Lecture Notes On Abstract Algebra (Week 13)

Guohua PENG (彭国华)
email: peng@scu.edu.cn

Contents

1 Lecture 24 (Nov 28, 2023): Galois Extensions and Finite Fields **1**
1.1 Galois Extensions 1
1.2 Finite Fields 3

2 Lecture 25 (Dec 30, 2023): Galois Group of a Polynomial and Cyclotomic Fields **6**
2.1 Group Action 6
2.2 Galois Group of a Polynomial 9
2.3 The Galois Group of $x^4 - 2$ over $\mathbb{Q}$ 11

1 Lecture 24 (Nov 28, 2023): Galois Extensions and Finite Fields

1.1 Galois Extensions

We have proved the following results.

Fact 1 For an algebraic extension K/F, the following three are equivalent:

1. The extension K/F is *normal*;
2. Every irreducible polynomial $f(x) \in F[x]$ that has a root in K splits completely over F;
3. If $f(x) \in F[x]$ is irreducible and has a root in K, then all roots of $f(x)$ are in K.
4. For every F-embedding on K, we have $\sigma(K) = K$.

Fact 2 A finite extension extension K/F of degree n is *separable* if and only if there are exactly n F-embeddings on K.

Hence a finite extension K/F is normal if and only if K/F is a splitting field for some polynomial over F.

Definition 1.1. *An extension K/F of fields is called* **Galois** (伽罗瓦扩张) *if it is normal and separable.*

If K/F is a finite separable extension, then K/F is Galois if and only if K is a splitting field of some polynomial over F. Moreover, we have $K = F(\alpha)$ for some $\alpha \in K$, by the Primitive Element Theorem. In this case, K/F is Galois if and only if K is a splitting field of $m(x)$, where $m(x)$ is the minimal polynomial of α over F.

A finite Galois extension is a splitting field of some separable polynomial.

Theorem 1.1. *Let K/F be a finite extension of fields. Then the following claims are equivalent.*

1. *The extension K/F is Galois.*
2. *The K is a splitting field of some separable polynomial over F.*
3. $|\mathrm{Gal}(K/F)| = [K : F]$.

Proof. By what we discussed in normal and separable extensions, the equivalence of Claim 1 and Claim 2 are clear. Furthermore, Claim 1 implies Claim 3.

Assume $|\mathrm{Gal}(K/F)| = [K : F] = n$. Then there are exactly n F-automorphisms on K, hence there are at least n F-embeddings on K. Notice that there are at most n F-embeddings on K and every F-automorphism is an F-embedding. So there are exactly n F-embeddings on K and every F-embedding is essentially an F-automorphism. By previous facts, we know that K/F is separable and normal. Thus K/F is Galois and Claim 1 and Claim 3 are equivalent. □

Definition 1.2. *Let K/F be a Galois extension. If $\mathrm{Gal}(K/F)$ is an abelian group, then K/F is called an* **abelian extsnsion** (Abel 扩张). *If $\mathrm{Gal}(K/F)$ is a cyclic group, then the extension K/F is called* **cyclic** (循环的).

Example 1.1. Every quadratic extension over $\mathbb{Q}$ is of the form $\mathbb{Q}(\sqrt{d}\,)$, where $|d|$ is a square-free integer and $d \neq 1$. Hence such quadratic extensions are Galois and cyclic.

Example 1.2. Let $\zeta_n = e^{\frac{2\pi i}{n}}$ be a primitive n-th root of unity. Then the cyclotomic field $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois and we will see that

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) = \{\sigma_i \mid i \in \mathbb{Z}, (i, n) = 1\} \cong (\mathbb{Z}/n\mathbb{Z})^{\times},$$

where $\sigma_i(\zeta_n) = \zeta_n^i$. Hence a cyclotomic field is an abelian extension over $\mathbb{Q}$. Notice that the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^{\times}$ is cyclic if and only if $n = 2, 4, p^m, 2p^m$, where p is an odd prime. It follows that the cyclotomic field $\mathbb{Q}(\zeta_n)$ is a cyclic extension over $\mathbb{Q}$ if and only if $n = 2, 4, p^m, 2p^m$.

Remark 1.1. We will show that every extension of finite fields is cyclic.

Exercises

1. Show that every finite separable extension is contained in a finite Galois extension.
2. Let K/F be a finite Galois extension. Show that K is the splitting field of some irreducible polynomial $m(x)$ over F and $K = F(\alpha)$ holds for any root α of $m(x)$.
3. Let K/F be a finite Galois extension of degree n. Show that K is a splitting field of a separable irreducible polynomial of degree n.
4. Let K/F be a Galois extension and M an intermediate subfield. Is it true that the extensions K/M and M/F are still Galois?
5. Let L, M be intermediate subfields of K/F such that L and M both are finite Galois extensions over F. Is it true that LM and $L \cap M$ are Galois extensions over F?

1.2 Finite Fields

A finite field is a field that contains a finite number of elements. We have seen, in the previous lectures, some examples of finite fields. For example, the residue class ring $\mathbb{Z}/p\mathbb{Z}$ (when p is a prime) forms a field with p elements which may be identified with the Galois field $\mathbb{F}_p$ of order p.

The fields $\mathbb{F}_p$ are important in field theory. From the previous chapter, every field of characteristic p contains a copy of $\mathbb{F}_p$ (its prime subfield) and can therefore be thought of as an extension of $\mathbb{F}_p$. Since every finite field must have characteristic p, this helps us to classify finite fields.

Finite fields are important in number theory, algebraic geometry, Galois theory, cryptography, coding theory and quantum error correction. The finite fields are classified by size.

Basic Observation Let F be a finite field with $|F| = q$ and K/F an extension of degree m. Then K is an m-dimensional vector space over F and $|K| = q^m$.

Lemma 1.1. *Let F be a finite field with characteristic p, a prime. Then the prime subfield $\mathbb{F}_p$ can be canonically embedded as a subfield of F and $|F| = p^n$ with $n = [F : \mathbb{F}_p]$.*

Remark 1.2. Remember that the prime field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, where p is a prime.

The cardinality of a finite field must be a prime power.

Hence there is no finite field with 6 elements, for example. The next question: does there exist a finite field of order p^n for every prime power p^n? How can such fields be constructed?

According to previous lectures, we can start with the prime fields $\mathbb{F}_p$ and construct other finite fields from them by adjoining roots of polynomials. If $f \in \mathbb{F}_p[x]$ is irreducible of degree n over $\mathbb{F}_p$, then adjoining a root of f to $\mathbb{F}_p$ yields a finite field of p^n elements. However, it is not clear whether we can find an irreducible polynomial in $\mathbb{F}_p[x]$ of degree n, for every integer n. A positive answer will be given at the end of the lecture.

Example 1.3. A finite field F with 9 elements can be constructed in the following way: $F = \mathbb{F}_3(\theta)$, where θ is a root of the polynomial $x^2 + x + 2 \in \mathbb{F}_3[x]$.

We construct finite fields from another approach. The following lemma will help us to characterize fields using root adjunction.

Lemma 1.2. *Let F be a finite field with q elements, where $q = p^n$ and* $\mathrm{char}(F) = p$.

(1) Every $a \in F$ satisfies $a^q = a$. And the polynomial $x^q - x$ in $\mathbb{F}_p[x]$ factors in $F[x]$ as

$$x^q - x = \prod_{a \in F} (x - a).$$

(2) The finite field F is a splitting field of $x^q - x$ over $\mathbb{F}_p$.

We are now ready to prove the main characterization theorem for finite fields.

Theorem 1.2 (Existence and Uniqueness of Finite Fields)**.** *Let $q = p^n$, where p is a prime and $n \geq 1$.*

(1) There does exist a finite field with q elements: the splitting field of $x^q - x$ over $\mathbb{F}_p$ in $\overline{\mathbb{F}}_p$.

(2) All finite fields with q elements are isomorphic. In other words, there is only one finite field with q elements up to isomorphism.

Proof. (Existence) For $q = p^n$, consider $f(x) = x^q - x \in \mathbb{F}_p[x]$, and let F be its splitting field over $\mathbb{F}_p$. Since its derivative $f'(x) = qx^{q-1} - 1 = -1$ in $\mathbb{F}_p[x]$, it can have no common root with $f(x)$. So $x^q - x$ has q distinct roots in F. Let

$$L = \{a \in F \mid a^q - a = 0\}.$$

Direct check shows that L is a subfield of F and $|L| = p^n$.

On the other hand, $x^q - x$ must split in L, since L contains all its roots, i.e, its splitting field F is a subfield of L. Thus $F = L$ and, since L has q elements, F is a finite field with $q = p^n$ elements.

(Uniqueness) Let F be a finite field with $q = p^n$ elements. Then F has characteristic p, and contains $\mathbb{F}_p$ as a subfield. So F is a splitting field of $x^q - x$ by Lemma 1.2. The result now follows from the uniqueness (up to isomorphism) of splitting fields. □

Fixing a splitting field of $x^q - x$ over $\mathbb{F}_p$, the proof of Theorem 1.2 shows that every finite field with q elements is isomorphic to this splitting field. Essentially, there is only one finite field with q elements for a prime power q. So we may speak of the finite field of q elements.

A finite field is also called a **Galois field**.

The finite field with q elements is denoted by $\mathbb{F}_q$ or $GF(q)$.

Example 1.4. We constructed a field $F = \mathbb{F}_2(\theta)$ of 4 elements, where θ is a root of the polynomial $x^2 + x + 1 \in \mathbb{F}_2[x]$. By Theorem 1.2, F is the field of 4 elements, i.e. $\mathbb{F}_4$.

We can also completely describe the subfields of a finite field $\mathbb{F}_q$.

Theorem 1.3. *Let $\mathbb{F}_q$ be the finite field with $q = p^n$ elements. Then every subfield of $\mathbb{F}_q$ has cardinality p^m with $m \mid n$. Conversely, if m is a positive divisor of n, then there is exactly one subfield of $\mathbb{F}_q$ with p^m elements. In other words, $\mathbb{F}_{p^m}$ is a subfield of $\mathbb{F}_{p^n}$ if and only if $m \mid n$.*

Proof. Clearly, a subfield L of $\mathbb{F}_q$ must have order p^m with $m = [L : \mathbb{F}_p] \leq n = [\mathbb{F}_q : \mathbb{F}_p]$. But $[\mathbb{F}_q : \mathbb{F}_p] = [\mathbb{F}_q : L][L : \mathbb{F}_p]$. Hence $m \mid n$.

Conversely, if m is a positive divisor of n, then $p^m - 1 \mid p^n - 1$, and so $x^{p^m-1} - 1 \mid x^{p^n-1} - 1$ in $\mathbb{F}_p[x]$. So, every root of $x^{p^m} - x$ is a root of $x^{p^n} - x$, and hence belongs to $\mathbb{F}_q$. It follows that $\mathbb{F}_q$ must contain a splitting field of $x^{p^m} - x$ over $\mathbb{F}_p$ as a subfield, and (from proof of Theorem 1.2) such a splitting field has order p^m. If there were two distinct subfields of order p^m in $\mathbb{F}_q$, they would together contain more than p^m roots of $x^{p^m} - x$ in $\mathbb{F}_q$, a contradiction. □

Remark 1.3. Notice that $\mathbb{F}_4$ is not a subfield of $\mathbb{F}_8$.

The multiplicative group of nonzero elements in a finite field is essentially cyclic. More generally, we have the following

Theorem 1.4. *Every finite subgroup of the multiplicative group of nonzero elements of a field is cyclic.*

Proof. Let G be a finite group of order n in F^*, where F is a field, not necessarily finite. Then G is abelian and $g^n = 1$ for every $g \in G$.

If G is not cyclic, then $g^m - 1 = 0$ holds for some positive integer $m < n$ and all elements in G (why? think of the structure theorem on finite abelian groups). This shows that $f(x) = x^m - 1$ has at least n roots in F, as is impossible. □

Corollary 1.1. *For every finite field $\mathbb{F}_q$, the multiplicative group $\mathbb{F}_q^\times$ of nonzero elements of $\mathbb{F}_q$ is cyclic of order $q-1$.*

A generator of the cyclic group $\mathbb{F}_q^\times$ is called a **primitive element** (原根, 本原元) of $\mathbb{F}_q$.

Theorem 1.5. *Every finite extension of finite fields is simple. More precisely, every primitive element θ of $\mathbb{F}_{q^n}$ can serve as a defining element of $\mathbb{F}_{q^n}/\mathbb{F}_q$.*

Proof. Let θ be a primitive element of $\mathbb{F}_{q^n}$. Clearly, $\mathbb{F}_q(\theta) \subseteq \mathbb{F}_{q^n}$. On the other hand, since $\mathbb{F}_q(\theta)$ contains 0 and all powers of θ, it contains all elements of $\mathbb{F}_{q^n}$. So $\mathbb{F}_{q^n} = \mathbb{F}_q(\theta)$. □

Corollary 1.2. *For every finite field $\mathbb{F}_q$ and every positive integer n, there exists an irreducible polynomial in $\mathbb{F}_q[x]$ of degree n.*

Proof. Notice $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$. By Theorem 1.6, $\mathbb{F}_{q^n} = \mathbb{F}_q(\theta)$ for some $\theta \in \mathbb{F}_{q^n}$. Then, by properties of minimal polynomials, the minimal polynomial of θ over $\mathbb{F}_q$ is an irreducible polynomial in $\mathbb{F}_q[x]$ of degree n. □

Theorem 1.6. *Every extension of finite fields is cyclic. More precisely, $\mathbb{F}_{q^n}/\mathbb{F}_q$ is a Galois extension with Galois group $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle \sigma_q \rangle$, where*

$$\begin{aligned} \sigma_q : \mathbb{F}_{q^n} &\to \mathbb{F}_{q^n} \\ \alpha &\mapsto \alpha^q \end{aligned}$$

is called the the q-th **Frobenius map**.

- A finite field of q elements exists $\iff q = p^n$ and $p = \mathrm{char}(F)$.
- Up to isomorphism, there is only one field of q elements: $\mathbb{F}_q$.
- For $n \geq 1$, there does exist an irreducible polynomial of degree n over $\mathbb{F}_q$.
- $\mathbb{F}_q^\times$ is cyclic of order $q-1$.
- $\mathbb{F}_{q^m}$ is a subfield of $\mathbb{F}_{q^n} \iff m \mid n$.
- The extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is Galois and $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle \sigma_q \rangle$, where $\sigma_q(x) = x^q$ is the q-th Frobenius map.

Exercises

1. Let $\mathrm{char}\, F = p \neq 0$. Is F necessarily a finite field?
2. Is there a finite field with 2023 elements?
3. Show that $\mathbb{F}_{13}[x]/(x^3 + x + 2)$ is a finite field with 2197 elements.
4. Construct a finite field with 25 elements.
5. Show that every extension of finite fields is Galois.
6. Let $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial over $\mathbb{F}_q$ of degree m. Then $f(x) \mid x^{q^n} - x$ if and only if $m \mid n$.

7. If $f(x)$ is an irreducible polynomial in $\mathbb{F}_q[x]$ of degree m, then f has a root $\alpha \in \mathbb{F}_{q^m}$. Moreover, all the roots of $f(x)$ are simple and are given by the m distinct elements $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ of $\mathbb{F}_{q^m}$.

8. Let $f(x)$ be an irreducible polynomial in $\mathbb{F}_q[x]$ of degree m. Then the splitting field of $f(x)$ over $\mathbb{F}_q$ is $\mathbb{F}_{q^m}$.

9. Any two irreducible polynomials over the same finite field of the same degree have isomorphic splitting fields.

10. For every finite field $\mathbb{F}_q$ and every positive integer n, the product of all monic irreducible polynomials over $\mathbb{F}_q$ whose degrees divide n is equal to $x^{q^n} - x$.

11. Let $\mathbb{F}_q$ be a finite field with q elements, where $q = p^n$.

    (a) Show that $\mathbb{F}_q/\mathbb{F}_p$ is a Galois extension and $\mathrm{Gal}\,(\mathbb{F}_q/\mathbb{F}_p)$ is a cyclic group of order n generated by σ_p, where the map σ_p, which is called the p-th Frobenius, is given by

    $$\begin{aligned} \sigma_p : \mathbb{F}_q &\to \mathbb{F}_q \\ a &\mapsto a^p. \end{aligned}$$

    (b) Let $\alpha \in \mathbb{F}_q$. Show that the $\mathbb{F}_p$-conjugates of α must be of the form α^{p^m}.

12. Let q be a power a prime number. Show that $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle \sigma_q \rangle$, where $\sigma_q(x) = x^q$ is the q-th Frobenius map.

13. Let q be a prime power. Show that for every $\alpha \in \mathbb{F}_q$, there exists some $\beta \in \mathbb{F}_{q^2}$ such that $\alpha = \beta^{q+1}$.

14. Let p be a prime and n an positive integer. Show that the splitting field of $x^n - 1$ over $\mathbb{F}_p$ is $\mathbb{F}_{p^m}$, where m is the order of p modulo n (i.e. m is the smallest positive integer such that $p^m \equiv 1 (\mathrm{mod}\, n)$).

15. Let F be a finite extension of $\mathbb{Q}$ and let W_F denote the set of roots of unity in F. Show that W_F is a multiplicative cyclic group.

2 Lecture 25 (Dec 30, 2023): Galois Group of a Polynomial and Cyclotomic Fields

2.1 Group Action

Let X be a set and G a group. A (left) **action** of G on X is a map $G \times X \to X$ given by $(g, x) \mapsto g * x$, such that

1. $1 * x = x$ for all $x \in X$;

2. $(g_1 g_2) * x = g_1 * (g_2 * x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

For simplicity, we may write gx for $g * x$. Under these considerations, we also say $\underline{G \text{ acts on } X}$, or X is called a $\underline{G\text{-set}}$. Notice that we are not requiring X to be related to G in any way. It is true that every group G acts on every set X by the trivial action $(g, x) \mapsto x$; however, group actions are more interesting if the set X is somehow related to the group G.

Historically, the first group action studied was the action of the Galois group on the roots of a polynomial. However, there are numerous examples and applications of group actions in many branches

of mathematics, including algebra, topology, geometry, number theory, and analysis, as well as the sciences, including chemistry and physics.

Example 2.1. Let $G = \mathrm{GL}_n(\mathbb{R})$ be the multiplicative group of all $n \times n$ invertible matrix over (generalized linear group) and let $X = \mathbb{R}^n$ be the n-dimensional column vector space. Then G acts on X by left multiplication: for $A \in \mathrm{GL}_n(\mathbb{R})$ and $v \in \mathbb{R}^n$, $A * v = Av$. If $v \in \mathbb{R}^n$, then $I * v = Iv = v$, where I is the identity matrix. If A and B are $n \times n$ invertible matrices, then $(AB)v = A(Bv)$ implies $(AB) * v = A * (B * v)$.

Example 2.2. Let $G = D_4$ be the symmetry group of a square. If $X = \{1, 2, 3, 4\}$ is the set of vertices of the square, then we can consider D_4 to consist of the following permutations:

$$\{(1), (1\,3), (2\,4), (1\,4\,3\,2), (1\,2\,3\,4), (1\,2)(3\,4), (1\,4)(2\,3), (1\,3)(2\,4)\}.$$

The elements of D_4 act on X as functions. The permutation $(1\,3)(2\,4)$ acts on vertex 1 by sending it to vertex 3, on vertex 2 by sending it to vertex 4, and so on. It is easy to see that the axioms of a group action are satisfied. In general, if X is any set with n elements and G is a subgroup of S_n, the group of all permutations acting on X, then X is a G-set under the group action

$$(\sigma, x) \mapsto \sigma(x)$$

for $\sigma \in G$ and $x \in X$.

Example 2.3. Let $X = G$, then every group G acts on itself by the left regular representation. That is, $(g, x) \mapsto \lambda_g(x) = g \cdot x$, where λ_g is left multiplication:

$$1 \cdot x = \lambda_1(x) = 1x = x$$
$$(gh) \cdot x = \lambda_{gh}(x) = \lambda_g(\lambda_h(x)) = \lambda_g(hx) = g \cdot (h \cdot x).$$

If H is a subgroup of G, then G is an H-set under left multiplication by elements of H.

Example 2.4. Let G be a group and set $X = G$. If H is a subgroup of G, then G is an H-set under conjugation; that is, we can define an action of H on G,

$$H \times G \to G,$$

via

$$(h, g) \mapsto hgh^{-1}$$

for $h \in H$ and $g \in G$.

Clearly, the first axiom for a group action holds. Observing that

$$\begin{aligned}(h_1h_2, g) &= h_1h_2g(h_1h_2)^{-1} \\ &= h_1(h_2gh_2^{-1})h_1^{-1} \\ &= (h_1, (h_2, g)),\end{aligned}$$

we see that the second condition is also satisfied.

Example 2.5. Let H be a subgroup of G and $\mathcal{L}_H$ the set of left cosets of H. It's easy to check that the set $\mathcal{L}_H$ is a G-set under the action

$$(g, xH) \mapsto gxH.$$

Let $S(X)$ denote the transformation group of X, i.e.

$$S(X) = \{f : X \to X \mid f \text{ is a bijective map}\}.$$

The group operation in $S(X)$ is the composition of maps. If $|X| = n$, the $S(X) = S_n$, the symmetric group of n elements.

If G acts on X and $g \in G$, it's easy to check that g induces a bijection τ_g on X, where

$$\begin{aligned} \tau_g : X &\to X \\ x &\mapsto gx. \end{aligned}$$

Consequently,

$$\begin{aligned} \tau : G &\to S(X) \\ g &\mapsto \tau_g \end{aligned}$$

is a group homomorphism.

Conversely, a group homomorphism $\tau : G \to S(X)$ defines a G action on X:

$$\begin{aligned} G \times S &\to S \\ (g, x) &\mapsto \tau(g)(s). \end{aligned}$$

An action of G on a set X is equivalent to a group homomorphism $\tau : G \to S(X)$.

A group action $G \times X \to X$ is called **faithful** if there are no group elements g (except the identity element) such that $gx = x$ for all $x \in X$. Equivalently, the group action induces the group homomorphism $\tau : G \to S(X)$ is injective. So G can be identified with a permutation subgroup. In particular, if $|X| = n$ and G acts faithfully on X, then G can be embedded in to S_n.

If G acts on a set X and $x, y \in X$, then x is said to be G**-equivalent** to y if there exists a $g \in G$ such that $gx = y$. We write $x \sim_G y$ or $x \sim y$ if two elements are G-equivalent. One can easily see that the G-equivalence is an equivalence relation on X. The equivalence classes of this action are called **orbits**. If we denote the orbit that contains an element x of X by $\mathcal{O}_x$, then

$$\mathcal{O}_x = \{gx \mid g \in G\}.$$

It's clear that $\mathcal{O}_x$ is a G-set.

Example 2.6. Let G be the permutation group defined by

$$G = \{(1), (1\,2\,3), (1\,3\,2), (4\,5), (1\,2\,3)(4\,5), (1\,3\,2)(4\,5)\}$$

and $X = \{1, 2, 3, 4, 5\}$.

Then X is a G-set. The orbits are $\mathcal{O}_1 = \mathcal{O}_2 = \mathcal{O}_3 = \{1, 2, 3\}$ and $\mathcal{O}_4 = \mathcal{O}_5 = \{4, 5\}$.

The action is said to be **transitive** if there is only one orbit. If G acts transitively on X, then $X = \mathcal{O}_x$ for every $x \in X$.

Let X be a G-set and $x \in X$. The **stabilizer** of x, denoted by G_x, is defined by

$$G_x = \{g \in G \mid gx = x\}.$$

It's easy yo show that G_x is a subgroup of G. The stabilizer of x is also called the **isotropy subgroup** of x.

Example 2.7. Let $X = \{1,2,3,4,5,6\}$ and suppose that G is the permutation group given by the permutations

$$\{(1), (1\,2)(3\,4\,5\,6), (3\,5)(4\,6), (1\,2)(3\,6\,5\,4)\}.$$

Then the stabilizer subgroups are

$$G_1 = G_2 = \{(1), (3\,5)(4\,6)\},$$
$$G_3 = G_4 = G_5 = G_6 = \{(1)\}.$$

It is easily seen that G_x is a subgroup of G for each $x \in X$.

Let G be a finite group and X a finite G-set. If $x \in X$, then $|\mathcal{O}_x| = [G : G_x]$.

2.2 Galois Group of a Polynomial

For a field extension K/F, $\mathrm{Gal}(K/F)$ is called the **Galois group** (伽罗瓦群) of K/F.

$$\begin{aligned}\mathrm{Gal}(K/F) &= \text{the group of all } F\text{-automorphisms of } K \\ &= \text{the group of all automorphisms of } K \text{ extending the identity map on } F \\ &= \{\sigma : K \to K \mid \sigma \text{ is an automorphism of rings and } \sigma(\alpha) = \alpha \text{ for all } \alpha \in F\}.\end{aligned}$$

Recall:

- $\mathrm{Aut}(K)$: the automorphism group of a field K.
- $\mathrm{Gal}(K/F)$: the automorphism group of the field extension K/F.
- A Galois extension is a separable and normal extension.
- A finite extension K/F is Galois if and only if K is a splitting field of some separable polynomial over F.
- If K/F is a finite Galois extension, then $|\mathrm{Gal}(K/F)| = [K : F]$.

Definition 2.1. *If K is a splitting field of a separable polynomial $f(x) \in F[x]$ and $F \subseteq K$, then the Galois group $\mathrm{Gal}(K/F)$ is called the* **Galois group of the polynomial** *$f(x)$ over F, which is also denoted by $\mathrm{Gal}(f(x)/F)$, or simply G_f.*

The Galois group of $f(x) \in F[x]$ over F is $\mathrm{Gal}(K/F)$, where K is a splitting field of $f(x)$ over F.

Remark 2.1. For $f(x) \in F[x]$, $\mathrm{Gal}(f(x)/F)$ is also called the *group of $f(x)$ over F*.

Let K/F be a finite Galois extension. Then K is a splitting field of some separable irreducible polynomial $f(x) \in F[x]$ over F. If $\deg f(x) = n$, then $f(x)$ has exactly n distinct roots in K, on which the Galois group $\mathrm{Gal}(L/F)$ acts. More precisely, let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be all roots of $f(x)$, then for each $i = 1, 2, \ldots, n$, $\sigma(\alpha_i) = \alpha_j$ for some j. Hence the Galois group $\mathrm{Gal}(L/F)$ acts on the set $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. This group action induces a permutation on n elements. So we have

Theorem 2.1. *Let $f(x) \in F[x]$ with $\deg f(x) = n$. The Galois group of $f(x)$ can be embedded in the full symmetric group S_n. That is, $\mathrm{Gal}(f(x)/F) \hookrightarrow S_n$.*

Proof. Let $G = \mathrm{Gal}(f(x)/F)$. If $f(x)$ is irreducible and $X = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is the set of all roots of $f(x)$, then G acts on X and induces a group homomorphism

$$\begin{aligned} \tau : G &\to S_n = S(X) \\ \sigma &\mapsto (i_1\, i_2\, \cdots\, i_n) = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}, \text{ if } \sigma(\alpha_k) = \alpha_{i_k}. \end{aligned}$$

Since an element of G is completely determined by its action on X, τ is injective. Hence $G \hookrightarrow S_n$, i.e. every element of G can be regarded as a permutation of n elements.

If $f(x)$ is reducible, $m_1(x), m_2(x), \ldots, m_r(x)$ are all monic irreducible factors of $f(x)$, then G is the Galois group of $m_1(x)m_2(x)\cdots m_r(x)$. So we may assume $f(x) = m_1(x)m_2(x)\cdots m_r(x)$. In particular, $\deg m_i(x) = n_i < n$.

For $\sigma \in G$ and a root α of $m_i(x)$, $\sigma(\alpha)$ is also a root of $m_i(x)$. Hence σ acts on the roots of $m_i(x)$ and induces a permutation $\sigma_i \in S_{n_i} \subseteq S_n$. For $i \neq j$, the roots of $m_i(x)$ and roots of $m_j(x)$ are not conjugate over F. It follows $\sigma = \sigma_1\sigma_2\cdots\sigma_r \in S_n$. Therefore $G \hookrightarrow S_n$. □

Example 2.8. Let $K = \mathbb{Q}(\sqrt{2})$. Then K is a splitting field of x^2-2 and $\mathrm{Gal}((x^2-2)/\mathbb{Q}) = S_2$. Actually, $\mathrm{Gal}(x^2 - 2/\mathbb{Q}) = \{\mathrm{id}, \sigma\}$, where $\sigma(\sqrt{2}) = -\sqrt{2}$. And

$$\begin{aligned} \mathrm{Gal}\left((x^2-2)/\mathbb{Q}\right) &\to S_2 = \{(1), (12)\} \\ \mathrm{id} &\mapsto (1) \\ \sigma &\mapsto (12). \end{aligned}$$

Here (12) denotes the permutation

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix},$$

which is a 2-cycle.

Galois group of a cubic polynomial Let F be a field whose characteristic is not 3. Then every monic cubic polynomial can be modified to be of the form $x^3 + px + q$ by a translation. Assume $f(x) = x^3 + px + q$ is irreducible and let G be the Galois group of $f(x)$ over F. Then $G \cong A_3$ if if and only if the discriminant $D(f) = -(4p^3 + 27q^2)$ of $f(x)$ has a square root in the field F. Otherwise, $G \cong S_3$.

Let $\mathrm{char}F \neq 3$ and $f(x) = x^3+px+q \in F[x]$ with discriminant $D(f) = -(4p^3+27q^2)$. Then

$$\mathrm{Gal}(f(x)/F) = \begin{cases} 1, & \text{if all roots of } f(x) \text{ are in } F, \\ S_2, & \text{if only one root of } f(x) \text{ are in } F, \\ A_3, & \text{if } f(x) \text{ is irreducible and } D(f) \text{ is a square in } F, \\ S_3, & \text{if } f(x) \text{ is irreducible and } D(f) \text{ is not a square in } F. \end{cases}$$

Exercises

1. Let $f(x)$ be a polynomial over F and E its splitting field. Show that $\mathrm{Gal}(E/F)$ of $f(x)$ can be embedded in S_m, where m is the maximum of the degrees of the irreducible factors of $f(x)$.

2. Let K be a splitting field of a separable polynomial $f(x) \in F[x]$ and $\deg f = n$. Show that G_f is transitive (i.e. G_f acts transitively on the set of roots) if and only if $f(x)$ is irreducible over F.

3. Let K be a splitting field of a separable polynomial $f(x) \in F[x]$ and $\deg f = n$. Define the discriminant of f by $D(f) = \delta^2$, where $\delta = \prod_{1 \le i < j \le n}(\alpha_i - \alpha_j)$ and $\alpha_1, \alpha_2, \ldots, \alpha_n$ are all roots of $f(x)$.

   (a) Show that $D(f) \in F$.

   (b) For $f(x) = x^3 + ax + b \in F[x]$. Show that $D(f) = -4a^3 - 27b^2$.

   (c) We know that G_f acts on the set $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ and that this action induces an embedding $G_f \hookrightarrow S_n$ in a natural way. Let $\sigma \in G_f$. Show that σ induces an even permutation if and only if $\sigma(\delta) = \delta$, and that σ induces an odd permutation if and only if $\sigma(\delta) = -\delta$.

   (d) Show that $G \hookrightarrow A_n$ according to the above embedding (i.e, every element of F induces an even permutation) if and only if $\delta \in F$.

4. Let p be a prime and let $f(x)$ be a polynomial of degree p over F with splitting field E.

   (1) If $p \mid |\mathrm{Gal}(E/F)|$, then $f(x)$ is irreducible and separable over F.

   (2) If $p \mid [E : F]$, then $f(x)$ is irreducible over F.

   (3) If $[E : F] = np$ for some integer n which is bigger than 1, then $f(x)$ is irreducible and separable over F.

5. Let $f(x) = x^3 + x + 3 \in \mathbb{F}_5[x]$. Determine the Galois group of $f(x)$ over $\mathbb{F}_5$.

6. Let p be a prime integer and n a positive integer. Determine the Galois group of $x^n - 1$ over $\mathbb{F}_p$.

7. Let $f(x) \in \mathbb{Q}[x]$ be a monic integer polynomial and $\deg f(x) = n$. For a prime integer p, we write $\overline{f}(x) = f(x)$ modulo p. Hence $\overline{f}(x) = f(x) \bmod p \in \mathbb{F}_p[x]$. Assume $\overline{f}(x)$ has no multiple roots.

   (1) Show that $G_{\overline{f}}$ can be viewed as a subgroup of G_f.

   (2) Let $\overline{f}(x)$ be irreducible over $\mathbb{F}_p$. Show that G_f has an n-cycle.

2.3 The Galois Group of $x^4 - 2$ over $\mathbb{Q}$

Basic Observation Let $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ be a Galois extension of F. Then an element $\sigma \in \mathrm{Gal}(K/F)$ is completely determined by $\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_n)$. In particular, if $K = \mathbb{Q}(\alpha)$ is a splitting field of a polynomial $f(x)$, then an element $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is completely determined by $\sigma(\alpha)$.

A straightforward application of Eisenstein's Criterion shows that the polynomial $x^4 - 2$ is irreducible over $\mathbb{Q}$. Let α be the unique positive real number satisfying $\alpha^4 = 2$ (i.e., $\alpha = \sqrt[4]{2}$). Then the roots of $x^4 - 2$ in the field $\mathbb{C}$ of complex numbers are $\alpha, i\alpha, -\alpha$ and $-i\alpha$, where $i = \sqrt{-1}$. That is,

$$\alpha, i\alpha, -\alpha, -i\alpha$$

are all $\mathbb{Q}$-conjugates of α in $\mathbb{C}$. Thus $K = \mathbb{Q}(\alpha, i)$ is a splitting field for the polynomial $x^4 - 2$ over $\mathbb{Q}$.

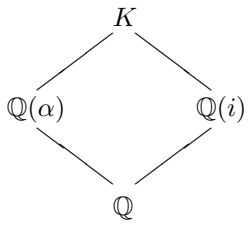
Now the polynomial $x^4 - 2$ is the minimum polynomial of α over $\mathbb{Q}$, since this polynomial is irreducible. It follows that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Now i does not belong to $\mathbb{Q}(\alpha)$, since $\mathbb{Q}(\alpha) \subset \mathbb{R}$. Therefore the polynomial $x^2 + 1$ is the minimum polynomial of i over $\mathbb{Q}(\alpha)$. So we have $[K : \mathbb{Q}(\alpha)] = [\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] = 2$. It follows

from the Tower Law (Transitivity of Degree of Field Extensions) that $[K:\mathbb{Q}] = [K:\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}] = 8$. Moreover the extension $K/\mathbb{Q}$ is a Galois extension. Actually K is the splitting field of

$$(x^2+1)(x^4-2)$$

over $\mathbb{Q}$, and therefore $\mathrm{Gal}(K/\mathbb{Q})$ is a group of order 8.

Another application of the Tower Law now shows that $[K:\mathbb{Q}(i)] = 4$, since $[K:\mathbb{Q}] = [K:\mathbb{Q}(i)][\mathbb{Q}(i):\mathbb{Q}]$ and $[\mathbb{Q}(i):\mathbb{Q}] = 2$. Therefore the minimum polynomial of α over $\mathbb{Q}(i)$ is a polynomial of degree 4. But α is a root of x^4-2. Therefore x^4-2 is irreducible over $\mathbb{Q}(i)$, and is the minimum polynomial of α over $\mathbb{Q}(i)$.



Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Since $K = \mathbb{Q}(\alpha, i)$, the action of σ is determined by its action on α and i. Notice that $\sigma(\alpha)$ must be one of $\alpha, i\alpha, -\alpha, -i\alpha$ and $\sigma(i)$ must be one of $i, -i$. For $a \in \mathbb{Q}$, define

$$\begin{array}{cccc}
\sigma_1 : K \to K, & \sigma_2 : K \to K, & \sigma_3 : K \to K, & \sigma_4 : K \to K, \\
\mathbb{Q} \ni a \mapsto a & a \mapsto a & a \mapsto a & a \mapsto a \\
\alpha \mapsto \alpha & \alpha \mapsto i\alpha & \alpha \mapsto -\alpha & \alpha \mapsto -i\alpha \\
i \mapsto i & i \mapsto i & i \mapsto i & i \mapsto i, \\
\\
\sigma_5 : K \to K, & \sigma_6 : K \to K, & \sigma_7 : K \to K, & \sigma_8 : K \to K, \\
a \mapsto a & a \mapsto a & a \mapsto a & a \mapsto a \\
\alpha \mapsto \alpha & \alpha \mapsto i\alpha & \alpha \mapsto -\alpha & \alpha \mapsto -i\alpha \\
i \mapsto -i & i \mapsto -i & i \mapsto -i & i \mapsto -i.
\end{array}$$

One can see that each σ_i can be extended to a $\mathbb{Q}$-automorphisms of K. For example, noting that the elements in $K = \mathbb{Q}(\alpha)(i)$ can be expresses as $\sum_{j=0}^{3} a_j\alpha^j + \sum_{j=0}^{3} b_j\alpha^j i$, the $\mathbb{Q}$-automorphism σ_6 is given by

$$\begin{aligned}
&\sigma_6\left(a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + b_0 i + b_1\alpha i + b_2\alpha^2 i + b_3\alpha^3 i\right) \\
=&\sigma_6(a_0) + \sigma_6(a_1\alpha) + \sigma_6(a_2\alpha^2) + \sigma_6(a_3\alpha^3) + \sigma_6(b_0 i) + \sigma_6(b_1\alpha i) + \sigma_6(b_2\alpha^2 i) + \sigma_6(b_3\alpha^3 i) \\
=&\, a_0 + a_1\alpha i - a_2\alpha^2 - a_3\alpha^3 i - b_0 i + b_1\alpha + b_2\alpha^2 i - b_3\alpha^3.
\end{aligned}$$

In particular, $\sigma_1 = \mathrm{id}$.

Therefore,

$$\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7, \sigma_8\}. \tag{1}$$

Now take $\sigma = \sigma_2, \tau = \sigma_5$. Then

$$\sigma_1 = \sigma^4 = \tau^2 = \mathrm{id}, \quad \sigma_3 = \sigma^2, \quad \sigma_4 = \sigma^3, \quad \sigma_6 = \sigma\tau, \quad \sigma_7 = \sigma^2\tau, \quad \sigma_8 = \sigma^3\tau$$

and $\tau\sigma = \sigma^3\tau$.

Conventional we write "1" for σ_1 (the identity map). So

$$\begin{aligned}\mathrm{Gal}(K/\mathbb{Q}) =& \{1, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\} \\ =& \langle \sigma, \tau \rangle,\end{aligned} \tag{2}$$

where

$$o(\sigma) = 4, \quad o(\tau) = 2, \quad \tau\sigma = \sigma^3\tau. \tag{3}$$

Hence $\mathrm{Gal}((x^4-2)/\mathbb{Q}) = \mathrm{Gal}(K/\mathbb{Q}) \cong D_4$, the dihedral group (二面体群) of order 8, which is the transformation group of a square. In particular, the extension $K/\mathbb{Q}$ is not cyclic.

Let's investigate $\mathrm{Gal}((x^4-2)/\mathbb{Q})$ from another point of view. Note that σ_i permutes the conjugates of α and conjugates of i. Set four symbols:

$$\alpha = a_1, \quad i\alpha = a_2, \quad -\alpha = a_3, \quad -i\alpha = a_4.$$

We find

$$\sigma = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_3 & a_4 & a_1 \end{pmatrix}, \quad \tau = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_4 & a_3 & a_2 \end{pmatrix}.$$

In this way, we can regard $\sigma, \tau \in S_4$, the symmetric group over 4 symbols. In fact, we can write σ, τ as the disjoint product of cycles:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1234), \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (24).$$

It's clear

$$o((1234)) = 4, \ o((24)) = 2$$

and

$$(24) \cdot (1234) \cdot (24) = (1432) = (1234)^3.$$

This is essentially the relation in (3). So we have embedded $\mathrm{Gal}(x^4 - 2/\mathbb{Q})$ as a subgroup of S_4:

$$\begin{aligned}\mathrm{Gal}\left((x^4-2)/\mathbb{Q}\right) &\hookrightarrow S_4 \\ \sigma_2 = \sigma &\mapsto (1234) \\ \sigma_5 = \tau &\mapsto (24) \\ \sigma_3 = \sigma^2 &\mapsto (13)(24) \\ \sigma_4 = \sigma^3 &\mapsto (1432) \\ \sigma_6 = \sigma\tau &\mapsto (12)(34) \\ \sigma_7 = \sigma^2\tau &\mapsto (13) \\ \sigma_8 = \sigma^3\tau &\mapsto (14)(23) \\ \sigma_1 = \sigma^4 = \tau^2 &\mapsto 1.\end{aligned}$$

Exercises

1. Let $p_1, p_2, \ldots, p_n$ be distinct prime integers and $K = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n})$. Show that $K/\mathbb{Q}$ is an abelian extension.

2. Show that $\mathbb{Q}(\sqrt{-7}, \sqrt{23})$ is Galois and compute its Galois group. Is it an abelian extension?

3. Let F be a number field containing all n-th roots of unity and let K be a splitting field of $x^n - 2$. Show that K/F is a cyclic extension.

4. Let $f(x) = x^4 - 6$. Compute the splitting field K of $f(x)$ and the Galois group of the extension $K/\mathbb{Q}$. Is $K/\mathbb{Q}$ a cyclic extension?

5. Compute the Galois group of $f(x) = (x^2 + 5)(x^2 - 2023)$ over $\mathbb{Q}$.

6. Let p be an odd prime and ζ_p a p-th root of unity. Show that $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is a Galois extension and $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$, the multiplication group of the ring $\mathbb{Z}/p\mathbb{Z}$.

7. Let H/F be a Galois extension and K/F an finite extension.

   (a) Show that HK/K is a Galois extension.

   (b) Show that $H \subseteq K$ if and only if for all $\sigma \in \mathrm{Gal}(HK/K)$, $\sigma|_H = \mathrm{id}_H$.

8. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 4 with exactly 2 real roots. Show that the Galois group of $f(x)$ over $\mathbb{Q}$ is either S_4 or the dihedral group D_4 of order 8.

9. Let p be a prime number and let $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree p. Suppose that $f(x)$ is irreducible over $\mathbb{Q}$ and has exactly $p - 2$ real roots. Show that the Galois group of $f(x)$ over $\mathbb{Q}$ is isomorphic to the symmetric group S_p. (Hint: S_n is generated by (12) and $(12\cdots n)$.)

10. Let F be a field of characteristic $p > 0$, and let $f(x) = x^p - x + c \in F[x]$.

    (a) Prove that if α is a root of $f(x)$ in some extension field, then so is $\alpha + 1$.

    (b) Let K be the splitting field of $f(x)$ over F. Show that either $[K : F] = 1$ and $f(x)$ splits completely over F, or $[K : F] = p$ and $f(x)$ is irreducible over F.

Homework Exercise 21(1), 22, 24 on page 244. Exercise 16(1)(2)(3), 18 on page 316-317.