n = [K : k]$ different k-monomorphisms $\sigma : K \to C$*

For a proof of the theorem see e.g. [2, p.178] or [1, p.244]. In the following let $G = \{\sigma_1, ..., \sigma_n\}$ denote the set of these k-monomorphisms $\sigma : K \to C$.

In order to prove the Primitive Element Theorem the following concept will be fundamental:

Definition. *Let $\mathcal{A} = \{A_1, ...A_k\}$ be a partition of G. We say $\beta \in K$ 'obeys' $\mathcal{A}$, if for every i and for any two elements $\sigma_u, \sigma_v \in A_i$ we have $\sigma_u(\beta) = \sigma_v(\beta)$.*

Obviously the set of elements 'obeying' a fixed partition $\mathcal{A}$ forms a field beetween k and K. Therefore we have a mapping from the set of partitions of G into the set of fields beetween k and K. In the following we denote the subfield of K that corresponds to that partition $\mathcal{A}$ by $K_{\mathcal{A}}$.

It may be interesting to mention the following analogy with Galois-theory: There the main tool is the isotonic bijection from the set of the subgroups of the Galoisgroup $G(K/k)$ onto the set of fields beetween k and K (if K/k is normal). Instead of subgroups of we use partitions of G and if we define $\mathcal{A}_1 \leq \mathcal{A}_2$ if $\mathcal{A}_2$ refines $\mathcal{A}_1$, the mapping $\mathcal{A} \to K_{\mathcal{A}}$ becomes isotonic, too. Note that our mapping is not bijectiv.

We denote the largest partition concerning this ordering by $\mathcal{E} = \{\{\sigma_1\}, \ldots, \{\sigma_n\}\}$.

3. The proof of the theorem

First we will see that it suffices to show that there exists a $\alpha \in K$ such that all $\sigma_i(\alpha)$ are distinct: Let $f(X) \in k[X]$ be the minimal polynomial of $\sigma_1(\alpha)$ over k. The k-monomorphism which sends $\sigma_1(\alpha)$ to $\sigma_i(\alpha)$ and holds each element of k fixed applied to the equation $f(\sigma_1(\alpha)) = 0$ gives $f(\sigma_i(\alpha)) = 0$, $i = 1, 2, \ldots, n$. Therefore $[k[\sigma_1(\alpha)] : k] \geq n$. On the other hand $[k[\sigma_1(\alpha)] : k] = [k[\alpha] : k] \leq [K : k] = n$. We obtain $[k[\alpha] : k] = n$ and together with $k[\alpha] \subseteq K$ this implies $K = k[\alpha]$.

The mapping $\mathcal{A} \to K_{\mathcal{A}}$ is generally not injective, but $K_{\mathcal{A}} = K$ if and only if $\mathcal{A} = \mathcal{E}$ (Assume the existence of a partition $\mathcal{A} \neq \mathcal{E}$ with $K_{\mathcal{A}} = K$. Let $|A_i| \geq 2$ with $A_i \in \mathcal{A}$, $\sigma_u \neq \sigma_v \in A_i$ and $\gamma \in K = K_{\mathcal{A}}$. Then $\sigma_u(\gamma) = \sigma_v(\gamma)$ and since γ was arbitrary, this contradicts $\sigma_u \neq \sigma_v$.). The main tool of the proof is the following

Lemma. *Let $K_1, K_2, \ldots, K_m$ be proper subfields of K. Then $K_1 \cup \cdots \cup K_m \subsetneq K$.*

(For a proof see section 4.)

The fact that $|G| < \infty, K_{\mathcal{A}} \subsetneq K$ when $\mathcal{A} \neq \mathcal{E}$ and the lemma result in

$$\bigcup_{\mathcal{A} \neq \mathcal{E}} K_{\mathcal{A}} \subsetneq K.$$

Hence, there exists an element $\alpha \in K = K_{\mathcal{E}}$ with $\alpha \notin K_{\mathcal{A}}$ for every $\mathcal{A} \neq \mathcal{E}$. That implies that all $\sigma_i(\alpha)$, $i = 1, 2, \ldots n$, are distinct and completes the proof of the theorem. □

4. The proof of the lemma

Now we consider the lemma. It seems likely to be a well-known result, but I was unable to find a reference in literature.

Proof of the lemma. We assume the contrary (i.e. $K_1 \cup \cdots \cup K_m = K$, K_i being proper subfields of K). Without loss of generality we may additionally suppose the existence of elements $x_i \in K_i \setminus \bigcup_{j \neq i} K_j, i = 1, 2, \ldots, m$. Let $L = \bigcap_{i=1}^{m} K_i$.

First we show that $\alpha^{(m-1)!(m-2)!\ldots 1!} \in L$ for every $\alpha \in K$: Without loss of generality we may assume $\alpha \in K_1 \setminus \{0\}$. The m elements $x_2, x_2\alpha, \ldots, x_2\alpha^{m-1}$ are in $K_2 \cup \cdots \cup K_m$, since $\alpha \in K_1$ but $x_2 \notin K_1$. Therefore at least one of the fields K_i $(i = 2, 3, \ldots, m)$, without loss of generality K_2, includes at least two of these elements, say $x_2\alpha^p$ and $x_2\alpha^q$. We obtain $x_2\alpha^p / x_2\alpha^q = \alpha^{p-q} \in K_2$, and since $1 \leq |p - q| \leq m - 1$ we have $\alpha^{(m-1)!} \in K_1 \cap K_2$.

Now we consider the $m - 1$ elements $x_3, x_3\alpha^{(m-1)!}, \ldots, x_3\alpha^{(m-1)!(m-2)} \in K_3 \cup \cdots \cup K_m$ (since $\alpha^{(m-1)!} \in K_1, K_2$, but $x_3 \notin K_1, K_2$). Thus we may assume that there exist distinct

$p, q \in \{0, 1, \ldots, m-2\}$ with $x_3\alpha^{(m-1)!p}, x_3\alpha^{(m-1)!q} \in K_3$ and in the same way as above this implies $\alpha^{(m-1)!(m-2)!} \in K_1 \cap K_2 \cap K_3$.

After $m-1$ steps of this kind (of which we did two) we obtain $\alpha^{(m-1)!(m-2)!\ldots 1!} \in L$.

Next we show that every element $\beta \in L \setminus \{0\}$ is a root of unity with degree $\leq m$ and therefore $\beta^{m!} = 1$. This together with our last observation will then imply $\alpha^{m!(m-1)!\ldots 1!} = 1$ for every $\alpha \in K \setminus \{0\}$.

Assume that $\beta \in L \setminus \{0\}$ is not a root of unity with degree $\leq m$. Then the m elements $1, \beta, \ldots, \beta^m$ are distinct. We consider the $m+1$ elements $x_1 + x_2\beta^i, i = 0, 1, \ldots, m$, of K. There exists a subfield K_i, which includes at least two of these elements, say $x_1 + x_2\beta^j$ and $x_1 + x_2\beta^k$. The difference $x_2(\beta^j - \beta^k) \in K_i$, and thus $x_2 \in K_i$, since $\beta^j - \beta^k \in K_i \setminus \{0\} \supseteq L \setminus \{0\}$. Therefore $i = 2$. But then $x_1 = (x_1 + x_2\beta^j) - (x_2\beta^j) \in K_2$. This contradicts our choice of the elements x_i's.

Since there exists a natural number $R \neq 0$, namely $R = m!(m-1)!\ldots 1!$, such that every non-zero element of K is an R-th root of unity, we may choose the smallest natural number $r \neq 0$ with this property. The equation $X^r - 1 = 0$ in X has at most r solutions in the field K and therefore we already know that $|K| \leq r + 1$.

We claim the existence of a primitive r-th root of unity in K: If this was not the case, let $s \in \mathbb{N}$ be maximal such that there exists a primitive s-th root of unity $\zeta_1 \in K$. According to our assumption we have $s < r$. Additionally we may suppose the existence of an element $\zeta_2 \in K$ such that ζ_2 is a primitive t-th root of unity and $t \not| s$ (If not, every element in $K \setminus \{0\}$ would be a s-th root of unity and that contradicts the choice of r and s). It is easy to see that $\zeta_1 \cdot \zeta_2$ is a primitve $\frac{st}{ggt(s,t)}$-th root of unity. But since $t \not| s$ we have $\frac{st}{ggt(s,t)} > s$ and this contradicts the choice of r.

Let $\zeta \in K$ be this r-th root of unity. Then the r elements $\zeta^i, i = 0, 1, \ldots, r-1$, are distinct. This together with $|K| \leq r+1$ shows that every non-zero element of K must be a power of ζ. Finally this implies that the subfield K_i, which includes ζ, equals K, and contradicts our assumption that the K_i's are proper subfields of K. $\square$

By the way: The following stronger generalization of the student exercise mentioned in Section 1 is not true:

Let G be a group and $G_1, G_2, \ldots, G_n$ be proper subgroups of G. Then $G_1 \cup G_2 \cup \cdots \cup G_n \neq G$.

A counterexample: Let $G = \mathbb{F}_2^2$, where $\mathbb{F}_2$ denotes the field with two elements. Then

$$G = G_1 \cup G_2 \cup G_3,$$

where $G_1 = \{(0,0), (1,0)\}$, $G_2 = \{(0,0), (0,1)\}$ and $G_3 = \{(0,0), (1,1)\}$.

References

[1] J. Cigler. Körper, Ringe, Gleichungen. Spektrum 1995
[2] S. Lange. Algebra, Addison-Wesley 1968.