Lecture 17A: The Primitive Element Theorem

MAT205 Abstract Algebra II

Ma, Jia-Jun

Xiamen University Malaysia

Primitive Element Theorem — Statement

Theorem (Primitive Element Theorem). Let E/F be a finite separable extension. Then there exists $\alpha \in E$ with $E = F(\alpha)$. Such α is called a *primitive element* of E over F.

Significance. Every finite Galois extension (= finite normal + separable) is generated by a single element.

Examples.

- $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.
- $\mathbb{F}_{p^n} = \mathbb{F}_p(\gamma)$ where γ generates the cyclic group $\mathbb{F}_{p^n}^{\times}$.

The proof is a classical constructive argument via polynomial GCD (Fraleigh §51.15).

Setup: Reduction and the Finite Case

Reduction by induction. E/F is finite, so $E = F(\beta_1, \ldots, \beta_n)$ for some elements. By induction on n, it suffices to show that $F(\beta, \gamma)/F$ is simple for any two elements β, γ. We then prove:

$$F(\beta, \gamma) = F(\alpha) \quad \text{for some } \alpha \in E.$$

Notation. For α algebraic over F, the *minimal polynomial* of α over F is the unique monic irreducible polynomial in $F[x]$ having α as a root; denote it m_α^F.

Setup. Let $f(x) = m_\beta^F$ and $g(x) = m_\gamma^F$, with roots

$$\beta = \beta_1, \ldots, \beta_n \quad \text{and} \quad \gamma = \gamma_1, \ldots, \gamma_m \quad \text{in } \overline{F}.$$

Separability of E/F forces all roots distinct.

Finite F case. If F is finite then E is finite, so $E^\times$ is cyclic and any generator α of $E^\times$ satisfies $E = F(\alpha)$. Done in this case — assume F infinite for the remainder.

Construction: Choosing the Coefficient c

Try $\alpha = \beta + c\gamma$ for $c \in F$ to be chosen. Then $F(\alpha) \subseteq F(\beta, \gamma)$ is automatic; for the reverse inclusion it suffices to show $\gamma \in F(\alpha)$, because then $\beta = \alpha - c\gamma \in F(\alpha)$.

Bad values of c. For $i \neq 1$ and $j \neq 1$, the equation $\beta_1 + c\gamma_1 = \beta_i + c\gamma_j$ in $\overline{F}$ rearranges to

$$c = \frac{\beta_i - \beta_1}{\gamma_1 - \gamma_j} \qquad (\gamma_1 - \gamma_j \neq 0 \text{ since } j \neq 1).$$

There are at most $(n-1)(m-1)$ such values.

Choice of c. F is infinite, so pick $c \in F$ avoiding all these bad values. Set $\alpha = \beta + c\gamma$. By construction,

$$\alpha - c\gamma_j \neq \beta_i \quad \text{for all } i \neq 1 \text{ and all } j \neq 1.$$

(For $j = 1$: $\alpha - c\gamma_1 = \alpha - c\gamma = \beta = \beta_1$ — the unique "good" identity we want.)

The Auxiliary Polynomial $h(x)$ and Its Roots

Define

$$h(x) = f(\alpha - cx) \ \in \ F(\alpha)[x].$$

Note h has coefficients in $F(\alpha)$ because $\alpha \in F(\alpha)$ and $f \in F[x] \subseteq F(\alpha)[x]$.

Roots of h among $\gamma_1, \ldots, \gamma_m$.

- $h(\gamma_1) = f(\alpha - c\gamma_1) = f(\beta_1) = 0$ — so $\gamma = \gamma_1$ is a root of h.
- For $j \neq 1$: $h(\gamma_j) = f(\alpha - c\gamma_j) \neq 0$, because $\alpha - c\gamma_j$ is not any root β_i of f (by the choice of c).

$g(x) = m_\gamma^F$ has roots $\gamma_1, \ldots, \gamma_m$ in $\overline{F}$. The previous analysis shows $\gamma = \gamma_1$ is the **unique common root** of h and g in $\overline{F}$.

GCD in $F(\alpha)[x]$, and Conclusion

Both g and h lie in $F(\alpha)[x]$. Compute their GCD by the Euclidean algorithm *in* $F(\alpha)[x]$; the result has the same roots in $\overline{F}$ as the gcd computed in any larger field (it divides both, and is divided by any common factor).

The only common root of g and h is γ, and g is separable — so $\gcd(g,h)$ is squarefree and has exactly one root, giving

$$\gcd(g,h) \;=\; x-\gamma \quad \text{in } F(\alpha)[x].$$

The coefficient $-\gamma$ lies in $F(\alpha)$, hence $\gamma \in F(\alpha)$.

Conclusion. $\gamma \in F(\alpha)$ gives $\beta = \alpha - c\gamma \in F(\alpha)$, so $F(\beta,\gamma) \subseteq F(\alpha)$. Combined with the automatic $F(\alpha) \subseteq F(\beta,\gamma)$:

$$F(\beta,\gamma) \;=\; F(\alpha). \quad \square$$

Counterexample: $\mathbb{F}_p(s,t)/\mathbb{F}_p(s^p,t^p)$

Separability is essential. Without it, finite extensions can fail to be simple.

Setup. Let p be prime, s,t independent transcendentals over $\mathbb{F}_p$. Set

$$F = \mathbb{F}_p(s^p,t^p), \qquad E = \mathbb{F}_p(s,t).$$

Both s and t satisfy purely inseparable polynomials over F: s is a root of $x^p - s^p \in F[x]$, and t is a root of $x^p - t^p \in F[x]$. So $[E:F] = p^2$.

E **has no primitive element.** For any $\alpha \in E = \mathbb{F}_p(s,t)$, write $\alpha = P(s,t)/Q(s,t)$ with $P,Q \in \mathbb{F}_p[s,t]$. In characteristic p, $(a+b)^p = a^p + b^p$, so $P(s,t)^p = P(s^p,t^p)$ and similarly for Q. Hence

$$\alpha^p = \frac{P(s,t)^p}{Q(s,t)^p} = \frac{P(s^p,t^p)}{Q(s^p,t^p)} \in F.$$

So α is a root of $x^p - \alpha^p \in F[x]$, giving $[F(\alpha):F] \le p$.

Since $[E:F] = p^2 > p$, no single α generates E over F. So E/F is finite (degree p^2) but *not simple*. □