On the Primitive Element Theorem

Rohan Mukherjee

February 16, 2024

Abstract

In this short excerpt we prove the primitive element theorem and discuss an important counterexample.

It is a central fact of Galois theory that inseparable extensions only exist in characteristic p. Indeed, let k be a field of characteristic 0, and $f(x) \in k[x]$ be an irreducible polynomial. Suppose that f were inseparable–i.e. that there exists α a root of f with multiplicity $m \geq 2$ in an algebraic closure $\overline{k}$, and write $f(x) = (x-\alpha)^m g(x)$. Then we can take the formal derivative,

$$\frac{\mathrm{d}}{\mathrm{d}x} : \sum_{i=0}^{n} a_n x^n \mapsto \sum_{i=1}^{n} n a_n x^{n-1}.$$

It is clear that this map is linear and that the product and chain rules hold. Then,

$$f'(x) = (x-a)^n g'(x) + n(x-a)^{n-1} g(x) = (x-a)^{n-1} q(x)$$

For some polynomial q. In particular, α is also a root of f'. Letting $d(x) = \gcd(f(x), f'(x))$, by Bezout's lemma we can find $r(x), s(x)$ so that,

$$r(x)f'(x) + s(x)f(x) = d(x)$$

f is irreducible, so its only (monic) divisors are 1 and itself. Since $\deg f' = \deg f - 1$, $d(x) \neq f(x)$, which shows that $d(x) = 1$. Plugging in α to the above equation shows that $0 = 1$, a contradiction. But how does this argument fail outside of characteristic 0? It turns out that the derivative could be equivalently 0, in which case $d(x) = f(x)$. As an example, consider the polynomial

$$f(x) = x^p - a^p \in \mathbb{F}_p[x]$$

A simple exercise shows that $f(x) = x^p - a^p = (x-a)^p$. In particular, this shows that $f : k \to k$ defined by $f(x) = x^p$ is a field homomorphism of k if k has characteristic p. As k is an integral domain, taking $0 \neq y \in k$ shows that $f(y) = y^p \neq 0$, so $\ker f \neq k$ implying that f is actually injective. Injective maps from a vector space to another vector space of the same dimension are surjective, thus f is an automorphism. f is called the *Frobenius automorphism*, and is extremely helpful in describing the Galois group of $\mathbb{F}_{p^n}/\mathbb{F}_p$. An important consequence of this observation is that pth roots always exist in $\mathbb{F}_{p^n}$.

We now describe an irreducible, inseparable polynomial in a field (necessarily) of characteristic p. Consider $K = \mathbb{F}_p(t) = \mathrm{Frac}(\mathbb{F}_p[t])$. We claim the polynomial $f(x) = x^p - t$ is irreducible over K. Indeed, since,

$$\frac{\mathbb{F}_p[t]}{(t)} \cong \mathbb{F}_p$$

(t) is prime ideal of $\mathbb{F}_p[t]$, so we can apply Eisenstein's criterion to see that $f(x)$ is irreducible over $\mathbb{F}_p[t]$, and, by Gauss's lemma, over $\mathbb{F}_p(t)$. Let $\sqrt[p]{t}$ be a root of f in some algebraic closure. Then $f(x) = (x - \sqrt[p]{t})^p$ is a factorization in the algebraic closure by our discussion above, so f is not separable. Notice indeed that $f'(x) = px^{p-1} \equiv 0$.

We now provide a proof of the primitive element theorem, and discuss a counterexample of a similar flavor as above.

Theorem 1. *Let K/k be a finite field extension. Then there exists $\alpha \in K$ so that $K = k(\alpha)$ iff there are only finitely many distinct subextensions $k \subset E \subset K$. In particular, if K is separable then $K = k(\alpha)$.*

Proof. Let $K = k(\alpha)$ and let $k \subset E \subset K$ be a subextension. Define

$$\psi : E \mapsto \mathrm{Irr}_E(\alpha)$$

We shall show that ψ is injective. First, let $p(x) = \mathrm{Irr}_k(\alpha)$ and fix $q(x) = \mathrm{Irr}_E(\alpha)$. Let $d(x) = \gcd(p(x), q(x)) \in E[x]$. Since $q(x)$ is irreducible, if $d(x) \neq q(x)$, $d(x) = 1$. Once again by Bezout, there is some r, s so that $rp + qs = 1$. Plugging in α shows $0 = 1$ a contradiction, so $q(x) \mid p(x)$. Let $q(x) = \sum_{k=0}^{n} a_n x^n$, and consider $F = k(a_1, \cdots, a_n)$. Clearly, $F \subset E$, $q(x) \in F[x]$, and combined with the fact that $\mathrm{Irr}_E(\alpha) \mid \mathrm{Irr}_F(\alpha)$, shows that $F = E$ by comparing degrees. Thus, if E'/k is another subextension with $\mathrm{Irr}_{E'}(\alpha) = q(x)$, $F \subset E'$ as well and by the same argument $F = E' = E$, so ψ is injective. Now, let,

$$p(x) = \prod_i (x - \alpha_i)$$

Be a factorization of $p(x)$ in an algebraic closure of k containing K. Since there are only finitely many monic divisors of $p(x)$ (every divisor would have only a subset of the above product terms), and since $q(x) \mid p(x)$, the number of distinct subextensions of K is finite.

Now let K/k be a finite extension of k with only finitely many subextensions. If k is finite, then $k = \mathbb{F}_{p^n}$ and $K = \mathbb{F}_{p^m}$ for $n \mid m$. We first prove the following lemma.

Lemma 1. *Let F be a field and $G \subset F$ be a finite multiplicative subgroup. Then G is cyclic.*

Proof. Let $n = |G|$, and let $y \in G$ be an element of maximal order $|y| = m$. Then for any $x \in G$, it follows (nontrivially!) that $|x| \mid m$. Thus every $x \in G$ is a solution to the equation $x^m - 1 = 0$. Since $|G| = n$, this equation has $\geq n$ solutions, and since F is a field, this equation has $\leq m$ solutions, which shows that $m = n$. Thus $G = \langle y \rangle$ is cyclic. □

Applying this lemma to $\mathbb{F}_{p^m}^\times$ yields an element $a \in \mathbb{F}_{p^m}$ such that $\mathbb{F}_{p^m}^\times = \langle a \rangle$. From here we see that $\mathbb{F}_{p^m} = \mathbb{F}_{p^n}(a)$, completing the proof for the case where k is finite. Now we shall prove that $k(\alpha, \beta) = k(\gamma)$ which will complete the proof by induction. Consider $k(\alpha + c\beta)$ for $\lambda \in k$. Since k is infinite, and the number of distinct subextensions is finite, there exists $d \neq c$ so that $k(\alpha + c\beta) = k(\alpha + d\beta)$. Immediately, $\alpha + c\beta - (\alpha + d\beta) = (c - d)\beta \in k(\alpha + c\beta)$, and since $c \neq d$, $c - d$ is invertible which shows that $\beta \in k(\alpha + c\beta)$. This shows that $\alpha \in k(\alpha + c\beta)$, completing the proof in the infinite case.

Let K/k be a finite separable extension, and let $K/E/k$ be a subextension. Consider

$$\varphi : E \mapsto \Sigma_{\mathrm{id}}(E/k)$$

We show that φ is injective. Suppose that $\Sigma_{\mathrm{id}}(E'/k) = \Sigma_{\mathrm{id}}(E/k)$, but $E \neq E'$. Suppose that $E \neq E'$, and take (WLOG) $\alpha \in E \setminus E'$. Producing a $\sigma \in \Sigma_{\mathrm{id}}(E'/k) \setminus \Sigma_{\mathrm{id}}(E/k)$ will complete the proof. Let $p(x) = \mathrm{Irr}_{E'}(\alpha)$, and we have that $\deg p \geq 2$. The key use of separability is the following: since E' is a separable extension, and since $\deg p \geq 2$, $p(x)$ has at least 1 other root $\beta \neq \alpha$. Now define

$$\begin{aligned} \sigma : E(\alpha) &\to \overline{k} \\ E &= E \\ \alpha &\mapsto \beta \end{aligned}$$

Extending this to a homomorphism $K \to \overline{k}$ yields a contradiction, since every $\sigma \in \Sigma_{\mathrm{id}}(E/k)$ fixes α. Since every $\varphi(E) \subset \Sigma_{\mathrm{id}}(K/k)$, and since there are only finitely many subsets of $\sigma_{id}(K/k)$, this shows that separable extensions have only finitely many subextensions, completing the proof. $\square$

We now discuss a counterexample to the primitive element theorem for inseparable extensions. let k be a field of characteristic p (by necessity) and let α, β be two algebraically independent elements over k (i.e., if $p(x, y) \in k[x, y]$) is nonzero then $p(\alpha, \beta) \neq 0$). We first show that $|k(\alpha, \beta) : k(\alpha^p, \beta^p)| = p^2$. We start by showing that $x^p - \alpha^p$ is irreducible over $k(\alpha^p, \beta^p)$. We recall that the minimal polynomial of α over $k(\alpha^p, \beta^p)$ must now divide this polynomial, so suppose it was $(x - \alpha)^i$ for some $1 \leq i < p$. Then the coefficient of x^{i-1} is $\binom{i}{i-1}(-1)^{i-1}\alpha^1 = (-1)^{i-1} i\alpha$. If $p \nmid i$, then $(-1)^{i-1} i$ is invertible, so $\alpha \in k(\alpha^p, \beta^p)$. This would say that there is a polynomial $f(x, y) \in k[x, y]$ so that $f(\alpha^p, \beta^p) = \alpha$. Defining $q(x, y) = f(x^p, y^p) - x$, we see that $q(\alpha, \beta) = 0$, which shows that $q \equiv 0$ by algebraic independence. Thus the coefficient of x in $f(x^p, y^p)$ is 1, a contradiction, since powers of x can only show up divisible by p. Thus $|k(\alpha, \beta^p) : k(\alpha^p, \beta^p)| = p$ and similarly $|k(\alpha, \beta) : k(\alpha, \beta^p)| = p$, showing that $|k(\alpha, \beta) : k(\alpha^p, \beta^p)| = p^2$. Define $E = k(\alpha^p, \beta^p)$ and consider the fields $E(\alpha + c\beta)$. E is infinite, as $\{1, \alpha^p, \alpha^{2p}, \dots\}$ is linearly independent since being algebraically independent from β also implies that α is transcendental over k. We see that $(\alpha + c\beta)^p = \alpha^p + c^p\beta^p \in E$, so the minimal polynomial of $\alpha + c\beta$ over E has degree $\leq p$. If there existed $c \neq d$ so that $E(\alpha + c\beta) = E(\alpha + d\beta)$, the proof of the primitive element theorem as before would show that $E(\alpha + c\beta) = k(\alpha, \beta)$, but this would say that $p^2 = |E(\alpha + c\beta) : E| \leq p$, a contradiction. We used characteristic p in two places: first, showing that $x^p - \alpha^p$ is irreducible, and secondly to conclude an upper bound on the degree of the minimal polynomial of $\alpha + c\beta$ over E.