Galois Theory

MATH 440

Steven Xia

April 15, 2023

Galois Theory studies symmetries among roots of polynomials.

— Professor (Spring 2023)

Contents

1 Author's Notes

- The following are sometimes used without reference: Theorem 2.1, Theorem 4.1.
- Unless otherwise stated, assume p denotes a prime number and n denotes a natural number.

2 Field Extensions

Theorem 2.1. *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. □

Theorem 2.2. *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 2.1 asserts $F \to K$ is finite. □

Corollary 2.2.1. *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 $K' = F(c_0, \dots, c_{n-1})$, 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. □

Theorem 2.3 (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. □

Theorem 2.4. *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 2.3 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. □

Theorem 2.5. *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 2.3 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. □

Theorem 2.6 (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 $(E_1, \sigma_1) \leq (E_2, \sigma_2) \leq \dots$ 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. □

Theorem 2.7. *Let F be a field and fix some $\overline{F}$. Every algebraic closure of F is isomorphic to $\overline{F}$.*

Proof. Suppose K is an algebraic closure of F. By Theorem 2.6, there is an isomorphism between K and a subfield E of $\overline{F}$. But E is algebraically closed, so $[\overline{F} : E] = 1$, and therefore $E = \overline{F}$. □

Theorem 2.8 (Symmetric Polynomials)**.** *Every symmetric polynomial can be written uniquely as a polynomial in the elementary symmetric polynomials.*

Theorem 2.9 (Algebra)**.** *The set of complex numbers is algebraically closed.*

3 Normal Extensions

Theorem 3.1. *If $F \to K$ is algebraic, then it is equivalent to say*

(i) that K is a splitting field,

(ii) that every $\phi : K \to \overline{F}$ fixing F induces an isomorphism on K, or

(iii) that the minimal polynomial of every $\alpha \in K$ splits in $K[x]$.

Proof. We first show $(i) \implies (ii)$. Suppose K is a splitting field, and that $\phi : K \to \overline{F}$ fixes F. Let $\alpha \in K$, and see that $\phi(\alpha)$ must still be a root of $m_{\alpha,F}$, so therefore $\phi(\alpha) \in K$, and $\phi(K) \subseteq K$. On the other hand, since ϕ defines an injective endomap on the roots of $m_{\alpha,F}$, of which there are finitely many, it must in fact permute these roots. In particular, this means ϕ is bijective over K, so then $\phi(K) = K$.

Now we show $(ii) \implies (iii)$. Let $\alpha \in K$, take $\beta \in \overline{F}$ a root of $m_{\alpha,F}$, and see that $\psi : F(\alpha) \to F(\beta)$ generated by $\psi(\alpha) = \beta$ is an isomorphism. By Theorem 2.6, there exists $\phi : K \to \overline{F}$ satisfying $\phi|_{F(\alpha)} = \psi$. But this means ϕ fixes F, so it induces an automorphism on K. In particular, this means $\phi(\alpha) = \beta \in K$, so every root of $m_{\alpha,F}$ is in K, which implies $m_{\alpha,F}$ splits in $K[x]$.

Now for $(iii) \implies (i)$, see that K is the splitting field of the minimal polynomials of every $\alpha \in K$. □

4 Seperable Extensions

Lemma 4.1. *Suppose $\phi : F \to F'$ is an isomorphism with $\overline{F} = \overline{F'}$, and $F \to K$ is algebraic. Then there is a bijection between $\{\psi : K \to \overline{F} \mid \psi|_F = \iota\}$ and $\{\chi : K \to \overline{F} \mid \psi|_F = \phi\}$.*

Proof. By Theorem 2.6, there is an isomorphism σ between K and a subfield K' of $\overline{F}$ satisfying $\sigma|_F = \phi$. See that there is a bijection from $\{\psi : K \to \overline{F} \mid \psi|_F = \iota\}$ to $\{\tau : K' \to \overline{F} \mid \tau|_{F'} = \iota\}$ by applying σ to K. □

Theorem 4.1. *If $F \to K$ and $K \to L$ are finite and algebraic, then $[L : F]_s = [L : K]_s[K : F]_s$.*

Proof. Define $S = \{\phi : L \to \overline{F} \mid \phi|_F = \iota\}$ and $T = \{\psi : K \to \overline{F} \mid \psi|_F = \iota\}$, and see that

$$[L : F]_s = |S| = \sum_{\psi \in T} \#\{\chi : L \to \overline{F} \mid \chi|_K = \psi\} = \sum_{\psi \in T} [L : K]_s = [K : F]_s[L : K]_s.$$

□

Theorem 4.2. *If $F \to K$ is finite and algebraic, then $[K : F]_s \leq [K : F]$.*

Proof. From Theorem 2.1 and Theorem 4.1, we may assume $K = F(\alpha)$. Since every $\phi : K \to \overline{F}$ contributing to $[K : F]_s$ is completely determined by its mapping of α, the number of such embeddings is the number of distinct roots of $m_{\alpha,F}$. But this is at most the degree of $m_{\alpha,F}$, which is $[K : F]$. □

Theorem 4.3. *If $F \to K$ is finite, then $F \to K$ is separable if and only if every $\alpha \in K$ is separable.*

Proof. Suppose $F \to K$ is separable, let $\alpha \in K$, and Theorem 4.2 asserts that

$$[K : F]_s = [K : F(\alpha)]_s[F(\alpha) : F]_s \leq [K : F(\alpha)][F(\alpha) : F] = [K : F].$$

Separability implies $[K : F]_s = [K : F]$, so $m_{\alpha,F}$ has $[F(\alpha) : F]_s = [F(\alpha) : F]$ distinct roots.

Now suppose every $\alpha \in K$ is separable. By Theorem 2.2, we know $F \to K$ is algebraic and finitely generated. Since $[F(\alpha) : F]_s = [F(\alpha) : F]$ for every $\alpha \in K$, we can show $F \to K$ is separable by induction on the number of generators of K, using Theorem 2.1 and Theorem 4.1. □

Theorem 4.4 (Primitive Element)**.** *If $F \to K$ is finite and separable, then $K = F(\alpha)$ for some $\alpha \in K$.*

Proof. For now, we will only prove this for infinite fields F. The case for finite fields follows from the multiplicative group of every finite field being cyclic.

From Theorem 2.2, it suffices to show separable $F \to F(\alpha, \beta)$ implies that there exists a primitive element. Fix $c \in F$ and let $\gamma = \alpha + c\beta$. To show γ is primitive, it suffices to show $\beta \in F(\gamma)$. Instead, we will show that $\beta \notin F(\gamma)$ implies c must equal an expression given in terms of roots of $m_{\alpha,F}$ and $m_{\beta,F}$. Since there are only a finite number of combinations of these roots, there then must exist c for which γ is primitive.

Suppose $\beta \notin F(\gamma)$, and see that β is a root of both $m_{\beta,F}$ and $m_{\alpha,F}(\gamma - cx)$ in $F(\gamma)[x]$, so $m_{\beta,F(\gamma)}$ divides both $m_{\beta,F}$ and $m_{\alpha,F}(\gamma - cx)$. Since $\beta \notin F(\gamma)$ implies $\deg(m_{\beta,F(\gamma)}) \geq 2$, separability ensures we can choose a root β' of $m_{\beta,F(\gamma)}$ satisfying $\beta' \neq \beta$. This gives that $\alpha' = \gamma - c\beta' \in \overline{F}$ is a root of $m_{\alpha,F}$, but we can now plug in the original definition of γ to see that

$$\alpha' = \gamma - c\beta' \iff \alpha' = (\alpha + c\beta) - c\beta' \iff c = \frac{\alpha' - \alpha}{\beta - \beta'}.$$

□

5 Galois Correspondece

Definition 5.1. An algebraic extension $F \to K$ is *Galois* if it is normal and algebraic.

Definition 5.2. Let $F \subseteq K$ be a field extension with $H \leq \mathrm{Gal}(K/F)$. The *fixed field* of K under H is

$$K^H := \{\alpha \in K \mid \forall \sigma \in H, \sigma(\alpha) = \alpha\}.$$

Theorem 5.1 (Galois Theory)**.** *If $F \subseteq K$ is finite Galois, there is a bijection between subgroups of $G =$ $\mathrm{Gal}(K/F)$ and subfields of K containing F where $H \leq G \mapsto K^H$ and $L \subseteq K \mapsto \mathrm{Gal}(K/L)$.*

Proof. Suppose $F \subseteq K' \subseteq K$ and $G = \mathrm{Gal}(K/K')$. We have $K' \subseteq K^G$ by definition, so we show $K^G \subseteq K'$. Let $\alpha \in K \setminus K'$, and separability ensures there exists a root β of $m_{\alpha,K'}$ satisfying $\beta \neq \alpha$. Since there exists an isomorphism $\sigma : K'(\alpha) \to K'(\beta)$ where $\sigma|_{K'} = \iota$ and $\sigma(\alpha) = \beta$, we can use Theorem 2.6 to find an isomorphism τ of K where $\tau|_{K'} = \sigma$. But this $\tau \in G$ doesn't fix α, so $\alpha \notin K^G$ and $K^G \subseteq K'$.

Now suppose $H \leq G = \mathrm{Gal}(K/F)$. It is immediate that $H \subseteq \mathrm{Gal}(K/K^H)$, so we show $|\mathrm{Gal}(K/K^H)| \leq |H|$. By Theorem 4.4, choose $\alpha \in K$ such that $F(\alpha) = K$, define $S := \mathrm{Orb}_H(\alpha)$, and also $p(x) := \prod_{a \in S}(x - a) \in K[x]$. We note that the coefficients of $p(x)$ are fixed by H, so in fact $p(x) \in K^H[x]$. But now we know that m_{α,K^H} divides p, which gives $|\mathrm{Gal}(K/K^H)| = [K : K^H] = \deg(m_{\alpha,K^H}) \leq \deg(p) = |\mathrm{Orb}(H)| = |H|$. $\square$

Theorem 5.2. *If $F \subseteq K$ is finite Galois, and $H \leq \mathrm{Gal}(K/F) = G$, then H is a normal subgroup if and only if $F \subseteq K^H$ is normal. It holds that $\mathrm{Gal}(K^H/F) \cong G/H$.*

Theorem 5.3 (Base Change)**.** *If $F \subseteq K, L \subseteq \overline{F}$ are fields, then $\mathrm{Gal}(KL/L) \cong \mathrm{Gal}(L/K \cap L)$.*

6 Solvable Extensions

Definition 6.1. A field extension $F \to K$ is *principal radical* if there exists $\alpha \in K$ and $n \in \mathbb{N}$ which satisfy $F(\alpha) = K$ and $\alpha^n \in F$.

Definition 6.2. A field extension $F \to K$ is *radical* if it is the composition of finitely many principal radical field extensions.

Definition 6.3. A field extension $F \to K$ is *solvable* if there exists a field K' which satisfies $K \subseteq K'$ and that $F \to K'$ is radical.

Lemma 6.1. *If $F \to K$ is Galois with $\mathrm{Gal}(K/F) \cong \mathbb{Z}_p$ and F has all p-th roots of unity, then $F \to K$ is a principal radical extension.*

Theorem 6.1. *If $F \to K$ is finite Galois and $\mathrm{char}(F) = 0$, then $F \to K$ is solvable if and only if $\mathrm{Gal}(K/F)$ is solvable.*

7 Constructibility

Theorem 7.1. *Some $\alpha \in \mathbb{R}$ is constructible if and only if there exists a tower $\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_n \subseteq \mathbb{R}$ which satisfies $\alpha \in F_n$ and $[F_i : F_{i-1}]$ for all $i \in [n]$.*

Remark 7.1. The complex constructible numbers are written $a+bi$ where a and b are constructible. We note that $a+bi \in \mathbb{C}$ is constructible if and only if a and b are constructible.

Theorem 7.2. *Some $\alpha \in \mathbb{C}$ is constructible if and only if the splitting field of $m_{\alpha,\mathbb{Q}}$ has degree a power of 2.*

Theorem 7.3. *If α is a primitive n-th root of unity, then $\Phi_n = m_{\alpha,\mathbb{Q}} \in \mathbb{Q}$.*