Lecture 12 : The Primitive Element Theorem

Objectives

(1) Factorization of polynomials over finite fields.
(2) The Primitive element theorem.
(3) Finite separable extensions have a primitive element.

Key words and phrases: Primitive element, finite separable extensions, factorization.

Example 12.1. We know that the polynomial $x^{p^n} - x$ is the product of all the degree d monic irreducible polynomials in $\mathbb{F}_p[x]$ where $d \mid n$. This is useful for constructing irreducible polynomials over $\mathbb{F}_p$. Let us factorize $x^{16}-x$ over $\mathbb{F}_2$. The irreducible quadratic polynomials are factors of $x^4-x = x(x+1)(x^2+x+1)$. Hence there is only one quadratic irreducible polynomial over $\mathbb{F}_2$. The cubic irreducible are factors of

$$x^8 - x = x(x^7 + 1) = x(x + 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1).$$

By Gauss' formula $N_2(3) = 2$. Therefore the irreducible cubics over $\mathbb{F}_2$ are $x^3 + x^2 + 1$ and $x^3 + x + 1$. By Gauss' formula, we count irreducible quartics over $\mathbb{F}_2$:

$$4N_2(4) = \sum_{d|4} \mu(4/d)2^d = \mu(4)2 + \mu(2)2^2 + \mu(1)2^4 = -4 + 16 = 12.$$

Hence $N_2(4) = 3$. These quartics are factors of $x^{16} - x$. The irreducible factors of this polynomial have degrees $1, 2$ and 4. Therefore the irreducible quartics are factors of

$$\frac{x^{16} - x}{x(x + 1)(x^2 + x + 1)} = (x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1).$$

We end this section by an interesting application of finite fields.

Proposition 12.2. *The polynomial $x^4 + 1$ is irreducible in $\mathbb{Z}[x]$ but it is reducible over $\mathbb{F}_p$ for every p.*

Proof. Let $f(x) = x^4 + 1$. Then $f(x+1)$ is irreducible over $\mathbb{Z}$ by Eisenstein's criterion. For $p = 2$, we have $x^4 + 1 = (x + 1)^4$. Now let p be odd. Then $8 \mid p^2 - 1$. Hence

$$x^4 + 1 \mid x^8 - 1 \mid x^{p^2-1} - 1 \mid x^{p^2} - x.$$

The splitting field of $x^{p^2} - x$ over $\mathbb{F}_p$ is the finite field $F = \mathbb{F}_{p^2}$. Hence $[F : \mathbb{F}_p] = 2$. Therefore the roots of $x^4 + 1$ in F have degree 1 or 2. Therefore $x^4 + 1$ cannot have a cubic or quartic irreducible factor over $\mathbb{F}_p$. Hence it is reducible over $\mathbb{F}_p$ for each prime p.

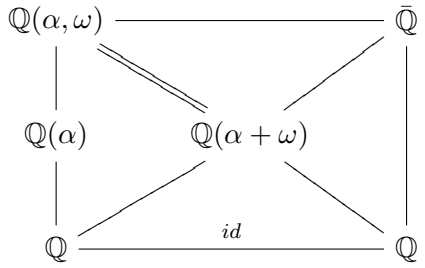
□

The Primitive Element Theorem

Since $\mathbb{F}_{q^n}^\times$ is a cyclic group, $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$ where α is a generator of $\mathbb{F}_{q^n}^\times$. We say that α is primitive element of the field extension $\mathbb{F}_q \subset \mathbb{F}_{q^n}$. In this section we discuss existence of primitive elements in finite algebraic field extensions. We will show that in a finite separable extension, primitive elements always exist.

Definition 12.3. *Let E/F be a field extension. An element $\alpha \in E$ is called* **a primitive element** *of E over F if $E = F(\alpha)$.*

Example 12.4. (1) Let $f(x) = x^3 - 2$, $\alpha = \sqrt[3]{2}$ and $\omega = e^{2\pi i/3}$. Then $\mathbb{Q}(\alpha, \omega)$ is a splitting field of $f(x)$. Moreover $[Q(\alpha, \omega) : \mathbb{Q}] = 6$. Since $Q(\alpha) \subseteq \mathbb{R}, \alpha + \omega \notin Q(\alpha)$.



We know that the number of ways $id : \mathbb{Q} \to \bar{\mathbb{Q}}$ can be extended to an embedding $\sigma : \mathbb{Q}(\alpha + \omega) \to \bar{\mathbb{Q}}$ is $\deg \operatorname{irr}(\alpha + \omega, \mathbb{Q}) = [\mathbb{Q}(\alpha + \omega) : Q]$. Since degree $\operatorname{irr}(\omega, \mathbb{Q}(\alpha)) = 2$, $id : \mathbb{Q}(\alpha) \to \bar{\mathbb{Q}}$ can be extended in two ways: $\omega \to \omega^2$ or $\omega \to \omega$. Restriction of this embedding to $\mathbb{Q}(\alpha + \omega)$ maps

$\alpha+\omega$ to $\alpha+\omega^2$ or $\alpha+\omega$. In a similar way we can embed $\mathbb{Q}(\alpha+\omega)$ onto $Q(\alpha\omega+\omega), \mathbb{Q}(\alpha\omega+\omega^2), Q(\alpha\omega^2+\omega^2)$ and $\mathbb{Q}(\alpha\omega^2+\omega)$. Thus $[\mathbb{Q}(\alpha+\omega) : \mathbb{Q}] = 6$. So $Q(\alpha,\omega) = \mathbb{Q}(\alpha+\omega)$. Therefore $\alpha+\omega$ is a primitive element.

(2) An algebraic extension need not have a primitive element. Let field k be a field with $char(k) = p$ and let u, v be indeterminates. Let $E = k(u,v)$ and $F = k(u^p, v^p)$. Then $f(u,v)^p \in F$ for any $f(u,v) \in E$. But $[E:F] = p^2$. If $y \in E$ is a primitive element of E/F then $\deg \mathrm{irr}(y,F) = p^2$. But $y^p \in F$. This is a contradiction.

Theorem 12.5 (**The Primitive Element Theorem).** *Let E/k be a finite extension.*

(1) *There is a primitive element for E/k if and only if the number of intermediate subfields F such that $k \subset F \subset E$ is finite.*

(2) *If E/k is a finite and separable extension then it has a primitive element.*

Proof. (1) If k is a finite field then E is finite and hence $E^\times$ is a cyclic group. Thus E/k has a primitive element.

Let k be infinite and let E/k have finitely many intermediate fields. Suppose $\alpha, \beta \in E$. As c varies in k, $k(\alpha + c\beta)$ varies over finitely many intermediate subfields of E/k. Hence, there are $c_1 \neq c_2 \in k$ such that $k(\alpha + c_1\beta) = k(\alpha + c_2\beta) := L$. Thus $(c_1 - c_2)\beta \in L$. Therefore $\beta \in L$. Hence $\alpha \in L$. Thus $k(\alpha,\beta) = k(\alpha + c_1\beta)$. Proceed inductively to show that $E = k(\alpha_1, \ldots, \alpha_n) = k(\alpha_1 + c_2\alpha_2 + \cdots + \alpha_n c_n)$ for some $c_2, \ldots, c_n \in k$.

Conversely, let $E = k(\alpha)$ for some $\alpha \in E$ and $f(x) = \mathrm{irr}(\alpha, k)$. Let $k \subset F \subset E$ be a tower of fields. Set $h_F = \mathrm{irr}(\alpha, F)$. Then $h_F \mid f(x)$ as F varies over all the intermediate subfields of E/k.

Since h_F is irreducible over F, it is also irreducible over F_0, a subfield of F generated by the coefficients of $h_F(x)$ over k. Since $\deg h_F(x) = [E:F] = [E:F_0]$, it follows that $F = F_0$. Since there are finitely many divisors of $f(x)$, there can be only finitely many intermediate fields of E/k.

(2) Now let E/k be a finite separable extension. Then $E = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$. To show that E/k has a primitive element it is enough to find a primitive element when $n = 2$ and then apply induction on n. So let $E = k(\alpha,\beta)$. We look for a primitive element of the form $\alpha + c\beta$ where $c \in k$.

Let $[E : k] = n$. If $\alpha + c\beta$ generates E/k, then $\alpha + c\beta$ must have n conjugates (images of $\alpha + c\beta$ under the action of n embeddings of E into k^a). Hence there exist n k-embeddings $\sigma_1, \sigma_2, \ldots, \sigma_n : E \to \bar{k}$. which map $\alpha + c\beta$ to n distinct roots of $p(x) = \mathrm{irr}(\alpha + c\beta), k)$ in $\bar{k}$. Thus $\alpha + c\beta$ is a primitive element if and only if there exist n embeddings $\sigma_1, \ldots \sigma_n : E \to \bar{k}$ such that $\sigma_i(\alpha + c\beta) \neq \sigma_j(\alpha + c\beta)$, for all $i \neq j$, if and only if

$$\prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha)) + c(\sigma_i(\beta) - \sigma_j(\beta)) \neq 0$$

if and only if c is not a root of the polynomial

$$f(x) = \prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha)) + x(\sigma_i(\beta) - \sigma_j(\beta)).$$

Since k is infinite and $f(x)$ has finitely many roots, such a c exists. $\square$