Galois Theory

MATH 440

Steven Xia

February 5, 2023

Galois Theory is the study of symmetries among roots of polynomials.

— Professor (Spring 2023)

Contents

1 Exploration of Fields

Definition 1.1. The **degree** of K over L is written $[K : L]$.

Proposition 1.1. *Let $F \subseteq K$ and $K \subseteq L$ be field extensions. Then,* $[L : F] = [L : K][K : F]$.

Proof. We may assume $[L : K]$ and $[K : F]$ are finite. Then, L has K-basis $\{a_1, \ldots, a_k\}$ and K has F-basis $\{b_1, \ldots, b_f\}$. We can show $\{a_i b_j\}$ is an F-basis of L. $\square$

Definition 1.2. A field extension $F \subseteq K$ is **finite** if the degree of K over F is finite.

Definition 1.3. A field extension $F \subseteq K$ is **finitely generated** if there exists a finite set S such that $F(S) = K$.

Remark 1.1. A $F \subseteq K$ is finitely generated if it is finite.

Definition 1.4. For $F \subseteq K$, some $\alpha \in K$ is **algebraic** over F if there exists a non-constant $f \in F[x]$ such that $f(\alpha) = 0$.

Definition 1.5. The minimal polynoimial of α over F is written $m_{\alpha,F}(\alpha) = 0$. Then, the degree of α over F is $\deg(m_{\alpha,F})$.

Definition 1.6. A $F \subseteq K$ is an algebraic field extension if every $\alpha \in K$ is algebraic.

Theorem 1.1. *A $F \subseteq K$ is finite if and only if it is finitely generated and algebraic.*

Proof. Suppose $F \subseteq K$ is finite. We will show K is algebraic over F (finitely generated follows from Proposition 1.1). Let $\alpha \in K$ be nonzero and see that $\alpha^0, \ldots, \alpha^m \in K$ is linearly dependent if $m \geq \deg(m_{\alpha,F}) = [K : F]$.

Now, suppose $K = F(\alpha_1, \ldots, \alpha_m)$ is algebraic and define $K_i = K_{i-1}(\alpha_i)$ with $K_0 = F$. By an implicit induction on i, we see that $K_m = K$ is finite. $\square$

Corollary 1.1.1. *Finite composition of algebraic and finitely generated field extensions are also finite.*

Definition 1.7. A field F is **algebraically closed** if every non-constant $f \in F[x]$ has a root in F.

Remark 1.2. If F is algebraically closed, every $f \in F[x]$ can be written as a product of linear factors.

Proposition 1.2. *A field F is algebraically closed if and only if every field extension K of F satisfies $[K : F] = 1$.*

Proof. Assume F is algebraically closed. Then, the minimal polynomial of every element over F is linear, so any field extension over F is of degree one.

Now suppose every algebraic extension is of degree one. Consider some irreducible factor f of a polynomial in $F[x]$ and the algebraic extension $F \to F[x]/\langle f \rangle$. Since the extension is of degree one, the degree of f is also one. $\square$

Theorem 1.2 (Kronecker)**.** *Let F be a field and $f \in F[x]$ be non-constant. There exists a finite extension $F \subseteq K$ such that f has a root in K.*

Definition 1.8. An **algebraic closure** of a field F is an algebraic extension $F \subseteq K$ such that K is algebraically closed.

Theorem 1.3. *Every field F has an algebraic closure.*

Proof. Define S as the set of monic and irreducible polynomials in $F[x]$, $R = F[y_f \mid f \in S]$, and $I = \langle f(y_f) \mid f \in S \rangle$.

We claim that I is a proper ideal, that is, $1 \notin I$. Towards a contradiction, suppose $1 \in I$. Then, we can write $1 = \sum a_i f_i(y_{f_i})$ for $f_i \in S$ and $a_i \in R$. However, repeating Kronecker's Theorem for each f_i generates a field extension for which there exist α_i such that $f_i(\alpha_i) = 0$ for all i, so we can plug these values into the sum to give $1 = 0$, a contradiction.

Since every proper ideal is contained in a maximal ideal, there exists some $M \subseteq R$ such that $I \subseteq M$. Then, we define $F \subseteq K$ where $K = R/M$ as an algebraic field extension of F generated by the y_f. Since K contains a root to every irreducible polynomial, we conclude that it is an algebraic closure of F. $\square$

Theorem 1.4. *All algebraic closures of a field are isomorphic.*

Definition 1.9. A **symmetric polynomial** $p \in F[x_1, \dots, x_n]$ satisfies $p(x_1, \dots, x_n) = p(x_{\sigma(1)}, \dots, x_{\sigma(n)})$ for all $\sigma \in S_n$.

Definition 1.10. The elementary symmetric polynomials in n variables are written e_i for $1 \leq i \leq n$ and are the sum of the ith degree monomials in the expansion of $\prod_{j=1}^{n}(1 + x_j)$.

Theorem 1.5 (Symmetric Polynomials)**.** *All symmetric polynomials can be uniquely written as a polynomial in the elementary symmetric polynomials.*

Definition 1.11. The descriminant of a polynomial f with roots $\alpha_1, \dots, \alpha_n$ is $\Delta(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2$.

Remark 1.3. The **discriminant** of f is a symmetric polynomial in its roots, and the elementary symmetric polynomials are (up to negation) the coefficients of f.

Theorem 1.6 (Algebra)**.** *Every non-constant polynomial with complex coefficients has at least one complex root.*

2 Groups and Actions

Definition 2.1. The **automorphism group** of K, denoted $Aut(K)$, is the set of automorphisms of K.

Definition 2.2. The **Galois group** of a field extension $F \subseteq K$, denoted $Gal(K/F)$, is the set of automorphisms of K such that F is fixed pointwise.

Definition 2.3. A **left action** of a group G on a set X is a map $G \times X \to X$ written $(g, x) \mapsto g.x$ such that $e \in G$ satisfies $e.x = x$ for all x and $g.(h.x) = (gh).x$ for all $g, h \in G$.

Definition 2.4. The **standard left action** of $H \leq G$ on G is the left action defined $(h, g) \mapsto hg$.

Definition 2.5. The **conjugation action** of $H \leq G$ on G is the left action defined $(h, g) \mapsto hgh^{-1}$.

Definition 2.6. The **orbit** of $x \in X$ under group action G is defined $G.x = \{g.x : g \in G\}$.

Theorem 2.1. *The orbits under an action form a partition.*

Definition 2.7. The **stabilizers** of $x \in X$ under group action G is defined $G_x = \{g \in G : g.x = x\}$.

Theorem 2.2. *Every stabilizer forms a group.*

Definition 2.8. For groups $H \leq G$ and $g \in G$, a **left coset** of H in G is defined $gH = \{gh : h \in H\}$. We write G/H to denote the set of left cosets of H in G.

Definition 2.9. The **index** of H in G is the number of left cosets of H in G. We write $[G : H]$ to denote this value.

Theorem 2.3 (Orbit-stabilizer)**.** *Let $H \leq G$ be groups. For all $x \in G$, there is a bijection $G.x \to G/G_x$.*

Proof. Define $\phi : G \to G.x$ where $\phi(g) = g.x$, a surjective map. We see $\phi(g) = \phi(h) \iff g.x = h.x \iff g^{-1}h \in G_x \iff g^{-1}hG_x = G_x \iff hG_x = gG_x$, so $gG_x \mapsto g.x$ is bijective. $\square$

Theorem 2.4 (Lagrange)**.** *For $H \leq G$, $|G| = [G : H]|H|$.*

Definition 2.10. Orbits under a conjugation action $H \leq G$ are called **conjugacy classes** under conjugation by H.

Definition 2.11. The **center** of a group G is defined $Z(G) = \{z \in G : \forall g \in G, gz = zg\}$.

Theorem 2.5 (Class Equation)**.** *For a finite group G, $|G| = Z(G) + \sum_{H \in O}[G : H]$ for O the set of all conjugacy classes disjoint from the center of G.*

Definition 2.12. A **normal subgroup** $H \leq G$ is one which satisfies $gHg^{-1} = H$ for all $g \in G$. We then denote $H \trianglelefteq G$.

Remark 2.1. A subgroup $H \leq G$ is normal if and only if $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$.

Theorem 2.6. *The quotient by a normal subgroup is a group.*

Theorem 2.7. *The normal subgroups of G are exactly those which arise as kernels of group homomorphisms from G.*

Theorem 2.8 (Group Isomorphism)**.** *For $\phi : G \to H$ a surjective group homomorphism, $G/\ker\phi$ and H are isomorphic.*

Remark 2.2. A group action $\rho : G \times X \to X$ can be viewed as a group homomorphism $\phi : G \to S_X$, where $g \in G$ is mapped to the permutation of X that its associated action does.

3 Back to Fields