Galois Theory

Guo Haoyang

March 2025

Contents

1 Basic definitions

1.1 Assigning field extensions a group

Definition 1.1: Automorphism group

Let K/F be a field extension.

$$\mathrm{Aut}(K/F) := \{\sigma : K \to K \big| \, \sigma|_F = \mathrm{id}_F\}$$

Theorem 1.1: Automorphism group permutes the roots

Let $m_{\alpha,F}(x)$ be the minimal polynomial of α. $\forall \sigma \in \mathrm{Gal}(K/F)$, $m_{\alpha,F}(\sigma\alpha) = 0$.
In other words, $\mathrm{Aut}(K/F)$ permutes the roots of $m_{\alpha,F}$.

This theorem gives us a tool to compute the automorphism groups concretely.
Example (1) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$
(2) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$,
(3) $\mathbb{R}/\mathbb{Q}$

1.2 Assigning groups a field

Consider a subgroup $H \leq \mathrm{Aut}(K) = \mathrm{Aut}(K/\{0\})$. Let F be the collection of elements of K fixed by H, i.e.

$$F = \{k \in K : \forall \sigma \in H, \sigma(k) = k\}$$

Such a collection is called fixed field. Then, we would like to say:
(1) This collection F is indeed a field.
(2) We will see no matter H is the subgroup of $\mathrm{Aut}(K)$ (it could be just a set), F is a field. But only when H is the subgroup of $\mathrm{Aut}(K)$. F is called a fixed field.

Definition 1.2: Fixed field

Theorem 1.2: Fixed field is a field

1.3 Galois extension

Definition 1.3: Galois extension

Theorem 1.3: Characterisation theorem for Galois extension

Let K/F be a field extension. K/F is Galois $\Leftrightarrow$ K is the splitting field of **some** separable polynomial over F

Upshot: Criteria for an extension to be Galois:
(1) $|\mathrm{Aut}(K/F)| = [K : F]$
(2) K/F is a ?? finite extension and $f \in F[x]$ is a separable polynomial, then K is the splitting field of f.
(3) definition

1.3.1 Calculating some Galois groups

(1)
(2) Finite extension of a finite field $\mathbb{F}_{p^n}/\mathbb{F}_p$: This extension is separable since $f(x) = x^{p^n} - x$ is separable and $\mathbb{F}_{p^n}$

is the splitting field of f over $\mathbb{F}_p$.

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \langle \sigma_p \rangle \cong \mathbb{Z}/n\mathbb{Z}$$

(3) Finite extension of $\mathbb{K}/\mathbb{F}_p$: Let $\mathbb{K}$ be a finite extension of the finite field $\mathbb{F}_q$, $q = p^a$. Then, $\mathbb{K}/\mathbb{F}_q$ is a Galois extension and $\mathrm{Gal}(\mathbb{K}/\mathbb{F}_q)$ is a cyclic group of order $[\mathbb{K} : \mathbb{F}_q]$ generated by the Frobenius element ${}_q : \mathbb{K} \to \mathbb{K}, x \mapsto x^q$, i.e. $\mathrm{Gal}(\mathbb{K}/\mathbb{F}_q) = \langle {}_q \rangle$.
Proof: First, this extension is Galois.
Then, the Frobenius element belongs to the Galois group $\mathrm{Gal}(\mathbb{K}/\mathbb{F}_q)$. • ${}_q$ is an automorphism. • ${}_q$ fixes every element in $\mathbb{F}_q$. Since every element in $\mathbb{F}_q^\times$ has order $q-1$. So, $\forall x \in \mathbb{F}_q$, ${}_q(x) = x^q = x$. Thus, ${}_q \in \mathrm{Gal}(\mathbb{K}/\mathbb{F}_q)$.
There is nothing more than $\langle {}_q \rangle$ in $\mathrm{Gal}(\mathbb{K}/\mathbb{F}_q)$. ?? gives that $\mathbb{K}^\times$ is cyclic. So, $\exists y \in \mathbb{K}^\times$ with order q^n, i.e. $\forall 1 \le l \le q^n - 1$, $y^l \ne y$. Apply ${}_q$ k times: ${}_q^k(y) = y^{q^k}$. $\forall 1 \le k \le n-1$, ${}_q^k(y) \ne 1$. But for n, ${}_q^n(y) = y$. This shows that ${}_q$ generates a cyclic subgroup of order n in $\mathrm{Gal}(\mathbb{K}/\mathbb{F}_q)$. But, $|\mathrm{Gal}(\mathbb{K}/\mathbb{F}_q)| = [\mathbb{K} : \mathbb{F}_q] = n$. So, the only possibility is $\mathrm{Gal}(\mathbb{K}/\mathbb{F}_q) = \langle {}_q \rangle$. $\square$
(4) Finite cyclotomic extension over $\mathbb{Q}$

2 Fundamental theorem of Galois theory

Theorem 2.1: Artin's theorem[Conrad]

Let E be a field and $H \le \mathrm{Aut}(E)$ be a finite subgroup. $[E : E^H] < +\infty$. Then E/E^H is a Galois extension with $\mathrm{Gal}(E/E^H) = H$.
Moreover, this also implies that $[E : E^H] = |\mathrm{Gal}(E/E^H)| = |H|$.

Proof: • First we show that the field extension E/E^H is separable and every element $\alpha \in E$ has bounded degree. Suppose that $\{\sigma_1(\alpha), \dots, \sigma_k(\alpha)\}$ are distinct elements of $\{\sigma(\alpha) : \sigma \in H\}$ into . Consider the polynomial $h_\alpha(x) = \prod_{i=1}^k (x - \sigma_i(\alpha))$. Definitely, α is a root of $h_\alpha(x)$ and $h_\alpha(x) \in E^H[x]$ state the reason. Because every $\alpha \in E$ is algebraic and separable over E^H. So, E/E^H is an algebraic extension, and each α has a degree $\le |H|$ over E^H.
why extension finite
Hence, by the primitive element theorem, $\exists \alpha \in E$, such that $E = E^H(\alpha)$. So there is an element β, such that $[E^H(\beta) : E^H]$ is maximal.
• Next, we claim that $E = E^H(\beta)$ [1]: $\forall \gamma \in E$, $E^H(\beta) \subseteq E^H(\beta, \gamma) \subseteq E$. Since $E^H(\beta,\gamma)/E^H(\beta)$ is a finite separable extension, the primitive element theorem predicts again that $\exists \delta \in E$, $E^H(\beta,\gamma) = E^H(\delta)$. Then, $[E^H(\beta) : E^H] \le [E^H(\beta,\gamma) : E^H] = [E^H(\gamma) : E^H]$. But as we assumed, $[E^H(\beta) : E^H]$ is the largest, so $[E^H(\beta) : E^H] = [E^H(\gamma) : E^H]$, meaning $E^H(\beta) = E^H(\beta,\gamma)$ and then $\gamma \in E^H(\beta)$. Since this is for arbitrary $\gamma \in E$, this implies that $E \subseteq E^H(\beta)$. Hence, $E = E^H(\beta)$.
• Then, we are going to use the fact that $[E : E^H] < \infty$

$$[E : E^H] = [E^H(\alpha) : E^H] = \deg m_{\alpha, E^H}(x) \le \deg h_\alpha(x) \le |H|$$

$h_\alpha(x)$ splits over E splitting fields?, so E/E^H is a Galois extension. $\forall \sigma \in H$, $\sigma|_{E^H} = \mathrm{id}_{E^H}$, hence $H \le \mathrm{Gal}(E/E^H)$. So, we get the equality $|H| = |\mathrm{Gal}(E/E^H)|$ and then $H = \mathrm{Gal}(E/E^H)$. $\square$

[1]This β may not be agree with the α making $E^H(\alpha) = E$, so we cannot directly say that $E^H(\beta) = E$

Theorem 2.2: Fundamental theorem of Galois theory

Let K/F be a Galois extension. There is a bijection:

$$\{\text{intermediate field } E \text{ between } K \text{ and } F : K/E/F\} \longleftrightarrow \{\text{intermediate group } H : \{1\} \leq H \leq \mathrm{Gal}(K/F)\}$$
$$f: \quad E \mapsto \mathrm{Gal}(K/E)$$
$$g: \; K^H \leftarrow\!\shortmid H$$

so that $K^{\mathrm{Gal}(K/E)} = (g \circ f)(E) = E$ and $\mathrm{Gal}(K/K^H) = (f \circ g)(H) = H$. f, g are inverse to each other. Moreover, let intermediate fields E_1, E_2 correspond to two intermediate groups H_1, H_2, respectively. This bijection has the following properties:
(1) (inclusion-reversing) $E_1 \subseteq E_2 \Leftrightarrow H_2 \leq H_1$.
(2) $[E_2 : E_1] = [H_1 : H_2]$
(3) E_2/E_1 is a Galois extension $\Leftrightarrow H_2 \trianglelefteq H_1$. In this case, $\mathrm{Gal}(E_2/E_1) \cong H_1/H_2$
(4) $E_1 \cap E_2$ corresponds to the group $\langle H_1, H_2 \rangle$. $H_1 \cap H_2$ corresponds to the composite field E_1E_2

Remark The last properties is illustrated as:

$$\begin{tikzcd}
& E_1E_2 \arrow[dl, dash] \arrow[dr, dash] \arrow[rrr, leftrightarrow] & & & H_1 \cap H_2 \arrow[dl, dash] \arrow[dr, dash] & \\
E_1 \arrow[rr, dash] \arrow[dr, dash] & & E_2 \arrow[dl, dash] & H_1 \arrow[rr, dash] \arrow[dr, dash] & & H_2 \arrow[dl, dash] \\
& E_1 \cap E_2 \arrow[rrr, leftrightarrow] & & & \langle H_1, H_2 \rangle &
\end{tikzcd}$$

The lattice of subfields and the lattice of subgroups are dual–they are upside down to each other.
Proof: • This map is well-defined. Given $H \leq G$, we have the unique fixed field K^H. $\forall \sigma \in H \subseteq \mathrm{Gal}(K/F)$, σ fixes all elements in F. Hence, $F \subseteq K^H$. Hence, g is injective.
For the other side, since K/F is Galois, so theorem 1.3 gives the existence of a polynomial $f(x) \in F[x]$ such that K is the splitting field of f which is separable. $f(x)$ can also be viewed as $\in E[x]$. By theorem 1.3 again, K/E is Galois. So, f is well-defined. $\square$
Example (1) For finite fields $\mathbb{F}_p$, $\mathbb{F}_{p^n}$. Every subfield of $\mathbb{F}_{p^n}$ is $\mathbb{F}_{p^d}$ with $d|n$.
(2) For cyclotomic field extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, every intermediate field of this extension is $\mathbb{Q}(\zeta_m)$ with $m|n$.

2.1 Linear algebra under Galois theory

[DF03]

Definition 2.1: Norm of Galois extensions

Let $L/K/F$ be finite extensions with $\alpha \in K$, K/F finite and L/F Galois. The **norm** of α from K to F, denoted $\mathrm{Nm}_{K/F}(\alpha)$,

$$\mathrm{Nm}_{K/F}(\alpha) := \prod_{\sigma \in \{K \hookrightarrow \overline{F}\}} \sigma(\alpha)$$

In particular, if K/F is Galois, $\mathrm{Nm}_{K/F}(\alpha) := \prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha)$.

Remark Notice that this definition works broadly. Even for the extension K/F that is not Galois.

Theorem 2.3: Properties of norm

Let $L/K/F$ be finite extensions with $\alpha \in K$, K/F finite, L/F Galois.
(1) $\mathrm{Nm}_{K/F} : K \to F$ is a multiplicative map.
(2) Let $K = F(\sqrt{D})$ be a quadratic extension. Then, $\mathrm{Nm}_{K/F}(a + b\sqrt{D}) = a^2 - Db^2$.
(3) Let $m_\alpha(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 \in F[x]$ be the minimal polynomial for $\alpha \in K$ over F. Let $n := [K : F]$ and $d|n$, then $\mathrm{Nm}_{K/F}(\alpha) = (-1)^n a_0^{n/d}$.

Proof: • First, $\mathrm{Nm}_{K/F}(\alpha) \in F$, by showing it is fixed by any $\tau \in \mathrm{Gal}(K/F)$.
Suppose that $m_\alpha(x)$ has roots $\alpha_1, \alpha_2, \ldots, \alpha_n$, then $m_\alpha(x) = \prod_{i=1}^{d}(x - \alpha_i)$. Expand it and compare the coefficients with the form $x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$. $(-1)^d \alpha_0 \alpha_1 \cdots \alpha_d = a_0$. Since Galois group permutes the roots of $m_\alpha(x)$, there are d distinct elements of $m_\alpha(x)$. □

Definition 2.2: Trace of Galois extensions

Let $L/K/F$ be finite extensions with $\alpha \in K$, K/F finite and L/F Galois. The **trace** of α from K to F, denoted $\mathrm{Tr}_{K/F}(\alpha)$,

$$\mathrm{Tr}_{K/F}(\alpha) := \sum_{\sigma \in \{K \hookrightarrow \overline{F}\}} \sigma(\alpha)$$

Theorem 2.4: Properties of trace

Let $L/K/F$ be finite extensions with $\alpha \in K$, K/F finite, L/F Galois.
(1) $\mathrm{Tr}_{K/F} : K \to F$ is an additive map.
(2) Let $K = F(\sqrt{D})$ be a quadratic extension. Then, $\mathrm{Tr}_{K/F}(a + b\sqrt{D}) = a^2 - Db^2$.
(3) Let $m_\alpha(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 \in F[x]$ be the minimal polynomial for $\alpha \in K$ over F. Let $n := [K : F]$ and $d|n$, then $\mathrm{Tr}_{K/F}(\alpha) = (-1)^1 \frac{n}{d} a_{n-1}$.

Proof: □

2.2 An application: Hilbert's Theorem 90

3 Galois groups of some certain extensions

3.1 Finite field extensions

3.2 Composite and simple extensions

3.3 Cyclotomic and Abelian extensions over $\mathbb{Q}$

3.4 Kummer extension

3.5 Artin-Schreier extension

4 Galois group of polynomials

In section 1, by 1.1, since Galois group is the special case of automorphism groups, we know that for a polynomial $f(x) \in F[x]$, $\mathrm{Gal}(f)$ permutes the roots of f. If f has degree n, the roots of f can be listed: $\{\alpha_1, \ldots, \alpha_n\}$ (counting multiplicity). So, the effect of $\mathrm{Gal}(f)$ on each α_i is what some subgroup of S_n does for i. In this sense, $\mathrm{Gal}(f)$ can be thought of as a subgroup of S_n

$$\mathrm{Gal}(f) \hookrightarrow S_n$$

From another perspective, every finite group is asserted by Cayley's theorem to have a subgroup of S_N for some N. Seemingly, Cayley's theorem guarantees $\mathrm{Gal}(K/F) \hookrightarrow S_n$. But this is not the case, because we do not know in priori the N in S_N given by Cayley is exactly the n as the amount of roots of f.
This embedding tells us something: If K is the splitting field of $f(x) \in F[x]$ with $\deg f(x) = n$ over F, then $|\mathrm{Gal}(K/F)| \leq |S_n| = n!$. This is a group-theoretical way to explain why the degree of extension of a splitting field of f over $F \leq n!$.

If $f(x) = f_1(x) \cdots f_k(x)$ can be written as a product of irreducible polynomials (each $f_i(x)$ is irreducible). Then, $\mathrm{Gal}(f) \leq \mathrm{Gal}(f_1) \times \cdots \times \mathrm{Gal}(f_k)$

How does $\mathrm{Gal}(f)$ act on the roots of f? (What properties does this action have?) First, this action is transitive.

4.1 Galois Groups as S_n and A_n

4.1.1 Symmetric functions and S_n

Definition 4.1: Elementary symmetric polynomials

Consider the action of $S_n \curvearrowright \{s_1, \ldots, s_n\}$, for each i, s_i is invariant under $\sigma \in S_n$, i.e. $s_{\sigma(i)} = s_i$.
Then, consider an action $S_n \curvearrowright F(x_1, \ldots, x_n)$, by permuting the indexes. Then we have the general definition of symmetric polynomial

Definition 4.2: Symmetric polynomial

Theorem 4.1: Fundamental theorem of symmetric function

Definition 4.3: General polynomial

Let $x_1, x_2, \ldots, x_n$ be indeterminates over a field F. The general polynomial over K wit respect to these indeterminates is

$$(x - x_1)(x - x_2) \cdots (x - x_n)$$

Expand this polynomial, we get $(x-x_1)(x-x_2)\cdots(x-x_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n$. So, each s_i is an expression of these indeterminates. Then, consider the field by joining $s_1, \ldots, s_n$, $F(s_1, \ldots, s_n)$, $F(x_1, x_2, \ldots, x_n)$ is the splitting field of $F(s_1, \ldots, s_n)$ (it contains all roots $x_1, \ldots, x_n$, and $F(x_1, \ldots, x_n)$ is the smallest field generated by those roots). Hence, $F(x_1, x_2, \ldots, x_n)/F(s_1, s_2, \ldots, s_n)$ is **Galois**.
From now on, let's denote $F(\underline{x}) := F(x_1, \ldots, x_n)$ and $F(\underline{s}) := F(s_1, \ldots, s_n)$

Proposition 4.1: $\mathrm{Gal}(F(\underline{x})/F(\underline{s}))$

$$\mathrm{Gal}(F(\underline{x})/F(\underline{s})) = S_n$$

4.1.2 More on symmetric polynomials

Project: Write symmetric polynomials into elementary symmetric polynomials:
Newton's formula for symmetric polynomials:
[Mos19]

4.1.3 Discriminant and A_n

4.2 Compute the Galois groups over polynomials

Given any polynomial $f(x) \in \mathbb{F}_p[x]$, we want to find $\mathrm{Gal}(f(x))$. Let $\mathbb{K}$ be the splitting field of $f(x)$ over $\mathbb{F}_p$. !! $\mathbb{K}/\mathbb{F}_p$ is a finite extension. From !!, $\mathbb{K} = \mathbb{F}_{p^k}$ for some k. So, $\mathrm{Gal}(f(x)) = \mathrm{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p) = \langle_p\rangle$.
More precisely, write $f(x) = \prod_i f_i(x)$ into some irreducible polynomials. The Galois group will be a cyclic group of order $_i(\deg f_i)$.
What is the relation between this k and $n := \deg f(x)$? Actually, they are not relevant. k could be greater than, less than or equal to n. Here we give three examples:

(1) For an irreducible polynomial $f(x)$, $k = n$. Consider $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$.

(2) Consider $f(x) = x(x-1) \in \mathbb{F}_3[x]$. The roots $0, 1$ are in $\mathbb{F}_3$. So, $\mathbb{F}_3(0,1) = \mathbb{F}_3$ and $\mathrm{Gal}(f(x)) = \{\mathrm{id}\}$. In this case, $k = 1 < n = 2$.

(3) Consider $f(x) = g(x)h(x)$, where $g(x) = x^2 + x + 1$ and $h(x) = x^3 + x + 1$. $g(x), f(x)$ are irreducible over $\mathbb{F}_2$. So, the roots $g(x)$ are in $\mathbb{F}_{2^2}$ and the roots of $h(x)$ are in $\mathbb{F}_{2^3}$. $k = (2,3) = 6 > n = 5$.

4.3 Inverse Galois problem

5 Application to radical solutions of polynomials

Galois theory is developed to answer the question: Does any quintic polynomial(over $\mathbb{Q}$) have a solution formula in radicals? The answer is no. To rephrase 'radicals', we formulate this by introducing 'radical extensions' and prolong a chain of field extension till it enclose the solution. To be more straight-forward, this process is for example, given $\alpha := \frac{\sqrt{3+\sqrt{5}}}{2}$ and starting from $\mathbb{Q}$. First adding $\sqrt{5}$ into $\mathbb{Q}$ to get $\mathbb{Q}(\sqrt{5})$. But, $\alpha \notin \mathbb{Q}(\sqrt{5})$. ??.
Then, these field extensions are so special that they are Galois. So, they have connection with their Galois group.

5.1 Solvable and radical extensions

5.2 The main theorem

Theorem 5.1: (Abel, Galois)

Let F be a field of char$K = 0$, $f(x) \in F[x]$ and K be a splitting field of F with respect to $f(x)$.
$\exists$ a finite extension K'/K having a root tower over $F \Leftrightarrow \mathrm{Gal}(K'/F)$ is solvable

Proof:

Lemma 5.1 (Condition for irreducibility) *Let F be a field of any characteristic and p be a prime number. If $x^p - a \in F[x]$(or $a \in F$) has no solution in F, then $x^p - a$ is irreducible over F.*

proof of lemma: (1) First assume that char$F \neq p$.
(2) Then assume that char$F = p$ $\clubsuit$
$\square$

6 Transcendental extensions, inseparable extensions and infinite Galois groups

7 The Galois theory of étale algebras

provided by [Mil22]

References

[DF03] David S. Dummit and Richard M. Foote. *Abstract Algebra*. 3rd. Hoboken, NJ: John Wiley & Sons, 2003. ISBN: 978-0-471-43334-7.

[Mos19] Milan Mossé. *Newton's Identities*. Course notes for CS250 (Algebraic Methods in Computer Science), Stanford University. Winter 2019 Lecture Notes. 2019. URL: https://web.stanford.edu/~marykw/classes/CS250_W19/Netwons_Identities.pdf.

[Mil22] James S. Milne. *Fields and Galois Theory (v5.10)*. Available at www.jmilne.org/math/. 2022.

[Connd] Keith Conrad. *Fundamental Theorems of Galois Theory*. Expository notes, University of Connecticut. From the author's *Mathematical Blurbs* collection. n.d. URL: https://kconrad.math.uconn.edu/blurbs/galoistheory/galoiscorrthms.pdf (visited on 08/20/2023).