Galois Theory

MATH 440

Steven Xia

April 12, 2023

Galois Theory studies symmetries among roots of polynomials.

— Professor (Spring 2023)

Contents

1 Field Extensions

Theorem 1.1. *If $F \to K$ and $K \to L$ are finite, then $[L : F] = [L : K][K : L]$.*

Proof. Let $\{\alpha_1, \dots, \alpha_n\}$ and $\{\beta_1, \dots, \beta_m\}$ be bases for $F \to K$ and $K \to L$ respectively. We claim $S = \{\alpha_i \beta_j\}$ is an F-basis for L. It is immediate that S spans L, so we show that S is linearly independent.

Suppose some linear combination of S is zero, then factoring out by the α_i implies the coefficients of each group of α_i must be zero, but they are all linear combinations of the β_j, hence all coefficients must be zero. $\square$

Theorem 1.2. *A field extension is finite if and only if it is algebraic and finitely generated.*

Proof. Suppose $F \to K$ is a field extension. It is trivial to show that

  (i) if $F \to K$ is not algebraic, then it is not finite, and

  (ii) if $F \to K$ is not finitely generated, then it is not finite.

Suppose $F \to K$ is algebraic and finitely generated, and let $\{\alpha_1, \dots, \alpha_n\}$ be a basis for $F \to K$. Break the extension down by $F \to F(\alpha_1) \to F(\alpha_1, \alpha_2) \to \dots \to F(\alpha_1, \dots, \alpha_n) = K$, and see that each of these intermediate extensions are finite. Theorem 1.1 asserts $F \to K$ is finite. $\square$

Corollary 1.2.1. *Every composition of algebraic field extensions is algebraic.*

Proof. Suppose $F \to K$ and $K \to L$ are algebraic. Let $\alpha \in L$ with $m_{\alpha,K} = x^n + c_{n-1}x^{n-1} + \cdots + c_0$, and construct $K' = F(c_0, \ldots, c_{n-1})$, which is algebraic and finitely generated, hence finite. But $K' \to K'(\alpha)$ is also finite, so $F \to K'(\alpha)$ is finite, therefore α is algebraic over F. $\square$

Theorem 1.3 (Kronecker)**.** *If F is a field and $f \in F[x]$ is non-constant, then there exists a finite $F \to K$ such that f has a root in K.*

Proof. Without loss of generality, we may assume f is irreducible. Define $K = F[x]/\langle f \rangle$, which is a field because $\langle f \rangle$ is maximal. See that $x + \langle f \rangle \in K$ is a root of f. $\square$

Theorem 1.4. *A field F is algebraically closed if and only if every algebraic $F \to K$ has $[K : F] = 1$.*

Proof. The "only if" is trivial, so suppose every $F \to K$ has $[K : F] = 1$. Let $f \in F[x]$, and Theorem 1.3 asserts there exists a finite $F \to K$ in which f has a root. But $[K : F] = 1$, so this root is in fact in F. $\square$

Theorem 1.5. *Every field has an algebraic closure.*

Proof. Suppose F is a field, and define S to be the set of monic and irreducible polynomials in $F[x]$. Also construct $R = F[y_f \mid f \in S]$ and $I = \langle f(y_f) \mid f \in S \rangle$.

We claim $1 \notin I$. Towards a contradiction, suppose $1 \in I$, so we can write $1 = \sum_i a_i f_i(y_{f_i})$ for $a_i \in R$ and $f_i \in S$. Repeating Theorem 1.3 for each f_i generates a field extension in which there exist α_i such that $f_i(\alpha_i) = 0$ for all i, but now we have $1 = \sum_i a_i f_i(\alpha_i) = 0$, a contradiction.

Now we know I is a proper ideal, so it is contained in some maximal ideal M. Define $F \to K = R/M$, and see that $y_i + \langle M \rangle \in K$ is a root of f_i, so we conclude that K is an algebraic closure of F. $\square$

Theorem 1.6 (Isomorphism Extension)**.** *Let F and K be fields with isomorphism $\phi : F \to K$. If $F \to E$ is algebraic, then there exists an isomorphism ψ between E and a subfield of $\overline{K}$ satisfying $\psi|_F = \phi$.*

Proof. Let S be the set of (E', σ) where E' is a field satisfying $F \subseteq E' \subseteq E$ and σ an isomorphism from E' to a subfield of $\overline{K}$ satisfying $\sigma|_F = \phi$. Define a partial order on S by $(E_1, \sigma_1) \leq (E_2, \sigma_2)$ if and only if $E_1 \subseteq E_2$ and $\sigma_2|_{E_1} = \sigma_1$. We wish to apply Zorn's Lemma to S, so we note

(i) that $(F, \phi) \in S$ implies S is non-empty, and

(ii) that every chain $(E_1, \sigma_1) \leq (E_2, \sigma_2) \leq \ldots$ in S is bounded above by (E', σ), where $E' = \bigcup_i E_i$ and σ is defined by simply using whichever σ_i is available, since they are all compatible.

Therefore, there exists a maximal element $(M, \tau) \in S$, and we want to show $M = E$. Towards a contradiction, suppose $M \subsetneq E$ and choose $\alpha \in E \setminus M$ with minimal polynomial $m_{\alpha,M} = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in M[x]$. Define $L = \tau(M)$ and $f(x) = x^n + \tau(c_{n-1})x^{n-1} + \cdots + \tau(c_0) \in L[x]$, and see that

$$M(\alpha) \to M[x]/m_{\alpha,M} \to L[x]/f(x) \to L(\beta)$$

is an isomorphism for $\beta \in \overline{L} = \overline{K}$ a root of $f(x)$. Moreover, this extends τ, a contradiction. $\square$

Theorem 1.7. *If F is a field, then all algebraic closures of F are pairwise isomorphic.*

Theorem 1.8 (Symmetric Polynomials). *Every symmetric polynomial can be written uniquely as a polynomial in the elementary symmetric polynomials.*

Theorem 1.9 (Algebra). *The set of complex numbers is algebraically closed.*