Fields Galios Modules

Gudfit

Contents

0
Field Extensions

We have previously established that a field is a commutative ring F with unity $1 \neq 0$ in which every non-zero element is a unit. In this chapter, we explore the structural relationship between fields, a subject known as field theory. This theory is fundamentally the study of equations: specifically, whether the roots of a polynomial exist within a given field or require a larger structure to contain them.

These notes assume that you have some experience with Matrices, Groups, and Rings or bareminimum read my previous notes.

0.1 *Fundamental Concepts*

Definition 0.1. ***Field Extension.***
Let F be a subfield of a field K. We call K a **field extension** of F, denoted by K/F (read as "K over F").

定義

The structure of a field is rigidly constrained by its smallest subfield.

Remark.

Recall that for any field F, there is a unique ring homomorphism $\psi : \mathbb{Z} \to F$ defined by $n \mapsto n \cdot 1_F$. The kernel of this map characterizes the field.

1. If $\ker \psi = \{0\}$, then ψ extends to a monomorphism $\mathbb{Q} \hookrightarrow F$. Thus, F contains a copy of the rational numbers $\mathbb{Q}$. In this case, we say F has **characteristic 0**. A **number field** is a finite extension of $\mathbb{Q}$ (equivalently, a subfield of $\mathbb{C}$ of finite degree over $\mathbb{Q}$).
2. If $\ker \psi = p\mathbb{Z}$ for a prime p, then ψ induces an embedding $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z} \hookrightarrow F$. Here, F has **characteristic** p. If F is finite, it is called a **finite field**.

We may construct extensions by adjoining indeterminates.

Example 0.1. Rational Function Field. Let F be a field and x an indeterminate. The **rational function field** $F(x)$ is defined as the field of fractions of the polynomial ring $F[x]$. Its elements are formal

fractions:

$$F(x) = \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in F[x], g(x) \neq 0 \right\}.$$

$F(x)$ is a field extension of F.

範例

0.2 *Algebraic and Transcendental Elements*

Let K/F be a field extension and let $\alpha \in K$. We denote by $F(\alpha)$ the smallest subfield of K containing both F and α. More generally, for a subset $S \subset K$, $F(S)$ denotes the subfield generated by F and S.
To understand the structure of $F(\alpha)$, we analyse the relationship between α and the polynomials in $F[x]$. Consider the evaluation homomorphism:

$$\varphi_\alpha : F[x] \to K, \quad g(x) \mapsto g(\alpha).$$

The image of this map is the subring $F[\alpha] = \{g(\alpha) \mid g(x) \in F[x]\} \subseteq K$. Since K is a field (and thus an integral domain), the kernel $\ker \varphi_\alpha$ is a prime ideal of the principal ideal domain $F[x]$. This leads to a dichotomy comprising two distinct cases.

Definition 0.2. ***Algebraic and Transcendental Elements.***
Let K/F be an extension and $\alpha \in K$.

1. α is **transcendental** over F if $\ker \varphi_\alpha = \{0\}$. That is, $f(\alpha) \neq 0$ for all non-zero polynomials $f(x) \in F[x]$.
2. α is **algebraic** over F if $\ker \varphi_\alpha \neq \{0\}$. That is, there exists a non-zero polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$.

定義

Example 0.2. Elements in $\mathbb{C}/\mathbb{Q}$. Consider $K = \mathbb{C}$ and $F = \mathbb{Q}$.

- The element $\sqrt{2}$ is algebraic over $\mathbb{Q}$ because it is a root of $x^2 - 2 \in \mathbb{Q}[x]$.
- The elements π and e are transcendental over $\mathbb{Q}$ (though the proofs are non-trivial).

範例

The classification of the element α determines the algebraic structure of the extension $F(\alpha)$.

Proposition 0.1. ***Structure of Simple Extensions.***
Let K/F be a field extension and $\alpha \in K$.

1. If α is transcendental over F, then $F(\alpha)$ is isomorphic to the rational function field $F(x)$.
2. If α is algebraic over F, then there exists a unique monic irreducible

polynomial $m(x) \in F[x]$ such that

$$F(\alpha) = F[\alpha] \cong F[x]/(m(x)).$$

命題

Case (i): Transcendental.

If $\ker \varphi_\alpha = \{0\}$, the map φ_α is a monomorphism from $F[x]$ into K. This extends naturally to the field of fractions $F(x)$:

$$\tilde{\varphi} : F(x) \to K, \quad \frac{g(x)}{h(x)} \mapsto \frac{g(\alpha)}{h(\alpha)}.$$

The image of this extended map is precisely $F(\alpha)$. Thus $F(x) \cong F(\alpha)$.

証明終

Case (ii): Algebraic.

If $\ker \varphi_\alpha \neq \{0\}$, then $\ker \varphi_\alpha$ is generated by a single monic polynomial $m(x)$ because $F[x]$ is a principal ideal domain. Since $\operatorname{im} \varphi_\alpha \subset K$ is an integral domain, the ideal $(m(x))$ is prime, which in $F[x]$ implies $m(x)$ is irreducible. By the Fundamental Homomorphism Theorem for rings, we have an isomorphism:

$$F[x]/(m(x)) \xrightarrow{\sim} \operatorname{im} \varphi_\alpha = F[\alpha].$$

Since $(m(x))$ is a maximal ideal (generated by an irreducible polynomial), the quotient $F[x]/(m(x))$ is a field. Therefore, the subring $F[\alpha]$ is already a field, implying $F(\alpha) = F[\alpha]$.

証明終

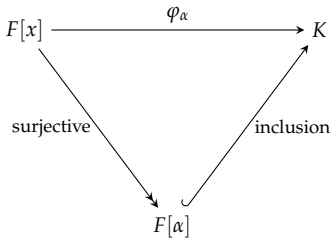


Figure 1: The evaluation homomorphism factors through the image $F[\alpha]$.

Definition 0.3. ***Minimal Polynomial.***
The monic irreducible polynomial $m(x)$ generating $\ker \varphi_\alpha$ in the algebraic case is called the **minimal polynomial** of α over F. Any polynomial $g(x) \in F[x]$ such that $g(\alpha) = 0$ is called a **vanishing polynomial** for α.

定義

Proposition 0.2. ***Divisibility of Vanishing Polynomials.***
Let α be algebraic over F with minimal polynomial $m(x)$. If $g(x) \in F[x]$ is any vanishing polynomial for α (i.e., $g(\alpha) = 0$), then $m(x)$ divides $g(x)$.

命題

Proof

By the division algorithm in $F[x]$, we can write

$$g(x) = q(x)m(x) + r(x), \quad \text{where } r(x) = 0 \text{ or } \deg r < \deg m.$$

Evaluating at α, we obtain:

$$g(\alpha) = q(\alpha)m(\alpha) + r(\alpha) \implies 0 = q(\alpha) \cdot 0 + r(\alpha).$$

Thus $r(\alpha) = 0$. Since $m(x)$ is the polynomial of least degree vanishing at α, the remainder $r(x)$ must be the zero polynomial.

■

We classify extensions based on the nature of their elements.

Definition 0.4. ***Types of Extensions.***
Let K/F be a field extension.

1. K/F is an **algebraic extension** if every element $\alpha \in K$ is algebraic over F.
2. K/F is a **transcendental extension** if there exists at least one element in K that is transcendental over F.
3. K/F is a **finitely generated extension** if $K = F(\alpha_1, \ldots, \alpha_n)$ for some finite set of elements.
4. K/F is a **simple extension** if $K = F(\alpha)$ for a single element α.

定義

0.3 *Properties of Algebraic Extensions*

Since a field K containing a subfield F is closed under addition and scalar multiplication by elements of F, K naturally carries the structure of a vector space over F. The "size" of the extension can thus be measured by linear algebra.

Definition 0.5. ***Degree of Extension.***
Let K/F be a field extension. The **degree** of K over F, denoted $[K : F]$, is the dimension of K as a vector space over F:

$$[K : F] := \dim_F K.$$

- If $[K : F]$ is finite, K is a **finite extension**.
- If $[K : F]$ is infinite, K is an **infinite extension**.

定義

Proposition 0.3. ***Degree of Simple Algebraic Extensions.***
Let $K = F(\alpha)$ be a simple extension where α is algebraic over F. Let $m(x)$ be the minimal polynomial of α with $\deg m = n$. Then:

$$[F(\alpha) : F] = n.$$

Moreover, the set $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ forms a basis for $F(\alpha)$ over F.

命題

Proof

Recall from the structure of simple extensions that $F(\alpha) \cong F[x]/(m(x))$. Any element in the quotient ring is represented uniquely by a polynomial $r(x)$ of degree less than n (the remainder modulo $m(x)$). Thus, every element $\beta \in F(\alpha)$ can be written uniquely as:

$$\beta = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}, \quad c_i \in F.$$

This implies that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ spans $F(\alpha)$ and is linearly independent over F.

■

Conversely, if $[F(\alpha) : F]$ is finite, the elements $1, \alpha, \alpha^2, \ldots$ cannot be linearly independent indefinitely; thus satisfy a linear dependence relation, implying α is algebraic.
For a sequence of extensions, the degrees behave multiplicatively. This result is fundamental to counting arguments in Galois theory and constructibility problems.

Theorem 0.1. ***The Tower Law.***
Let $F \subseteq M \subseteq K$ be a tower of fields. Then:

$$[K : F] = [K : M] \cdot [M : F].$$

定理

Proof

Let $[K : M] = m$ and $[M : F] = n$. Let $\{\alpha_1, \ldots, \alpha_m\}$ be a basis for K over M, and let $\{\beta_1, \ldots, \beta_n\}$ be a basis for M over F. We claim that the set of products $\mathcal{B} = \{\alpha_i\beta_j \mid 1 \le i \le m, 1 \le j \le n\}$ is a basis for K over F.

Spanning: Let $\gamma \in K$. Since $\{\alpha_i\}$ spans K over M, we can write $\gamma = \sum_{i=1}^{m} \lambda_i\alpha_i$ with $\lambda_i \in M$. Since $\{\beta_j\}$ spans M over F, each $\lambda_i = \sum_{j=1}^{n} c_{ij}\beta_j$ with $c_{ij} \in F$. Substituting this back:

$$\gamma = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} c_{ij}\beta_j \right) \alpha_i = \sum_{i=1}^{m} \sum_{j=1}^{n} c_{ij}(\alpha_i\beta_j).$$

Thus $\mathcal{B}$ spans K over F.

Linear Independence: Suppose $\sum_{i,j} c_{ij}\alpha_i\beta_j = 0$ for $c_{ij} \in F$. Rearranging terms, we have:

$$\sum_{i=1}^{m} \left(\sum_{j=1}^{n} c_{ij}\beta_j \right) \alpha_i = 0.$$

The inner sums are elements of M. Since the α_i are linearly inde-

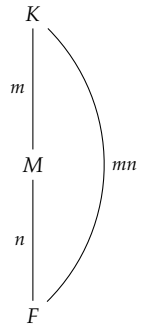


Figure 2: The degrees of a tower of fields multiply.

pendent over M, each coefficient must be zero:

$$\sum_{j=1}^{n} c_{ij}\beta_j = 0 \quad \text{for all } i.$$

Since the β_j are linearly independent over F, it follows that $c_{ij} = 0$ for all i, j.

Thus $[K : F] = mn$. The infinite case follows by a similar argument (if either sub-degree is infinite, the total degree is infinite).

■

This multiplicative property imposes strong arithmetic constraints on the degrees of elements.

Corollary 0.1. *Divisibility of Degrees.* Let K/F be a finite extension of degree n, and let $\alpha \in K$. Then the degree of the minimal polynomial of α over F divides n.

推論

Proof

Consider the tower $F \subseteq F(\alpha) \subseteq K$. By the Tower Law, $[K : F] = [K : F(\alpha)] \cdot [F(\alpha) : F]$. Thus $[F(\alpha) : F]$ divides $[K : F]$.

■

Corollary 0.2. *Prime Degree Extensions.* If $[K : F] = p$ where p is a prime number, then for any $\alpha \in K \setminus F$, $K = F(\alpha)$.

推論

Proof

Since $\alpha \notin F$, $[F(\alpha) : F] > 1$. Since $[F(\alpha) : F]$ divides the prime p, it must equal p. Thus $F(\alpha)$ is a subspace of K with the same dimension, so $F(\alpha) = K$.

■

We can now characterise finite extensions in terms of their generators.

Proposition 0.4. ***Finite vs Finitely Generated.***
A field extension K/F is finite if and only if it is a finitely generated algebraic extension.

命題

($\Longrightarrow$)

Let K/F be finite. Choose a basis $\{a_1, \ldots, a_n\}$. Then $K = F(a_1, \ldots, a_n)$. Since each $a_i \in K$, $[F(a_i) : F] \leq [K : F] < \infty$, so each a_i is algebraic.

証明終

($\Longleftarrow$)

Let $K = F(\alpha_1, \ldots, \alpha_n)$ where each α_i is algebraic over F. We proceed by induction on the tower of fields:

$$F_0 = F, \quad F_i = F_{i-1}(\alpha_i).$$

Since α_i is algebraic over F, it is algebraic over F_{i-1}. Thus $[F_i : F_{i-1}]$ is finite. By the Tower Law applied iteratively:

$$[K : F] = [F_n : F_{n-1}] \cdots [F_1 : F] < \infty.$$

証明終

Algebraic elements within an arbitrary extension form a coherent substructure.

Theorem 0.2. ***Closure of Algebraic Elements.***
Let K/F be an extension. The set $E = \{\alpha \in K \mid \alpha \text{ is algebraic over } F\}$ is a subfield of K.

定理

Proof

Let $\alpha, \beta \in E$. Then α and β are algebraic over F. The extension $F(\alpha, \beta)$ is finite over F (by the previous proposition). Consequently, any element generated by arithmetic operations on α and β (such as $\alpha \pm \beta$, $\alpha\beta$, α/β with $\beta \neq 0$) lies in $F(\alpha, \beta)$. Since $F(\alpha, \beta)$ is a finite extension, these elements are algebraic over F, and thus belong to E.

■

Theorem 0.3. ***Transitivity of Algebraicity.***
Let K be algebraic over M, and M be algebraic over F. Then K is algebraic over F.

定理

Proof

Let $\alpha \in K$. Since K/M is algebraic, α satisfies a polynomial equation with coefficients in M:

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0 = 0, \quad c_i \in M.$$

Let $M_0 = F(c_0, \ldots, c_{n-1})$. Since each c_i is algebraic over F, M_0/F is a finite extension. Since α is a root of a polynomial in $M_0[x]$, α is algebraic over M_0, so $[M_0(\alpha) : M_0]$ is finite. By the Tower Law, $[M_0(\alpha) : F] = [M_0(\alpha) : M_0][M_0 : F]$ is finite. Thus α is algebraic over F.

■

0.4 *Field Homomorphisms and Isomorphisms*

The structural equivalence of fields is described by isomorphisms that preserve the base field.

Definition 0.6. *F-Isomorphism.*
Let K and K' be extensions of F. A field isomorphism $\varphi : K \to K'$ is an **F-isomorphism** if it fixes F pointwise, i.e., $\varphi(a) = a$ for all $a \in F$. If $K = K'$, such a map is called an **F-automorphism**.

定義

We denote the group of F-automorphisms of K by $\mathrm{Gal}(K/F)$ (even when K/F is not Galois).

Proposition 0.5. *Roots Map to Roots.*
Let $\varphi : K \to K'$ be an F-isomorphism. Let $f(x) \in F[x]$ be a polynomial. If $\alpha \in K$ is a root of $f(x)$, then $\varphi(\alpha) \in K'$ is also a root of $f(x)$.

命題

Proof

Let $f(x) = \sum a_i x^i$ with $a_i \in F$. Applying φ to the equation $f(\alpha) = 0$:

$$\varphi\left(\sum a_i \alpha^i\right) = \sum \varphi(a_i)\varphi(\alpha)^i = \sum a_i(\varphi(\alpha))^i = f(\varphi(\alpha)).$$

Since $\varphi(0) = 0$, we have $f(\varphi(\alpha)) = 0$.

■

Proposition 0.6. *Automorphism Bound.*
Let K/F be a finite field extension. Then

$$|\mathrm{Gal}(K/F)| \leq [K : F].$$

命題

Proof

By *proposition* 0.4, write $K = F(\alpha_1, \ldots, \alpha_m)$ and set $F_0 = F$, $F_i = F_{i-1}(\alpha_i)$. For each i, any F_{i-1}-automorphism of F_i is determined by the image of α_i, which must be a root of its minimal polynomial over F_{i-1}. Hence

$$|\mathrm{Gal}(F_i/F_{i-1})| \leq [F_i : F_{i-1}].$$

Restricting automorphisms from F_i to F_{i-1} gives a group homomorphism, so for each automorphism of F_{i-1} there are at most $[F_i : F_{i-1}]$ extensions to F_i. Therefore,

$$|\mathrm{Gal}(K/F)| \leq \prod_{i=1}^{m} [F_i : F_{i-1}] = [K : F]$$

by the Tower Law.

■

This property implies that algebraic structure is determined by the minimal polynomial.

Proposition 0.7. ***Uniqueness of Minimal Polynomials.***
Let α and β be algebraic elements over F. There exists an F-isomorphism $F(\alpha) \cong F(\beta)$ mapping $\alpha \mapsto \beta$ if and only if α and β have the same minimal polynomial over F.

命題

($\Longrightarrow$)
Let $\varphi : F(\alpha) \to F(\beta)$ be such an isomorphism. Let $m_\alpha(x)$ be the minimal polynomial of α. By the previous proposition, $\varphi(\alpha) = \beta$ must be a root of $m_\alpha(x)$. Thus the minimal polynomial of β, $m_\beta(x)$, divides $m_\alpha(x)$. Considering φ^{-1}, we find $m_\alpha(x)$ divides $m_\beta(x)$.
Being monic, they are equal.

証明終

($\Longleftarrow$)
If $m_\alpha(x) = m_\beta(x) = m(x)$, we have the canonical isomorphisms:

$$F(\alpha) \cong F[x]/(m(x)) \cong F(\beta).$$

Composing these gives the desired map.

証明終

Splitting Fields and Normal Extensions

We have seen that if α, β are roots of the same irreducible polynomial, the fields $F(\alpha)$ and $F(\beta)$ are isomorphic. The detailed definitions, existence, and uniqueness of splitting fields as well as the normality characterisation are developed in Chapter 2. Here we only recall that a normal extension is, by definition, one that contains all the conjugates of its elements, so it can be realised as the splitting field of those minimal polynomials; see *definition* 2.8.
While splitting fields ensure all roots exist, we must also determine if they are distinct.

Definition 0.7. ***Formal Derivative.***
Let $f(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$. The **formal derivative** is the polynomial $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$.

定義

Proposition 0.8. ***Criterion for Multiple Roots.***
A non-zero polynomial $f(x) \in F[x]$ has a multiple root in some ex-

tension if and only if $f(x)$ and $f'(x)$ have a non-constant common factor.

命題

Proof

Let E be a field in which f splits. Suppose f has a multiple root $\alpha \in E$. Then

$$f(x) = (x-\alpha)^m q(x), \quad m \geq 2,\ q(\alpha) \neq 0.$$

Differentiating,

$$f'(x) = m(x-\alpha)^{m-1}q(x) + (x-\alpha)^m q'(x),$$

so $f'(\alpha) = 0$. Hence $x - \alpha$ divides both f and f' in $E[x]$, so their gcd is non-constant.
Conversely, if $\gcd(f, f')$ is non-constant, then in a splitting field E for f there exists $\alpha \in E$ with $f(\alpha) = f'(\alpha) = 0$. Write $f(x) = (x-\alpha)^m q(x)$ with $m \geq 1$ and $q(\alpha) \neq 0$. From the expression for $f'(x)$ above, $f'(\alpha) = 0$ forces $m \geq 2$. Thus α is a multiple root of f.

■

Separability Proof

If α is a multiple root, $f(x) = (x-\alpha)^2 g(x)$. Differentiating shows $f'(\alpha) = 0$, so $x - \alpha$ divides both. Conversely, if $\gcd(f, f') \neq 1$, they share a root in a splitting field, which must be a multiple root of f.

■

Definition 0.8. ***Separability.***
An irreducible polynomial $f(x) \in F[x]$ is **separable** if it has no multiple roots in its splitting field. An extension K/F is **separable** if the minimal polynomial of every element in K is separable.

定義

Remark.

In characteristic 0, every irreducible polynomial is separable since $f'(x)$ has strictly lower degree and cannot be zero. In characteristic p, $f'(x) = 0$ implies $f(x) = g(x^p)$, which leads to inseparable extensions.

Lemma 0.1. ***Artin–Schreier Translation.***
Let F be a field of characteristic $p > 0$ and let $c \in F$. For any $a \in \mathbb{F}_p$,

$$(x+a)^p - (x+a) - c = x^p - x - c.$$

If α is a root of $x^p - x - c$ in some extension, then $\alpha + a$ is also a root for all $a \in \mathbb{F}_p$. Hence if $x^p - x - c$ has a root in F, it splits in $F[x]$. If it has no root in F, then it is irreducible.

引理

Proof

The identity follows from $(x+a)^p = x^p + a^p = x^p + a$. If α is a root, then $\alpha + a$ is a root for each $a \in \mathbb{F}_p$, and these p roots are distinct. Let $m(x)$ be the minimal polynomial of α over F. Then $m(x)$ divides $x^p - x - c$ and has at least p roots, so $\deg m \geq p$. Since $\deg(x^p - x - c) = p$, either $\deg m = 1$ and $\alpha \in F$, or $\deg m = p$ and $x^p - x - c$ is irreducible.

■

0.5 *Algebraic Closure*

We conclude this chapter by asking whether we can find a field containing all possible roots of all polynomials.

Definition 0.9. ***Algebraic Closure.***
A field K is **algebraically closed** if every non-constant polynomial in $K[x]$ splits into linear factors (i.e., has roots in K). An extension $\bar{F}/F$ is called an **algebraic closure** of F if $\bar{F}$ is algebraic over F and $\bar{F}$ is algebraically closed.

定義

Before proving the existence of such a field, we establish that we can always adjoin a root of a single polynomial.

Lemma 0.2. ***Kronecker's Theorem.***
Let F be a field and $f(x) \in F[x]$ be a non-constant polynomial. There exists an extension E/F in which $f(x)$ has a root.

引理

Proof

Let $p(x)$ be an irreducible factor of $f(x)$. The quotient ring $E = F[x]/(p(x))$ is a field extension of F. The element $\bar{x} = x + (p(x)) \in E$ is a root of $p(x)$, and hence of $f(x)$.

■

We now generalise this to all polynomials simultaneously using a construction due to E. Artin.

Theorem 0.4. ***Existence of Algebraic Closure.***
Every field F has an algebraic closure.

定理

First we construct a field containing roots for every polynomial in $F[x]$ simultaneously. For every non-constant polynomial $f \in F[x]$, introduce a distinct indeterminate X_f. Let

$$S = \{X_f \mid f \in F[x], \deg f \geq 1\}.$$

Consider the polynomial ring $R = F[S]$ generated by these variables. Let I be the ideal in R generated by the polynomials $f(X_f)$ for all f.

Claim 0.1. . The ideal I is proper (i.e., $1 \notin I$).

主張

Proof

Suppose for contradiction that $1 \in I$. Then there exists a finite sum

$$1 = \sum_{i=1}^{n} g_i \cdot f_i(X_{f_i}), \quad g_i \in R.$$

This relation involves only finitely many polynomials $f_1, \ldots, f_n$. By iteratively applying Kronecker's Theorem, we can construct a finite extension E/F containing roots $\alpha_1, \ldots, \alpha_n$ for these specific polynomials. Evaluate the polynomial relation in E by assigning $X_{f_i} \mapsto \alpha_i$ (and other variables arbitrarily). The right-hand side becomes 0 (since $f_i(\alpha_i) = 0$), while the left-hand side remains 1. Thus $1 = 0$, a contradiction.

■

Proof of theorem 0.4

Since I is proper, it is contained in a maximal ideal $\mathfrak{m}$ (by Zorn's Lemma). The quotient $K_1 = R/\mathfrak{m}$ is a field extension of F in which every polynomial $f \in F[x]$ has at least one root (the image of X_f). However, K_1 might not be algebraically closed, as it may not contain roots for polynomials in $K_1[x]$. We iterate this process to form a chain $F \subseteq K_1 \subseteq K_2 \subseteq \ldots$.
Let

$$\bar{F} = \bigcup_{n=1}^{\infty} K_n.$$

Any polynomial in $\bar{F}[x]$ has coefficients in some K_n, hence has a root in $K_{n+1} \subset \bar{F}$. Thus $\bar{F}$ is algebraically closed. Each K_n is algebraic over F, so every element of $\bar{F}$ is algebraic over F. Hence $\bar{F}$ is an algebraic closure of F.

■

Theorem 0.5. ***Uniqueness of Algebraic Closure.***
Let $\bar{F}_1$ and $\bar{F}_2$ be two algebraic closures of F. Then there exists an F-isomorphism $\bar{F}_1 \cong \bar{F}_2$.

定理

Proof

The proof relies on Zorn's Lemma to extend the identity map on F to a maximal isomorphism between subfields of $\bar{F}_1$ and $\bar{F}_2$. Since both are algebraic extensions, this maximal isomorphism must

cover the entirety of the fields. ■

0.6 Exercises

1. **Odd Degree Algebraic Elements.** Let K/F be a field extension and let $u \in K$ be an algebraic element over F of odd degree (i.e., $[F(u) : F]$ is odd). Prove that $F(u) = F(u^2)$.

   Consider the inclusion $K(u^2) \subseteq K(u)$ and use the Tower Law with degrees.

2. **Cyclotomic Degrees.** Let $\zeta_n = e^{2\pi i/n}$ be a primitive n-th root of unity. Define the cyclotomic degree by

$$\Phi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}].$$

   Show $\mathbb{Q}(\zeta_{mn}) = \mathbb{Q}(\zeta_m, \zeta_n)$ and use the Tower Law; reduce to prime powers.

   (a) Prove that $\Phi(mn) = \Phi(m)\Phi(n)$ when $\gcd(m, n) = 1$.
   (b) Prove that $\Phi(p^k) = p^{k-1}(p-1)$ for prime p and $k \geq 1$.
   (c) Compute $\Phi(p)$ for prime p and $\Phi(8)$.
   (d) Deduce a general formula for $\Phi(n)$ in terms of the prime factorisation of n.

3. **Minimal Polynomials in Towers.** Determine the minimal polynomial of the element $\alpha = \sqrt{2} + \sqrt{3}$ over the field K in the following cases:

   (a) $K = \mathbb{Q}$
   (b) $K = \mathbb{Q}(\sqrt{2})$
   (c) $K = \mathbb{Q}(\sqrt{6})$

4. **Simple Extension Generator.** Prove explicitly that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

5. **Intermediate Domains.** Let K/F be an algebraic field extension. Let D be an integral domain such that $F \subseteq D \subseteq K$. Prove that D is a field.

6. **Minimal Polynomial Uniqueness.** Let u be algebraic over a field F.

   (a) Prove that the minimal polynomial $m(x)$ generates the ideal $I_u = \{g(x) \in F[x] \mid g(u) = 0\}$.
   (b) Conversely, prove that if $f(x)$ is a monic irreducible polynomial in $F[x]$ such that $f(u) = 0$, then $f(x)$ is the minimal polynomial of u.

7. **Algebraicity via Powers.** Let K/F be a field extension and let $a \in K$. Suppose that $a \in F(a^m)$ for some integer $m > 1$. Prove that a is algebraic over F.

8. **Transcendental Rational Functions.** Let $K(x_1, \ldots, x_n)$ be the field

of fractions of the polynomial ring $K[x_1, \ldots, x_n]$. Prove that any element $u \in K(x_1, \ldots, x_n)$ such that $u \notin K$ is transcendental over K.

9. **Inverting Transcendental Extensions.** Let K be a field and $u \in K(x)$ such that $u \notin K$. Prove that x is algebraic over the field $K(u)$.

10. **Computation in Cubic Fields.** Let $K = \mathbb{Q}(\alpha)$ where α is a root of $x^3 - x - 1 = 0$. Find the minimal polynomial of $\gamma = 1 + \alpha^2$ over $\mathbb{Q}$.

11. **Biquadratic Extensions.** Let a be a positive rational number that is not a square in $\mathbb{Q}$. Prove that $[\mathbb{Q}(\sqrt[4]{a}) : \mathbb{Q}] = 4$.

Establish the irreducibility of $x^4 - a$.

12. **Field Arithmetic.** Let u be a root of $x^3 - 6x^2 + 9x + 3$.

    (a) Prove that $[\mathbb{Q}(u) : \mathbb{Q}] = 3$.
    (b) Express u^4, $(u+1)^{-1}$, and $(u^2 - 6u + 8)^{-1}$ as linear combinations $a + bu + cu^2$ with rational coefficients.

13. **Rational Function Example.** Let x be transcendental over $\mathbb{Q}$ and let $u = \frac{x^3}{x+1}$. Calculate the degree $[\mathbb{Q}(x) : \mathbb{Q}(u)]$.

14. **Constructing Finite Fields.** Find a quadratic irreducible polynomial $f(x)$ over the binary field $\mathbb{F}_2$. Let u be a root of $f(x)$. List all elements of the field $\mathbb{F}_2(u)$ and construct their addition and multiplication tables.

15. **Composite Extensions.** Let M/K be a field extension containing algebraic elements u and v with degrees $m = [K(u) : K]$ and $n = [K(v) : K]$. Let $F = K(u)$ and $E = K(v)$.

    (a) Prove that $[FE : K] \leq mn$.
    (b) Prove that if $\gcd(m, n) = 1$, then $[FE : K] = mn$.

16. **Artin-Schreier Extensions.** Let F be a field of characteristic $p > 0$ and let $c \in F$.

    (a) Prove that the polynomial $x^p - x - c$ is irreducible in $F[x]$ if and only if it has no root in F.
    (b) Does this conclusion hold if $\text{char}(F) = 0$? Justify your answer.

17. **Quadratic Extensions.** Let F be a field of characteristic not equal to 2. Prove that every extension of degree 2 over F is of the form $F(\sqrt{a})$ for some $a \in F$. Does this classification hold if $\text{char}(F) = 2$?

18. **Automorphisms of a Quadratic Field.** Let $K = \mathbb{Q}(\sqrt{5})$. List all $\mathbb{Q}$-automorphisms of K and verify that $|\text{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}]$. Then explain why Proposition 0.6 immediately implies $|\text{Gal}(K/\mathbb{Q})| \leq [K : \mathbb{Q}]$ for every simple algebraic extension.

1
Applications of Field Theory

We now apply our knowledge of field extensions to a classical problem originating from Greek antiquity: which geometric constructions are possible using only a straightedge (an unmarked ruler) and a compass? To answer this, we must translate geometric operations into the language of algebra.

Definition 1.1. ***Constructible Points and Numbers.***
Let $P_0 = \{(0,0),(1,0)\} \subset \mathbb{R}^2$ be a set of initial points. A point (x,y) is **constructible** if it can be obtained from P_0 by a finite sequence of the following operations:

1. Drawing a line through two already constructed points.
2. Drawing a circle centred at a constructed point and passing through another constructed point.
3. Finding the intersection points of two lines, two circles, or a line and a circle constructed as above.

A real number α is a **constructible number** if the point $(\alpha,0)$ is constructible.

定義

To relate these geometric operations to field theory, we first establish that the elementary tools of geometry allow us to perform basic arithmetic on lengths.

Lemma 1.1. ***Geometric Subroutines.***
Given constructible points and lines, the following constructions are possible:

Perpendiculars: Given a line l and a point A (either on l or not), one can construct a line through A perpendicular to l.

Parallels: Given a line l and a point $A \notin l$, one can construct a line through A parallel to l.

Length Transfer: Given a point B on a line l and a constructible segment OA, one can construct a point C on l such that $|BC| = |OA|$.

引理

Proof

Perpendiculars: If $A \in l$, choose any other point $B \in l$. Draw the circle $C_1(A, B)$ (centre A, through B) intersecting l at C. Draw circles $C_2(B, C)$ and $C_3(C, B)$; their intersection determines a point D. The line AD is perpendicular to l. If $A \notin l$, draw a circle centred at A intersecting l at B and C. The perpendicular bisector of BC (constructed as above) passes through A.

Parallels: Construct a line l_0 through A perpendicular to l. Then construct a line l' through A perpendicular to l_0. Clearly $l' \parallel l$.

Length Transfer: This follows from constructing a parallelogram or by repeated application of circles if the target line is aligned with the segment.

■

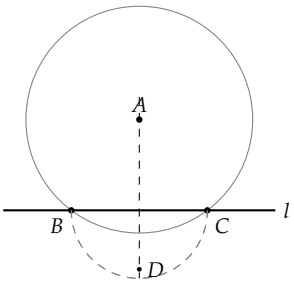


Figure 1.1: Dropping a perpendicular from $A \notin l$.

Intercept Theorem: in similar triangles, ratios of corresponding sides are equal. Geometric mean theorem: in a right triangle, the altitude to the hypotenuse has length squared equal to the product of the hypotenuse segments.

Proposition 1.1. ***The Field of Constructible Numbers.***
The set $\mathcal{K}$ of all constructible real numbers is a subfield of $\mathbb{R}$ closed under square roots of non-negative elements. That is:

1. If $\alpha, \beta \in \mathcal{K}$, then $\alpha \pm \beta \in \mathcal{K}$, $\alpha\beta \in \mathcal{K}$, and (if $\beta \neq 0$) $\alpha/\beta \in \mathcal{K}$.
2. If $\alpha \in \mathcal{K}$ and $\alpha > 0$, then $\sqrt{\alpha} \in \mathcal{K}$.

命題

Proof

The lengths 0 and 1 are given. Addition $\alpha + \beta$ and subtraction $\alpha - \beta$ correspond to extending a segment on a line. For multiplication and division, we use the Intercept Theorem (Thales' Theorem). To construct $\gamma = \alpha\beta$, construct a triangle with sides 1 and α. On the side of length 1, extend to length β. Draw a parallel line to scale the side α to γ. A similar construction yields α/β.
For the square root, construct a segment of length $1 + \alpha$. Draw a semicircle with this segment as the diameter. The perpendicular erected at the point joining the segments 1 and α meets the circle at a height h. By elementary geometry (geometric mean), $h^2 = 1 \cdot \alpha$, so $h = \sqrt{\alpha}$.

■

We now characterise these numbers algebraically. Every construction step involves intersecting lines and circles.

Lemma 1.2. ***Algebraic Characterisation of Steps.***
Let K be a subfield of $\mathbb{R}$. Let $A_1, \ldots, A_4$ be points with coordinates in K.

1. The intersection of two lines through these points has coordinates in K.

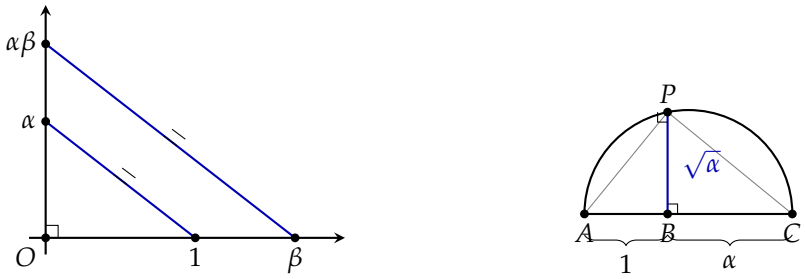


Figure 1.2: Left: Constructing the product $\alpha\beta$ via similar triangles. Right: Constructing $\sqrt{\alpha}$ using the geometric mean theorem ($BP^2 = AB \cdot BC$).

2. The intersection of a line and a circle (or two circles) defined by these points has coordinates in $K(\sqrt{r})$ for some $r \in K$, where $r \geq 0$.

引理

Proof

A line through points in K has an equation of the form $ax + by + c = 0$ with $a, b, c \in K$. The intersection of two such lines is the solution to a linear system over K, which lies in K. A circle with centre $(x_0, y_0) \in K^2$ and radius squared $R^2 \in K$ has the equation $(x - x_0)^2 + (y - y_0)^2 = R^2$. The intersection of a line and a circle requires substituting linear $y = mx + c$ into the quadratic circle equation, yielding a quadratic equation in x. The roots lie in $K(\sqrt{\Delta})$ where Δ is the discriminant. The intersection of two circles $x^2 + y^2 + D_1 x + \cdots = 0$ and $x^2 + y^2 + D_2 x + \cdots = 0$ can be found by subtracting the equations to get a linear relationship (the radical axis), reducing the problem to the line-circle case.

■

This leads to the fundamental theorem of constructibility.

Theorem 1.1. ***Constructible Numbers and Field Extensions.***
A real number α is constructible if and only if there exists a finite tower of subfields

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = K$$

such that $\alpha \in K$, and for each i, $F_{i+1} = F_i(\sqrt{r_i})$ for some $r_i \in F_i$ with $r_i > 0$.

定理

Proof

The forward direction follows immediately from the previous lemma: each construction step either leaves the field unchanged (linear intersection) or extends it by a square root (quadratic intersection). Conversely, since $\mathbb{Q}$ constructible (contains $0, 1$ and is closed under arithmetic), and square roots of constructible numbers are constructible (*figure* 1.2), any element in such a tower can be constructed.

■

Corollary 1.1. *Degree of Constructible Numbers.* If α is a constructible number, then α is algebraic over $\mathbb{Q}$ and its degree $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is a power of 2.

推論

Proof

Let K be the top field in the tower from the theorem. By the Tower Law (*figure 2*), $[K : \mathbb{Q}] = [K : F_{n-1}] \cdots [F_1 : \mathbb{Q}] = 2^n$. Since $\mathbb{Q}(\alpha) \subseteq K$, the degree $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ must divide $[K : \mathbb{Q}] = 2^n$. Thus it must be a power of 2.

■

This corollary allows us to prove the impossibility of several famous constructions sought by ancient geometers.

Corollary 1.2. *Impossibility of Angle Trisection.* It is impossible to trisect an arbitrary angle using only a straightedge and compass. Specifically, the angle 60° cannot be trisected.

推論

Proof

To trisect 60°, we would need to construct 20°, which implies constructing $\alpha = \cos 20^\circ$. Recall the triple angle formula:

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta.$$

Setting $\theta = 20^\circ$, we have $\cos 60^\circ = 1/2$. Let $x = \cos 20^\circ$. Then:

$$\frac{1}{2} = 4x^3 - 3x \implies 8x^3 - 6x - 1 = 0.$$

The polynomial $P(x) = 8x^3 - 6x - 1$ is irreducible over $\mathbb{Q}$ (a change of variable $y = 2x$ gives $y^3 - 3y - 1$, roots are ± 1 test fails). Thus $[\mathbb{Q}(\cos 20^\circ) : \mathbb{Q}] = 3$. Since 3 is not a power of 2, $\cos 20^\circ$ is not constructible.

■

Corollary 1.3. *Constructibility of Regular Polygons.* A regular p-gon (where p is prime) is constructible if and only if p is a **Fermat prime**, i.e., $p = 2^{2^k} + 1$.

推論

Proof

The construction of a regular p-gon is equivalent to constructing the length $\cos(2\pi/p)$. Let $\zeta = e^{2\pi i/p}$. The field extension $\mathbb{Q}(\zeta)$ has degree $p - 1$ over $\mathbb{Q}$. The real subfield containing $\cos(2\pi/p)$ is $\mathbb{Q}(\zeta + \zeta^{-1})$, which has degree $(p - 1)/2$. For this to be con-

structible, $(p-1)/2$ must be a power of 2, so $p-1 = 2^m$. If m has an odd factor $s > 1$, say $m = s \cdot r$, then $2^m + 1 = (2^r)^s + 1$ is divisible by $2^r + 1$, so p would not be prime. Thus m must be a power of 2, making p a Fermat prime.

■

Remark.

The converse (that every Fermat prime yields a constructible regular p-gon) is Exercise 5.

1.1 *The Fundamental Theorem of Algebra*

We now establish a result that, while analytic in nature, underpins the structural completeness of the complex numbers: the Fundamental Theorem of Algebra. This theorem asserts that the field construction process terminates at $\mathbb{C}$; no further algebraic extensions are necessary to contain roots of polynomials.

Theorem 1.2. ***Fundamental Theorem of Algebra.***
Let $f(z) \in \mathbb{C}[z]$ be a polynomial of degree $n \geq 1$. Then there exists $z_0 \in \mathbb{C}$ such that $f(z_0) = 0$.

定理

The proof proceeds by contradiction. We assume $f(z)$ is never zero and exploit the topological properties of $\mathbb{C}$ (specifically, compactness and the continuous nature of the modulus function) to derive an impossibility. The argument requires two subsidiary lemmas: one guaranteeing that $|f(z)|$ attains a minimum, and another asserting that this minimum cannot be non-zero.

Lemma 1.3. ***Existence of a Minimum.***
Let $f(z) \in \mathbb{C}[z]$. The function $|f(z)|$ attains a global minimum on $\mathbb{C}$. That is, there exists $z_0 \in \mathbb{C}$ such that $|f(z_0)| \leq |f(z)|$ for all $z \in \mathbb{C}$.

引理

Proof

Let $f(z) = a_n z^n + \cdots + a_0$ with $a_n \neq 0$. We examine the behaviour of $f(z)$ for large $|z|$. Factoring out the leading term:

$$|f(z)| = |z|^n \left| a_n + \frac{a_{n-1}}{z} + \cdots + \frac{a_0}{z^n} \right|.$$

As $|z| \to \infty$, the term in parentheses approaches $|a_n| \neq 0$. Consequently, $\lim_{|z|\to\infty} |f(z)| = \infty$. Choose a radius $R > 0$ sufficiently large such that for all $|z| \geq R$, we have $|f(z)| > |f(0)|$. Consider the closed disk $D_R = \{z \in \mathbb{C} \mid |z| \leq R\}$. Since polynomial functions are continuous, $|f(z)|$ is a continuous real-valued func-

tion. Since D_R is a compact set (closed and bounded), the Extreme Value Theorem ensures that $|f(z)|$ attains a minimum on D_R at some point z_0. Since $0 \in D_R$, the minimum on the disk satisfies $|f(z_0)| \leq |f(0)|$. For any z outside the disk ($|z| > R$), our choice of R implies $|f(z)| > |f(0)| \geq |f(z_0)|$. Thus, z_0 is a global minimum for the entire plane.

■

Lemma 1.4. ***d'Alembert's Lemma.***
Let $f(z) \in \mathbb{C}[z]$ be a non-constant polynomial and let $z_0 \in \mathbb{C}$. If $f(z_0) \neq 0$, then $|f(z_0)|$ is not the minimum value of $|f(z)|$.

引理

Proof

We may shift the coordinate system to the origin by defining $g(z) = f(z + z_0)$. Clearly, if $|g(z)|$ is not minimal at $z = 0$, then $|f(z)|$ is not minimal at z_0. Furthermore, we may normalise the function. Let $h(z) = g(z)/g(0)$. Then $h(0) = 1$. It suffices to show that there exists a point z such that $|h(z)| < 1$. Since $h(z)$ is a polynomial with constant term 1, we can write it in the form:

$$h(z) = 1 + az^k + z^{k+1}\psi(z),$$

where $a \neq 0$ is the first non-zero coefficient after the constant term, $k \geq 1$ is an integer, and $\psi(z)$ is a polynomial. We wish to choose a small perturbation z such that the term az^k is real and negative, thereby reducing the modulus. Let $a = |a|e^{i\phi}$. We set $z = re^{i\theta}$ with $r > 0$. The term of interest becomes:

$$az^k = |a|r^k e^{i(\phi + k\theta)}.$$

To make this real and negative, we choose θ such that $\phi + k\theta = \pi$. That is, $\theta = \frac{\pi - \phi}{k}$. Substituting this back into $h(z)$, we have $az^k = -|a|r^k$, and thus:

$$h(z) = 1 - |a|r^k + z^{k+1}\psi(z).$$

By the triangle inequality:

$$|h(z)| \leq |1 - |a|r^k| + |z^{k+1}\psi(z)| = 1 - |a|r^k + r^{k+1}|\psi(z)|.$$

(Note that for sufficiently small r, $|a|r^k < 1$, allowing us to drop the absolute value on the first term). Since $\psi(z)$ is a polynomial, it is bounded in a neighbourhood of 0; let $|\psi(z)| \leq M$ for small $|z|$. Then:

$$|h(z)| \leq 1 - r^k(|a| - Mr).$$

Since $|a| > 0$, we can choose r sufficiently small such that $|a| - Mr > 0$. For such an r, $|h(z)| < 1$. Thus, the origin is not a local minimum of $|h(z)|$, implying z_0 is not a local minimum of $|f(z)|$. ■

Proof of theorem 1.2

By *lemma 1.3*, there exists a point $z_0 \in \mathbb{C}$ where $|f(z)|$ attains its global minimum. Suppose, for the sake of contradiction, that $f(z_0) \neq 0$. By *lemma 1.4*, z_0 cannot be a minimum, as there exists a nearby point with a strictly smaller modulus. This contradiction implies that our assumption must be false. Therefore, $f(z_0) = 0$. ■

Remark.

This theorem implies that the field $\mathbb{C}$ is **algebraically closed**. In the language of field theory, the algebraic closure of $\mathbb{R}$ is $\mathbb{C}$, and $[\mathbb{C} : \mathbb{R}] = 2$.

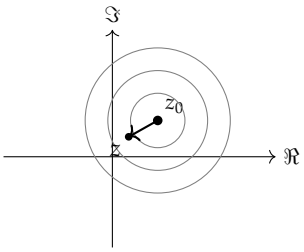


Figure 1.3: If $f(z_0) \neq 0$, there exists a direction in which $|f|$ decreases.

1.2 *Theory of Finite Fields*

We now turn our attention to fields with a finite number of elements, known as **Galois fields**. These structures are ubiquitous in number theory, coding theory, and cryptography. Their structure is exceptionally clean: they are completely classified by their order.

Definition 1.2. ***Characteristic and Order.***
Let K be a finite field. Since K is finite, it must have characteristic p for some prime p. Consequently, K contains a copy of $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ as its prime subfield. K is a vector space over $\mathbb{F}_p$. If $[K : \mathbb{F}_p] = n$, then $|K| = p^n$.

定義

Lemma 1.5. ***Order of Finite Fields.***
The order of any finite field is a prime power $q = p^n$.

引理

Example 1.1. A Field of Order 4. Consider the polynomial $f(x) = x^2 + x + 1$ over $\mathbb{F}_2$. Since $f(0) = 1$ and $f(1) = 1$, it has no roots in $\mathbb{F}_2$. Being of degree 2, it is irreducible. The quotient ring $K = \mathbb{F}_2[x]/(x^2 + x + 1)$ is a field. Its elements are $\{0, 1, \alpha, \alpha + 1\}$, where α is the image of x. Note that $\alpha^2 = \alpha + 1$ (since $-1 = 1$ in characteristic 2).

範例

The following theorem provides a complete structural description of all finite fields.

Theorem 1.3. ***Classification of Finite Fields.***
Let p be a prime and $q = p^n$ for some $n \geq 1$.

Existence: There exists a field of order q, unique up to isomorphism. We denote this field by $\mathbb{F}_q$.

Subfield Structure: A field of order p^n contains a subfield of order p^k if and only if k divides n.

Cyclic Multiplicative Group: The multiplicative group $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$ is cyclic of order $q-1$.

Root Structure: The elements of $\mathbb{F}_q$ are precisely the roots of the polynomial $x^q - x$. In the algebraic closure $\overline{\mathbb{F}}_p$, we have:

$$\mathbb{F}_q = \{\alpha \in \overline{\mathbb{F}}_p \mid \alpha^q = \alpha\}.$$

Polynomial Factorisation: The polynomial $x^{p^n} - x$ factors over $\mathbb{F}_p$ as the product of all monic irreducible polynomials in $\mathbb{F}_p[x]$ whose degrees divide n.

定理

Freshman's Dream: in characteristic p, $(a+b)^p = a^p + b^p$. Iterating gives $(a+b)^{p^n} = a^{p^n} + b^{p^n}$.

Existence and Uniqueness.

Consider the polynomial $f(x) = x^q - x$ in $\mathbb{F}_p[x]$. By *theorem* 0.4, let Ω be an algebraic closure of $\mathbb{F}_p$. Since Ω is algebraically closed, $f(x)$ splits completely in Ω.
The derivative is $f'(x) = qx^{q-1} - 1 = -1$ (since $q = p^n \equiv 0 \pmod{p}$). Since the derivative is nowhere zero, $f(x)$ has no repeated roots. Thus $f(x)$ has exactly q distinct roots in Ω. Let

$$S = \{\alpha \in \Omega \mid \alpha^q = \alpha\}.$$

We claim S is a field.

- Closure under multiplication: $(\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta$.
- Closure under addition: $(\alpha+\beta)^q = \alpha^q + \beta^q = \alpha + \beta$. (Recall the "Freshman's Dream" $(a+b)^p = a^p + b^p$ in characteristic p, iterated n times).
- Inverses: $(\alpha^{-1})^q = (\alpha^q)^{-1} = \alpha^{-1}$.

Thus S is a subfield of Ω with q elements. So a field of order q exists.
For uniqueness, let K be any field of order q. The multiplicative group $K^\times$ has order $q-1$, so $\alpha^{q-1} = 1$ for all $\alpha \in K^\times$. Thus $\alpha^q = \alpha$ for all $\alpha \in K$. This means every element of K is a root of $x^q - x$. Since K contains q roots and $x^q - x$ can have at most q roots, K is precisely the set of roots of $x^q - x$. If we embed K into Ω, its image must be exactly S. Thus $K \cong S$.

証明終

Subfields.

$\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^n}$ corresponds to the set of roots of $x^{p^k} - x$ being contained in the set of roots of $x^{p^n} - x$ inside $\overline{\mathbb{F}}_p$. If $k \mid n$, then for any α with $\alpha^{p^k} = \alpha$, we have $\alpha^{p^n} = (\alpha^{p^k})^{p^{n-k}} = \alpha$, so every root of $x^{p^k} - x$ is a root of $x^{p^n} - x$, hence $x^{p^k} - x \mid x^{p^n} - x$ in $\mathbb{F}_p[x]$. Conversely, if $x^{p^k} - x \mid x^{p^n} - x$, then every root of $x^{p^k} - x$ lies in $\mathbb{F}_{p^n}$, so $\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^n}$, which forces $k \mid n$ by the tower law.

証明終

Lemma 1.6. ***Finite Subgroups of Fields.***
Let G be a finite subgroup of the multiplicative group of a field F. Then G is cyclic.

引理

Proof

Let G have order N. Since G is a finite abelian group, $G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ with $n_1 \mid n_2 \mid \cdots \mid n_k$. The exponent of this group is n_k. Thus $x^{n_k} = 1$ for all $x \in G$. The polynomial $x^{n_k} - 1$ has at most n_k roots in the field F. Since all N elements of G are roots, we must have $N \leq n_k$. However, $N = n_1 \cdots n_k$, so clearly $N \geq n_k$. Thus $N = n_k$, implying $k = 1$ and $G \cong \mathbb{Z}_N$.

■

Cyclic Group.

This relies on a general fact about finite subgroups of fields. Applying this to $G = \mathbb{F}_q^\times$, we see it is cyclic.

証明終

Factorisation.

Divide the polynomial $x^q - x$ by its irreducible factors in $\mathbb{F}_p[x]$. An irreducible $g(x)$ of degree d divides $x^q - x$ iff its roots lie in $\mathbb{F}_q$. The field $\mathbb{F}_p[x]/(g(x)) \cong \mathbb{F}_{p^d}$ embeds into $\mathbb{F}_q$ iff $d \mid n$. Thus $x^{p^n} - x$ is the product of all irreducibles of degree d where $d \mid n$.

証明終

This classification guarantees the existence of irreducible polynomials of any degree.

Corollary 1.4. *Existence of Irreducible Polynomials.* For any prime p and $n \geq 1$, there exists an irreducible polynomial of degree n in $\mathbb{F}_p[x]$.

推論

Proof

Let K be a field of order p^n (*Classification of Finite Fields*). Since the multiplicative group $K^\times$ is cyclic (*Finite Subgroups of Fields*), $K = \mathbb{F}_p(\alpha)$ for some $\alpha \in K$. The minimal polynomial of α over $\mathbb{F}_p$ is

an irreducible polynomial of degree $[K : \mathbb{F}_p] = n$.

■

The automorphisms of finite fields are generated by the Frobenius map.

Theorem 1.4. ***Automorphisms of*** $\mathbb{F}_q$**.**
Let $K = \mathbb{F}_{p^n}$. The group $\mathrm{Gal}(K/\mathbb{F}_p)$ is cyclic of order n, generated by the Frobenius automorphism:

$$\sigma : K \to K, \quad x \mapsto x^p.$$

定理

Proof

The map σ is a homomorphism because $(x + y)^p = x^p + y^p$ and $(xy)^p = x^p y^p$. It is injective (kernel is trivial since fields have no zero divisors) and thus surjective (since K is finite). The fixed field of σ is $\{x \in K \mid x^p = x\}$, which is exactly the prime subfield $\mathbb{F}_p$. Let α be a generator of the cyclic group $K^\times$. Its minimal polynomial over $\mathbb{F}_p$ has degree n. The roots of this polynomial are $\alpha, \alpha^p, \ldots, \alpha^{p^{n-1}}$. These are distinct. Thus σ has order n. Since $|\mathrm{Gal}(K/\mathbb{F}_p)| \leq [K : \mathbb{F}_p] = n$ by *proposition* 0.6, the group is generated by σ.

■

Example 1.2. Frobenius on $\mathbb{F}_4$. Consider $K = \mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$ as defined in *A Field of Order 4*. The Frobenius automorphism $\sigma : x \mapsto x^2$ acts as:

$$0 \mapsto 0, \quad 1 \mapsto 1, \quad \alpha \mapsto \alpha^2 = \alpha + 1, \quad \alpha + 1 \mapsto (\alpha + 1)^2 = \alpha^2 + 1 = \alpha.$$

This map permutes the elements not in the prime subfield $\mathbb{F}_2$.

範例

We conclude with a practical criterion for irreducibility, often used to construct such fields.

Proposition 1.2. ***Eisenstein's Criterion.***
Let $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$. Suppose there exists a prime p such that:
1. $p \nmid a_n$,
2. $p \mid a_i$ for all $0 \leq i < n$,
3. $p^2 \nmid a_0$.

Then $f(x)$ is irreducible over $\mathbb{Q}$.

命題

Proof

Suppose $f(x) = g(x)h(x)$ over $\mathbb{Z}[x]$. Reduce modulo p:

$$\bar{f}(x) = \bar{a}_n x^n.$$

Thus $\bar{g}(x)\bar{h}(x) = \bar{a}_n x^n$. This implies $\bar{g}(x) = bx^k$ and $\bar{h}(x) = cx^{n-k}$ for some constants. Consequently, the constant terms of g and h are both divisible by p. But then the constant term of f, which is $a_0 = g(0)h(0)$, would be divisible by p^2, contradicting the assumption.

■

Proposition 1.3. ***Low Degree Irreducibility.***
A polynomial $f(x) \in K[x]$ of degree 2 or 3 is irreducible if and only if it has no roots in K.

命題

Proof

If reducible, it splits into factors. At least one factor must be degree 1 (since $2 = 1+1$ and $3 = 1+2$ or $1+1+1$), corresponding to a root.

■

1.3 *Exercises*

1. **Constructible Numbers.** Determine which of the following quantities can be constructed using only a straightedge and compass. Justify your answer using the degree of field extensions.
   (a) $\sqrt[3]{3} + 5\sqrt[3]{8}$
   (b) $\frac{3\sqrt{5}}{\sqrt{7}-4}$
   (c) $2 + \sqrt[5]{7}$
   (d) The roots of the polynomial $x^5 - 3x^2 + 6$

2. **Constructible Angles.** Prove that angles of 45° and 54° can be trisected with a straightedge and compass.

   To trisect 54° means constructing 18°. Consider the constructibility of the regular pentagon.

3. **Doubling the Cube.** Prove the impossibility of the classical problem of "doubling the cube" (constructing a cube with twice the volume of a given cube).

   This corresponds to constructing $\sqrt[3]{2}$.

4. **Constructible Polygons.** For each integer $3 \leq n \leq 10$, determine whether a regular n-gon can be constructed with straightedge and compass.

5. **Gauss's Direction.** Let p be a Fermat prime. Prove that a regular p-gon is constructible by showing that $\cos(2\pi/p)$ lies in a tower of quadratic extensions of $\mathbb{Q}$.

6. **Maximal Ideals and Geometry.**
   (a) Prove that there is a bijection between the maximal ideals of $\mathbb{C}[x]$ and the points in the complex plane $\mathbb{C}$.
   (b) Describe the geometric correspondence for the maximal ideals of $\mathbb{R}[x]$.

   For (b): Consider the Fundamental Theorem of Algebra and complex conjugation.

7. **Constructing Finite Fields.** Explicitly construct a field of 8 elements, $\mathbb{F}_8 = \mathbb{F}_2[x]/(f)$ for an irreducible cubic $f(x)$. Let u be the image of x. List the elements as powers of u, compute the multiplication table for $\mathbb{F}_8^\times$, determine all generators of $\mathbb{F}_8^\times$, and describe the Frobenius automorphism $x \mapsto x^2$ on $\mathbb{F}_8$.

8. **Irreducible Polynomials.**
   (a) List all irreducible polynomials of degree ≤ 4 over $\mathbb{F}_2$.
   (b) List all quadratic irreducible polynomials over $\mathbb{F}_3$.

9. **Counting Irreducibles.** Let p and l be primes, and n a positive integer. Find a formula for the number of monic irreducible polynomials of degree l^n in $\mathbb{F}_p[x]$.

   Use the inclusion-exclusion principle on subfields of $\mathbb{F}_{p^{l^n}}$.

   Count elements of $\mathbb{F}_{p^{l^n}}$ of degree exactly l^n over $\mathbb{F}_p$, then divide by l^n.

10. **Minimal Polynomials (computational).** Let $\alpha_1^2 = 2$ and $\alpha_2^2 = 3$, and set $\beta = \alpha_1 + \alpha_2$. For each base field below, first determine whether 2, 3, and 6 are squares, then compute $[\,F(\beta) : F\,]$, the minimal polynomial of β over F, and the minimal polynomial of β^2 over F. Decide when $F(\beta) = F(\beta^2)$.
    (a) $\mathbb{F}_5$
    (b) $\mathbb{F}_7$
    (c) $\mathbb{F}_{11}$

11. **Primitive Polynomials.** Let $f(x) \in \mathbb{F}_p[x]$ be a monic irreducible polynomial of degree n. Let $\varphi(m)$ denote Euler's totient function.
    (a) Let u be a root of $f(x)$. Prove that the roots of $f(x)$ are exactly $u, u^p, u^{p^2}, \ldots, u^{p^{n-1}}$.
    (b) A polynomial is called **primitive** if its root u generates the multiplicative group $\mathbb{F}_{p^n}^\times$. Prove that if one root is a generator, all roots are generators.
    (c) Prove that the number of primitive polynomials of degree n over $\mathbb{F}_p$ is $\varphi(p^n - 1)/n$.

12. **Reducibility.** Prove that for $n \geq 3$, the polynomial $x^{2^n} + x + 1$ is reducible in $\mathbb{F}_2[x]$.

13. **Subfields of $\mathbb{F}_{16}$.**
    (a) Prove that $x^4 + x + 1$ is a primitive polynomial in $\mathbb{F}_2[x]$.
    (b) Let $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$ where α is a root of $x^4 + x + 1$. List the elements of the unique subfield of order 4 within $\mathbb{F}_{16}$.
    (c) Find the minimal polynomial of α over $\mathbb{F}_4$.

14. Generators of $\mathbb{F}_{16}$.

(a) Prove that $f(x) = x^4 + x^3 + x^2 + x + 1$ is irreducible but **not** primitive in $\mathbb{F}_2[x]$.

(b) Let u be a root of $f(x)$. Identify which elements of $\mathbb{F}_{16} = \mathbb{F}_2(u)$ generate the multiplicative group $\mathbb{F}_{16}^\times$.

15. Quadratic Equations in Finite Fields. Let F be a finite field and $a, b \in F^\times$. Prove that for any $c \in F$, the equation $ax^2 + by^2 = c$ has a solution (x, y) in F^2.

Use a counting argument on the sets $\{ax^2\}$ and $\{c - by^2\}$.

16. Isomorphisms of Extensions. Prove that $f(x) = x^3 + x + 1$ and $g(x) = x^3 + x^2 + 1$ are irreducible over $\mathbb{F}_2$. Let K be the field generated by a root of f, and L by a root of g. Explicitly construct an isomorphism $\phi : K \to L$.

17. Wilson's Theorem for Fields. Let K be a finite field. Prove that the product of all non-zero elements of K is -1.

18. Factorisation in $\mathbb{F}_3$. Factor the polynomials $x^9 - x$ and $x^{27} - x$ into irreducibles over $\mathbb{F}_3$.

19. Trace and Norm. Let $F = \mathbb{F}_{p^n}$ and $G = \mathrm{Gal}(F/\mathbb{F}_p)$. Define the Trace and Norm maps:

$$\mathrm{Tr}(a) = \sum_{\sigma \in G} \sigma(a), \quad N(a) = \prod_{\sigma \in G} \sigma(a).$$

(a) Prove that $\mathrm{Tr} : F \to \mathbb{F}_p$ is a surjective group homomorphism.

(b) Prove that $N : F^\times \to \mathbb{F}_p^\times$ is a surjective group homomorphism.

20. Fixed Fields. Let $F = \mathbb{F}_{p^n}$ and let H be a subgroup of $\mathrm{Gal}(F/\mathbb{F}_p)$ of order m. Let $K = \{a \in F \mid \sigma(a) = a \text{ for all } \sigma \in H\}$.

(a) Prove that m divides n.

(b) Prove that K is the unique subfield of F of order $p^{n/m}$.

21. Repeated Roots in Characteristic p. Let F be a field of characteristic p, and let $f(x)$ be irreducible in $F[x]$. (A root α in a splitting field is called *multiple* if $(x - \alpha)^2$ divides $f(x)$.)

(a) Prove that $f'(x) = 0$ if and only if $f(x) = g(x^p)$ for some $g(x) \in F[x]$.

(b) If $f(x) = g(x^{p^m})$ but not $h(x^{p^{m+1}})$, prove that $\deg f$ is divisible by p^m, and that in a splitting field f has exactly $\deg(f)/p^m$ distinct roots, each with multiplicity p^m.

22. Linear Groups over Finite Fields. Let $F = \mathbb{F}_q$.

Count bases column by column to compute $|GL_n(F)|$, then use $\det : GL_n(F) \to F^\times$.

(a) Calculate the order of the special linear group $SL_n(F)$.

(b) Prove that the group of upper triangular matrices in $GL_n(\mathbb{F}_p)$ with 1s on the diagonal (the Heisenberg group for $n = 3$) has order $p^{n(n-1)/2}$. For $n = 3$, verify it is non-abelian of order p^3.

2
Galois Theory

We have previously explored field extensions K/F by analysing the degree $[K : F]$ and the algebraic properties of elements. In this chapter, we introduce the central object of Galois theory: the group of automorphisms of K that fix F. This group encodes the structural symmetry of the extension and provides a powerful bridge between field theory and group theory. Unless otherwise specified, we assume all extensions K/F are finite. We freely use results from the previous chapters.

2.1 *The Galois Group*

Recall that an isomorphism of fields $\sigma : K \to K$ is called an automorphism. If K is an extension of F, we are particularly interested in automorphisms that respect the base field.

Definition 2.1. ***Galois Group.***
Let K/F be a field extension. The set of all F-automorphisms of K,

$$\mathrm{Gal}(K/F) = \{\sigma \in \mathrm{Aut}(K) \mid \sigma(a) = a \text{ for all } a \in F\},$$

forms a group under composition. This group is called the **Galois group** of K over F.

定義

The action of the Galois group is tightly constrained by the polynomials defining the extension.

Remark.

Recall *proposition* 0.5: if $\sigma \in \mathrm{Gal}(K/F)$ and $\alpha \in K$ is a root of a polynomial $f(x) \in F[x]$, then $\sigma(\alpha)$ must also be a root of $f(x)$. Since σ is injective and K is a field, σ permutes the roots of $f(x)$ that lie in K.

We examine the size of this group in several standard cases.

Example 2.1. Inseparable Extension. Let $F = \mathbb{F}_p(T)$ be the field of rational functions over the finite field $\mathbb{F}_p$, and let $K = F(\sqrt[p]{T})$. Let

$\alpha = \sqrt[p]{T}$. The minimal polynomial of α over F is $m(x) = x^p - T$. In $K[x]$, this polynomial factorises as:

$$x^p - T = x^p - \alpha^p = (x - \alpha)^p.$$

Thus, α is the unique root of $m(x)$ in K (with multiplicity p). For any $\sigma \in \mathrm{Gal}(K/F)$, $\sigma(\alpha)$ must be a root of $m(x)$. Therefore, $\sigma(\alpha) = \alpha$. Since K is generated by α over F, σ must be the identity map.

$$\mathrm{Gal}(K/F) = \{1\}.$$

Here, $[K : F] = p$, but the Galois group has order 1.

範例

Example 2.2. Quadratic Extensions. Let K/F be a quadratic extension, so $[K : F] = 2$. Let $K = F(\alpha)$ where α has minimal polynomial $f(x) = x^2 + bx + c \in F[x]$. Let the roots of $f(x)$ in K be α and α'. We have the relations $\alpha + \alpha' = -b$ and $\alpha\alpha' = c$. Thus $\alpha' = -b - \alpha \in K$. Any $\sigma \in \mathrm{Gal}(K/F)$ must map α to a root of $f(x)$.

1. If $\sigma(\alpha) = \alpha$, then $\sigma = 1$ (the identity).
2. If $\alpha \neq \alpha'$, there may exist an automorphism τ such that $\tau(\alpha) = \alpha'$.

We distinguish cases based on the characteristic of F:

Case 1: $\alpha = \alpha'$**.** This implies the discriminant is zero. In characteristic $\neq 2$, this forces $f(x)$ to be reducible or linear, contradicting the degree 2 assumption. In characteristic 2, if $b = 0$, $f(x) = x^2 + c$ is irreducible but has a repeated root (inseparable). Here $\mathrm{Gal}(K/F) = \{1\}$.

Case 2: $\alpha \neq \alpha'$**.** If $\mathrm{char}(F) \neq 2$, we can complete the square. $f(x)$ corresponds to $x^2 - D$ for some non-square $D \in F$. Then $K = F(\sqrt{D})$. The map $\sqrt{D} \mapsto -\sqrt{D}$ is a valid F-automorphism. Thus $\mathrm{Gal}(K/F) \cong C_2$.

範例

For notation, C_2 denotes the cyclic group of order 2, and V_4 denotes the Klein four-group.

Example 2.3. Biquadratic Extension. Assume $\mathrm{char}(F) \neq 2$. Let $K = F(\alpha, \beta)$ where $\alpha^2 = D_1 \in F$ and $\beta^2 = D_2 \in F$, such that $[K : F] = 4$. The basis for K over F is $\{1, \alpha, \beta, \alpha\beta\}$. Any automorphism σ is determined by its action on the generators:

$$\sigma(\alpha) = \pm\alpha, \quad \sigma(\beta) = \pm\beta.$$

There are at most 4 such combinations. Since $[K : F] = 4$, it can be shown that all 4 define valid automorphisms. Thus $|\mathrm{Gal}(K/F)| = 4$. The group is isomorphic to the Klein four-group $V_4 \cong C_2 \times C_2$.

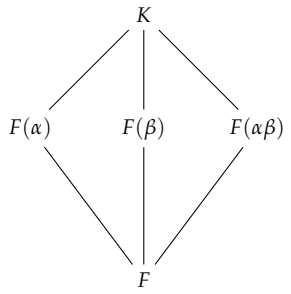


Figure 2.1: Lattice of subfields for a biquadratic extension.

範例

Example 2.4. Cubic Extension. Let $F = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt[3]{2})$. The minimal polynomial is $x^3 - 2$. The roots in $\mathbb{C}$ are $\alpha = \sqrt[3]{2}$, $\omega\alpha$, and $\omega^2\alpha$, where $\omega = e^{2\pi i/3}$. Since $K \subset \mathbb{R}$, it contains only the real root α. Any $\sigma \in \mathrm{Gal}(K/F)$ must map α to a root of $x^3 - 2$ contained in K. The only choice is α. Thus $\sigma(\alpha) = \alpha$, implying $\sigma = 1$.

$$\mathrm{Gal}(K/F) = \{1\}.$$

Here $[K : F] = 3$, but the group order is 1.

範例

2.2 *Galois Extensions*

In the examples above, we observed that $|\mathrm{Gal}(K/F)|$ is sometimes equal to $[K : F]$ (standard quadratic, biquadratic) and sometimes strictly smaller (inseparable quadratic, cubic $\mathbb{Q}(\sqrt[3]{2})$).

Theorem 2.1. ***Bound on Galois Group Size.***
Let K/F be a finite field extension. Then:

$$|\mathrm{Gal}(K/F)| \leq [K : F].$$

定理

Remark.

This is *proposition* 0.6 from Chapter 0. We will later reinterpret this bound using separability and normality.

Definition 2.2. ***Galois Extension.***
A finite extension K/F is a **Galois extension** if:

$$|\mathrm{Gal}(K/F)| = [K : F].$$

定義

Based on our previous examples:
· $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is Galois ($2 = 2$).
· $\mathbb{F}_p(\sqrt[p]{T})/\mathbb{F}_p(T)$ is not Galois ($1 < p$).
· $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois ($1 < 3$).
The Galois group acts on the field K. We can recover the base field F from this action if the extension is Galois.

Definition 2.3. ***Fixed Field.***
Let G be a subgroup of $\mathrm{Aut}(K)$. The **fixed field** of G is the set:

$$K^G = \{a \in K \mid \sigma(a) = a \text{ for all } \sigma \in G\}.$$

It is easily verified that K^G is a subfield of K.

定義

Corollary 2.1. *Fixed Field of Galois Extensions.* Let K/F be a Galois extension with Galois group $G = \mathrm{Gal}(K/F)$. Then:

$$K^G = F.$$

推論

Proof

Let $L = K^G$. By definition of the Galois group, every element of F is fixed by every $\sigma \in G$, so $F \subseteq L \subseteq K$. Any $\sigma \in G$ fixes L pointwise, so $G \subseteq \mathrm{Gal}(K/L)$. Conversely, by definition $\mathrm{Gal}(K/L)$ contains automorphisms fixing L, so $\mathrm{Gal}(K/L) \subseteq G$. Thus $G = \mathrm{Gal}(K/L)$. Using the definition of a Galois extension and the bound on group size:

$$[K : F] = |G| = |\mathrm{Gal}(K/L)| \leq [K : L].$$

By the Tower Law (*figure 2*), $[K : F] = [K : L][L : F]$. Substituting this into the inequality:

$$[K : L][L : F] \leq [K : L].$$

Since $[K : L]$ is finite and non-zero, we divide to obtain $[L : F] \leq 1$. Thus $[L : F] = 1$, implying $L = F$.

■

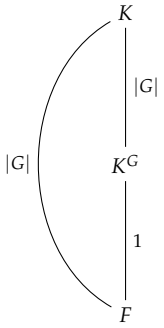


Figure 2.2: Since $[K : F] = |G| = [K : K^G]$, the Tower Law forces $[K^G : F] = 1$, hence $K^G = F$.

The failure of an extension to be Galois arises from two distinct issues:

Separability: The minimal polynomial has multiple roots (e.g., $x^p - T$).

Normality: The minimal polynomial has roots outside K (e.g., $x^3 - 2$).

2.3 *Separability*

We observed earlier that the size of the Galois group can be diminished if the minimal polynomial has multiple roots. We now formalise the conditions under which this pathology is avoided.

Definition 2.4. ***Separable Polynomials.***
We use the definition from *definition* 0.8. An arbitrary polynomial is separable if all its irreducible factors are separable.

定義

We can detect multiple roots purely algebraically using the formal derivative. Recall *proposition* 0.8: α is a multiple root of $f(x)$ if and

only if $f(\alpha) = 0$ and $f'(\alpha) = 0$. Consequently, $f(x)$ has multiple roots if and only if $f(x)$ and $f'(x)$ share a common factor, i.e., $\gcd(f, f') \neq 1$.

Proposition 2.1. ***Criterion for Inseparability.***
Let $f(x) \in F[x]$ be a monic irreducible polynomial. Then $f(x)$ is inseparable if and only if $f'(x) = 0$. This can only occur if $\text{char}(F) = p > 0$ and $f(x) = g(x^p)$ for some $g \in F[x]$.

命題

Proof

Since $f(x)$ is irreducible, its only divisors are units and associates of $f(x)$. The greatest common divisor (f, f') is non-trivial if and only if $f(x)$ divides $f'(x)$. However, $\deg f' < \deg f$. Thus $f(x) \mid f'(x)$ implies $f'(x) = 0$. If $\text{char}(F) = 0$, then $f'(x) = 0$ implies $f(x)$ is constant, contradicting irreducibility. If $\text{char}(F) = p > 0$, then $f'(x) = \sum i a_i x^{i-1} = 0$ implies $i a_i = 0$ for all i. Thus $a_i \neq 0$ only when $p \mid i$. Hence $f(x)$ is a polynomial in x^p.

■

This implies that for many fields, inseparability is impossible.

Definition 2.5. ***Perfect Fields.***
A field F is **perfect** if every irreducible polynomial in $F[x]$ is separable.

定義

Proposition 2.2. ***Characterisation of Perfect Fields.***
1. Every field of characteristic 0 is perfect.
2. A field of characteristic $p > 0$ is perfect if and only if the Frobenius endomorphism $x \mapsto x^p$ is surjective (i.e., every element is a p-th power).

命題

Proof

Case (i) follows immediately from the previous proposition ($f' \neq 0$ for non-constants).
For Case (ii), suppose F is perfect. If $\alpha \in F$ is not a p-th power and $m(x)$ is the minimal polynomial of a root of $x^p - \alpha$, then $m'(x) = 0$ since $m(x)$ divides $x^p - \alpha$. By the previous proposition, $m(x) = g(x^p)$, so $\deg m$ is a multiple of p. As $\deg m \leq p$, we have $\deg m = p$, hence $x^p - \alpha$ is irreducible, but inseparable ($f' = 0$), a contradiction. Conversely, if Frobenius is surjective, any inseparable irreducible $f(x) = g(x^p) = \sum a_i (x^p)^i$ can be written as $\sum b_i^p (x^i)^p = (\sum b_i x^i)^p$ where $a_i = b_i^p$. This contradicts the irreducibility of $f(x)$.

■

Corollary 2.2. *Finite Fields are Perfect.* Every finite field $\mathbb{F}_{p^n}$ is perfect.

推論

Proof

The Frobenius map $x \mapsto x^p$ is injective on a field. Since the field is finite, injectivity implies surjectivity.

■

We lift this concept to extensions.

Definition 2.6. ***Separable Extensions.***
An algebraic extension K/F is **separable** if the minimal polynomial of every element $\alpha \in K$ is separable over F.

定義

It follows that any algebraic extension of a perfect field (e.g., $\mathbb{Q}$, $\mathbb{F}_p$) is separable. The standard counterexample is $K = \mathbb{F}_p(\sqrt[p]{T})$ over $F = \mathbb{F}_p(T)$, where the element $\sqrt[p]{T}$ is inseparable.
Crucially, separability simplifies the structure of finite extensions.

Theorem 2.2. ***Primitive Element Theorem.***
Let K/F be a finite separable extension. Then K is a simple extension; that is, there exists a primitive element $\gamma \in K$ such that $K = F(\gamma)$.

定理

Proof

For infinite fields, the proof relies on linear algebra to find a linear combination $\gamma = \alpha + c\beta$ that generates the subfield $F(\alpha, \beta)$ by ensuring c avoids a finite set of ratios between roots. By induction on the number of generators, the result holds. For finite fields, the multiplicative group $K^\times$ is cyclic (*Finite Subgroups of Fields*). A generator of this group generates the field.

■

2.4 *Normal Extensions and Splitting Fields*

The second obstruction to an extension being Galois is the lack of roots within the field. To remedy this, we construct fields containing all roots of a given polynomial.

Definition 2.7. ***Splitting Field.***
Let $f(x) \in F[x]$. A field extension K/F is a **splitting field** for $f(x)$ if:
1. $f(x)$ splits into linear factors in $K[x]$:

$$f(x) = c(x - \alpha_1) \cdots (x - \alpha_n), \quad \alpha_i \in K.$$

2. K is generated by these roots: $K = F(\alpha_1, \ldots, \alpha_n)$.

定義

Example 2.5. Splitting Field of $x^3 - 2$. Consider $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. The roots in $\mathbb{C}$ are $\alpha = \sqrt[3]{2}$, $\omega\alpha$, and $\omega^2\alpha$, where $\omega = e^{2\pi i/3}$. The field $\mathbb{Q}(\alpha)$ contains only one root. It is not a splitting field. The splitting field is $K = \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha) = \mathbb{Q}(\sqrt[3]{2}, \omega)$. Note that $[K : \mathbb{Q}] = 6$.

範例

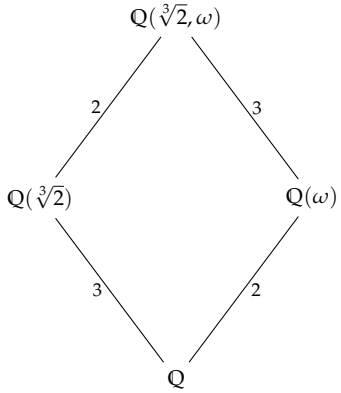


Figure 2.3: The splitting field of $x^3 - 2$ has degree 6 over $\mathbb{Q}$.

To define the Galois group, we ensure splitting fields are unique up to isomorphism. This relies on the ability to extend isomorphisms between base fields to their extensions.

Lemma 2.1. ***Extension of Isomorphisms.***
Let $\varphi : F \to \tilde{F}$ be a field isomorphism. Let $f(x) \in F[x]$ be irreducible and let $\tilde{f}(x) = \varphi(f(x)) \in \tilde{F}[x]$. Let α be a root of $f(x)$ in some extension of F, and let $\tilde{\alpha}$ be a root of $\tilde{f}(x)$ in some extension of $\tilde{F}$. Then there exists a unique isomorphism $\hat{\varphi} : F(\alpha) \to \tilde{F}(\tilde{\alpha})$ such that:

$$\hat{\varphi}|_F = \varphi \quad \text{and} \quad \hat{\varphi}(\alpha) = \tilde{\alpha}.$$

引理

Proof

We have natural isomorphisms induced by polynomial evaluation and quotients:

$$F(\alpha) \cong F[x]/(f(x)) \xrightarrow{\cong} \tilde{F}[x]/(\tilde{f}(x)) \cong \tilde{F}(\tilde{\alpha}).$$

The composite map satisfies the requirements.

■

Proposition 2.3. ***Uniqueness of Splitting Fields.***
Let $\varphi : F \to \tilde{F}$ be an isomorphism and let $K, \tilde{K}$ be splitting fields for $f(x)$ and $\varphi(f(x))$ respectively. Then there exists an isomorphism $\sigma : K \to \tilde{K}$ extending φ. In particular, the splitting field of a polynomial is unique up to F-isomorphism.

命題

Proof

We proceed by induction on $[K : F]$. If the degree is 1, $K = F$ and $\tilde{K} = \tilde{F}$, so $\sigma = \varphi$. Otherwise, let $p(x)$ be an irreducible factor of $f(x)$ with degree > 1. Let $\alpha \in K$ be a root of $p(x)$ and $\beta \in \tilde{K}$ be a root of $\varphi(p(x))$. By *lemma 2.1*, there is an isomorphism $\varphi_1 : F(\alpha) \to \tilde{F}(\beta)$. Now K is a splitting field for $f(x)$ over $F(\alpha)$, and $\tilde{K}$ is a splitting field over $\tilde{F}(\beta)$. Since $[K : F(\alpha)] < [K : F]$, the induction

hypothesis provides the required extension $\sigma : K \to \tilde{K}$.

■

Definition 2.8. ***Normal Extensions.***
An algebraic extension K/F is **normal** if it satisfies either (and thus both) of the following equivalent conditions:

1. K is the splitting field of some family of polynomials in $F[x]$.
2. For every irreducible polynomial $g(x) \in F[x]$, if $g(x)$ has one root in K, it splits completely into linear factors in $K[x]$.

定義

We combine normality and separability to characterise Galois extensions.

Theorem 2.3. ***Characterisation of Galois Extensions.***
Let K/F be a finite extension. The following are equivalent:

1. K/F is a Galois extension (i.e., $|\mathrm{Gal}(K/F)| = [K : F]$).
2. K is the splitting field of a separable polynomial $f(x) \in F[x]$.
3. K/F is both normal and separable.

定理

This theorem allows us to construct Galois extensions easily: simply take the splitting field of a separable polynomial.

Corollary 2.3. *Galois Closure.* Every finite separable extension K/F is contained in a finite Galois extension L/F. The smallest such L is called the **Galois closure** of K.

推論

Proof

Let $K = F(\alpha)$ (by the Primitive Element Theorem). Let $m(x)$ be the minimal polynomial of α over F. Let L be the splitting field of $m(x)$ containing K. Since K/F is separable, $m(x)$ is separable. Thus L/F is Galois.

■

Corollary 2.4. *Intermediate Galois Extensions.* Let K/F be a Galois extension and L be an intermediate field ($F \subseteq L \subseteq K$). Then K/L is always a Galois extension.

推論

Proof

If K is the splitting field of $f(x)$ over F, it is also the splitting field of $f(x)$ over L. Separability is preserved in subfields. Thus K/L is Galois. (Note: L/F is not necessarily Galois, as we saw with $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$).

■

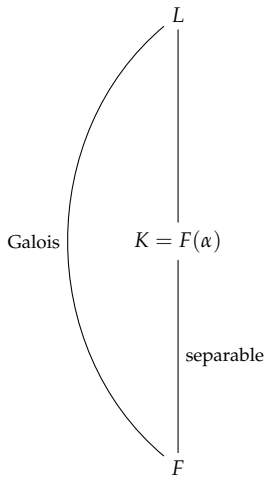


Figure 2.4: The Galois closure L is the splitting field of the minimal polynomial of α.

The Fundamental Theorem

We now state the crowning result of the theory, establishing a structural dictionary between the lattice of intermediate fields and the lattice of subgroups of the Galois group.

Theorem 2.4. ***The Fundamental Theorem of Galois Theory.***
Let K/F be a finite Galois extension with Galois group $G = \mathrm{Gal}(K/F)$.

1. There is a one-to-one inclusion-reversing correspondence between the subgroups of G and the intermediate fields of K/F:

$$\begin{aligned} \mathcal{H} = \{\text{Subgroups of } G\} &\longleftrightarrow \mathcal{F} = \{\text{Fields } L \mid F \subseteq L \subseteq K\} \\ H &\longmapsto K^H = \{x \in K \mid \sigma(x) = x \forall \sigma \in H\} \\ \mathrm{Gal}(K/L) &\longleftarrow L \end{aligned}$$

2. For any subgroup $H \leq G$ and corresponding field $L = K^H$:

$$[K : L] = |H| \quad \text{and} \quad [L : F] = (G : H),$$

   where $(G : H)$ is the index of H in G.

3. An intermediate field L is a normal extension of F (and thus Galois over F) if and only if the corresponding subgroup $H = \mathrm{Gal}(K/L)$ is a normal subgroup of G. In this case, there is a canonical isomorphism:

$$\mathrm{Gal}(L/F) \cong G/H.$$

定理

Figure 2.5: The inclusion-reversing correspondence between fields and subgroups.

The isomorphism $\mathrm{Gal}(L/F) \cong G/H$ is given by restriction: for $\sigma \in G$, the map $\sigma|_L$ is an automorphism of L (since L is normal, $\sigma(L) = L$). The kernel of the restriction map $G \to \mathrm{Gal}(L/F)$ is precisely the subgroup fixing L, which is H.

2.5 *Exercises*

1. **Splitting Fields over Finite Fields.** Let $F = \mathbb{F}_q$ be a finite field with q elements, and let n be an integer coprime to $p = \text{char}(F)$. Let E be the splitting field of $x^n - 1$ over F. Prove that the degree $[E : F]$ is the smallest positive integer k such that $q^k \equiv 1 \pmod{n}$.

2. **Degree Bound.** Let $f(x) \in F[x]$ be a polynomial of degree n, and let E be its splitting field over F. Prove that $[E : F]$ divides $n!$.

3. **Cyclotomic Extension of $\mathbb{Q}$.** Let E be the splitting field of $x^8 - 1$ over $\mathbb{Q}$.

   Factor $x^8 - 1$ into cyclotomic factors and use the Tower Law.

   (a) Determine the degree $[E : \mathbb{Q}]$.
   (b) Determine the Galois group $\text{Gal}(E/\mathbb{Q})$.

4. **Purely Transcendental Extensions.** An extension E/F is **purely transcendental** if every element $\alpha \in E \setminus F$ is transcendental over F.

   (a) Using the result from Chapter 0 that any element of $F(x)$ not in F is transcendental over F, prove that $F(x)/F$ is purely transcendental.

   Combine *proposition* 0.1 with Exercise 8 in Chapter 0.

   (b) Prove that for any extension E/F, there exists a unique intermediate field M such that E/M is purely transcendental and M/F is algebraic.

5. **Eliminating Multiple Roots.** Let F be a field of characteristic 0 and $f(x)$ a monic polynomial in $F[x]$. Let $d(x) = \gcd(f, f')$. Prove that $g(x) = f(x)/d(x)$ has the same roots as $f(x)$ but no multiple roots.

6. **Multiplicities in Characteristic p.** Let F be a field of characteristic $p > 0$ and $f(x) \in F[x]$ be irreducible. Prove that all roots of $f(x)$ have the same multiplicity, and this multiplicity is of the form p^n for some $n \geq 0$.

7. **Separability in Towers.** Let E/F be a separable extension and M an intermediate field. Prove that both E/M and M/F are separable.

8. **Pure Inseparability.** Let F be a field of characteristic $p > 0$ and E/F an algebraic extension. Prove that for every $\alpha \in E$, there exists $n \geq 0$ such that α^{p^n} is separable over F.

9. **Non-Simple Extension.** Let $E = \mathbb{F}_p(x, y)$ and $F = \mathbb{F}_p(x^p, y^p)$.

   (a) Prove that $[E : F] = p^2$.

   Show $\{x^i y^j \mid 0 \leq i, j < p\}$ spans E over F and use a minimality argument.

   (b) Prove that E/F is not a simple extension (i.e., $E \neq F(\gamma)$ for any γ).

   If $E = F(\gamma)$, compare $F(\gamma^p)$ with F and use inseparability.

   (c) Show that E/F has infinitely many intermediate fields.

   Consider $F(x^p, y^p, x + ay)$ with $a \in \mathbb{F}_p(t)$.

10. **Perfect Fields in Extensions.**

(a) If E/F is algebraic and F is perfect, prove E is perfect.
(b) If E/F is finitely generated and E is perfect, prove F is perfect.
(c) Does the conclusion of (b) hold if E/F is algebraic but not finitely generated?

11. Explicit Normality. Let $E = \mathbb{Q}(\alpha)$ where α is a root of $x^3 + x^2 - 2x - 1 = 0$.

(a) Verify that $\alpha^2 - 2$ is also a root of the same polynomial.
(b) Prove that $E/\mathbb{Q}$ is a normal extension.

12. Compositum of Normal Extensions. Let E/F and K/F be normal extensions contained in a common larger field. Let EK denote the compositum, the smallest subfield containing both E and K. Prove that EK/F is normal.

13. Normality in Towers.

(a) Give an example where E/M and M/F are normal, but E/F is **not** normal.
(b) If E/F is normal and M is intermediate, must E/M be normal? Must M/F be normal?

14. Degree Condition for Normality. Let E/F be a finite algebraic extension. Prove that E/F is normal if and only if for every irreducible polynomial $f(x) \in F[x]$, all irreducible factors of $f(x)$ in $E[x]$ have the same degree.

3
Galois Groups of Polynomials

We now apply the Fundamental Theorem of Galois Theory (*theorem 2.4*) to determine the Galois groups of concrete polynomials. The Galois group of a polynomial $f(x) \in F[x]$ is defined as the Galois group of its splitting field over F. This group acts by permuting the roots of $f(x)$, providing a representation of the group as a subgroup of the symmetric group S_n.

The Cubic Equation

Consider a general cubic polynomial $f(x) = x^3 + a_2x^2 + a_1x + a_0 \in F[x]$. Assuming $\text{char}(F) \neq 3$, we may eliminate the quadratic term via the substitution $x \mapsto x - \frac{a_2}{3}$. This yields the *depressed cubic*:

$$g(x) = x^3 + px + q, \quad p, q \in F.$$

Let K be the splitting field of $g(x)$ over F. Let the roots of $g(x)$ in K be $\alpha_1, \alpha_2, \alpha_3$. From the relations between roots and coefficients (Vieta's formulae), we have:

$$\begin{cases} \sum \alpha_i = 0 \\ \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = p \\ \alpha_1\alpha_2\alpha_3 = -q \end{cases}$$

The Galois group $G = \text{Gal}(K/F)$ permutes the set $\{\alpha_1, \alpha_2, \alpha_3\}$. Since $K = F(\alpha_1, \alpha_2, \alpha_3)$, the action is faithful, allowing us to view G as a subgroup of S_3. We have the tower of fields $F \subseteq F(\alpha_1) \subseteq K$. Since $[F(\alpha_1) : F] \leq 3$ and $[K : F(\alpha_1)] \leq 2$, the total degree $[K : F]$ divides 6. To classify G, we investigate specific elements within K that are invariant under certain permutations.

Definition 3.1. ***Discriminant of a Cubic.***
Let the roots of the cubic be $\alpha_1, \alpha_2, \alpha_3$. We define the quantity Δ by:

$$\Delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1).$$

The **discriminant** of the polynomial is $D = \Delta^2$.

定義

Assume $\text{char}(F) \neq 2$ so that the sign character takes values ± 1 with $\pm 1 \neq \mp 1$ in F. The action of S_3 on Δ is determined by the sign of the permutation. For any $\sigma \in G$:

$$\sigma(\Delta) = \text{sgn}(\sigma)\Delta.$$

Thus, $\sigma(D) = \sigma(\Delta^2) = (\text{sgn}(\sigma)\Delta)^2 = \Delta^2 = D$. Since the discriminant is fixed by the entire Galois group, by the Fundamental Theorem (*corollary 2.1*), $D \in F$.
However, Δ itself belongs to F if and only if $\sigma(\Delta) = \Delta$ for all $\sigma \in G$. This occurs precisely when every $\sigma \in G$ is an even permutation, i.e., $G \subseteq A_3$.

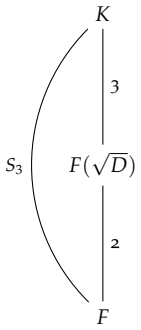
Theorem 3.1. ***Galois Group of a Cubic.***
Let $f(x) = x^3 + px + q \in F[x]$ be irreducible and separable, with discriminant D. Let K be its splitting field. Assume $\text{char}(F) \neq 2, 3$.
1. If D is a square in F (i.e., $\sqrt{D} \in F$), then $G \cong A_3 \cong C_3$.
2. If D is not a square in F, then $G \cong S_3$.

定理

Proof

Consider the subfield $F(\sqrt{D}) = F(\Delta)$. If D is a square in F, then $\Delta \in F$. Thus for all $\sigma \in G$, $\sigma(\Delta) = \Delta$, implying $\text{sgn}(\sigma) = 1$. Hence $G \subseteq A_3$. Since f is irreducible, $3 \mid [K : F]$, so $3 \mid |G|$. The only subgroup of A_3 with order divisible by 3 is A_3 itself. If D is not a square, $F(\Delta)$ is a quadratic extension of F. By the Tower Law, $[K : F] = [K : F(\Delta)][F(\Delta) : F] = 2[K : F(\Delta)]$. Since 3 divides $[K : F]$, it follows that $[K : F]$ is a multiple of 6. Since $G \leq S_3$, $|G| \leq 6$. Thus $|G| = 6$ and $G \cong S_3$.

■



Case $D \notin F^2$

Figure 3.1: Field tower for the splitting field of a cubic when the discriminant is not a square.

The General Case

We extend these concepts to a monic polynomial $f(x) \in F[x]$ of degree n with no repeated roots. Let K be the splitting field and roots $\alpha_1, \ldots, \alpha_n \in K$. The Galois group $G = \text{Gal}(K/F)$ embeds into S_n.

Definition 3.2. ***General Discriminant.***
The **discriminant** of $f(x)$ is defined as:

$$D(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

定義

As in the cubic case, $D(f) \neq 0$ if and only if f has no repeated roots.

Proposition 3.1. ***Discriminant and Alternating Group.***
The discriminant $D(f)$ lies in the base field F. Furthermore, the Galois group G is a subgroup of the alternating group A_n if and only if $D(f)$ is the square of an element in F. Assume $\text{char}(F) \neq 2$.

$$G \subseteq A_n \iff \sqrt{D} \in F.$$

命題

Proof

Let $\Delta = \prod_{i<j}(\alpha_i - \alpha_j)$. Then $D = \Delta^2$. Any permutation $\sigma \in S_n$ acts on Δ by $\sigma(\Delta) = \text{sgn}(\sigma)\Delta$. Consequently, $\sigma(D) = (\text{sgn}(\sigma)\Delta)^2 = \Delta^2 = D$ for all $\sigma \in G$. Since the Galois extension fixes elements if and only if they are in the base field, $D \in F$. The condition $G \subseteq A_n$ is equivalent to $\text{sgn}(\sigma) = 1$ for all $\sigma \in G$. This holds if and only if $\sigma(\Delta) = \Delta$ for all $\sigma \in G$, which by the Fundamental Theorem implies $\Delta \in F$, or equivalently, D is a square in F.

■

To utilise this proposition, we require a method to compute D without knowing the roots explicitly.

Lemma 3.1. ***Computing the Discriminant.***
Let $f(x) = \prod_{i=1}^{n}(x - \alpha_i)$. Then:

$$D(f) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} f'(\alpha_i).$$

引理

Proof

By the product rule, the derivative is $f'(x) = \sum_{k=1}^{n} \prod_{j\neq k}(x - \alpha_j)$. Evaluating at a root α_i annihilates all terms in the sum except the $k = i$ term:

$$f'(\alpha_i) = \prod_{j\neq i}(\alpha_i - \alpha_j).$$

The product of these values is:

$$\prod_{i=1}^{n} f'(\alpha_i) = \prod_{i=1}^{n} \prod_{j\neq i}(\alpha_i - \alpha_j).$$

Each pair of indices $\{i, j\}$ with $i \neq j$ appears twice in this product: once as $(\alpha_i - \alpha_j)$ and once as $(\alpha_j - \alpha_i)$. Since $(\alpha_j - \alpha_i) = -(\alpha_i - \alpha_j)$, we group them:

$$(\alpha_i - \alpha_j)(\alpha_j - \alpha_i) = -(\alpha_i - \alpha_j)^2.$$

There are $\binom{n}{2} = \frac{n(n-1)}{2}$ such pairs. Factoring out the -1 for each

pair yields:

$$\prod_{i=1}^{n} f'(\alpha_i) = (-1)^{\frac{n(n-1)}{2}} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} D(f).$$

Multiplying by the sign factor again (which is its own inverse) gives the result.

■

Example 3.1. Discriminant of $x^3 + px + q$. For $f(x) = x^3 + px + q$, we have $f'(x) = 3x^2 + p$. The discriminant is:

$$D = (-1)^{\frac{3(2)}{2}} \prod_{i=1}^{3} (3\alpha_i^2 + p) = -\prod_{i=1}^{3} (3\alpha_i^2 + p).$$

Using the fact that $\alpha_i^3 = -p\alpha_i - q$, we can reduce the powers (or use resultants). A standard calculation yields:

$$D = -4p^3 - 27q^2.$$

範例

Transitivity and Primitivity

The Galois group acts on the set of roots. The structure of the orbits of this action reveals factorisation properties of the polynomial.

Lemma 3.2. ***Transitivity of the Galois Group.***
Let $f(x) \in F[x]$ be a separable polynomial. The Galois group G acts transitively on the roots of $f(x)$ if and only if $f(x)$ is irreducible over F.

引理

Proof

Let α, β be distinct roots. If f is irreducible, $F(\alpha) \cong F(\beta)$ via an isomorphism fixing F. By the isomorphism extension property (*lemma 2.1*), this extends to an automorphism of the splitting field K, which is an element of G. Thus the action is transitive. Conversely, if the action is transitive, then for any root α, the orbit of α is the set of all roots. The polynomial $P(x) = \prod_{\sigma \in G} (x - \sigma(\alpha))$ has coefficients in F (fixed by G) and divides $f(x)$. Since all roots are in the orbit, $P(x)$ shares all roots with $f(x)$, so $f(x)$ is irreducible.

■

We conclude with a powerful theorem due to Dedekind that allows us to determine the Galois group of polynomials over $\mathbb{Q}$ by inspecting their roots in $\mathbb{C}$.

Theorem 3.2. ***Galois Group*** S_p**.**
Let p be a prime and let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree p. If $f(x)$ has exactly two non-real complex roots, then:

$$\mathrm{Gal}(K/\mathbb{Q}) \cong S_p.$$

定理

Proof

Let $G = \mathrm{Gal}(K/\mathbb{Q}) \subseteq S_p$. Since f is irreducible, p divides $[K : \mathbb{Q}]$. By Cauchy's Theorem for groups, G contains an element of order p. In S_p, the only elements of order p are p-cycles. Thus G contains a p-cycle.
Let $\sigma : \mathbb{C} \to \mathbb{C}$ be complex conjugation. The coefficients of f are rational (hence real), so $f(\sigma(z)) = \overline{f(z)}$. Thus σ permutes the roots of f. Since there are exactly two non-real roots (which must be a conjugate pair $z, \bar{z}$) and $p - 2$ real roots, σ fixes $p - 2$ roots and swaps two. Therefore, the restriction of σ to the splitting field K corresponds to a transposition in G.
A known result from group theory states that any subgroup of S_p containing a transposition and a p-cycle must be the entire group S_p. Consequently, $G \cong S_p$.

■

Example 3.2. Application to S_5. Consider $f(x) = x^5 - 6x + 3$. By Eisenstein's Criterion with $p = 3$, f is irreducible. Differentiation gives $f'(x) = 5x^4 - 6$, which has real roots at $\pm\sqrt[4]{6/5}$. The polynomial $f(x)$ has local extrema at these points.

$$f(\sqrt[4]{6/5}) \approx 3 - 6(1.04) < 0, \quad f(-\sqrt[4]{6/5}) \approx 3 + 6(1.04) > 0.$$

Since the limits at $\pm\infty$ are $\pm\infty$, the graph crosses the x-axis three times. Thus there are 3 real roots and 2 complex roots. Since 5 is prime, the Galois group is S_5.

範例

3.1 *Symmetric Polynomials*

We have seen that the Galois group of a polynomial encodes the permutations of its roots. In the general case, where the coefficients are independent variables, we expect the roots to exhibit no specific algebraic relations other than those imposed by the coefficients themselves. This leads to the study of symmetric polynomials.
Let E be a field and let $x_1, \ldots, x_n$ be independent indeterminates. We consider the field extension generated by these indeterminates,

$K = E(x_1, \ldots, x_n)$.

Definition 3.3. ***Elementary Symmetric Polynomials.***
The **elementary symmetric polynomials** $e_1, \ldots, e_n \in E[x_1, \ldots, x_n]$ are defined as:

$$\begin{aligned} e_1 &= \sum_{1 \le i \le n} x_i, \\ e_2 &= \sum_{1 \le i < j \le n} x_i x_j, \\ &\vdots \\ e_k &= \sum_{1 \le i_1 < \cdots < i_k \le n} x_{i_1} \cdots x_{i_k}, \\ &\vdots \\ e_n &= x_1 x_2 \cdots x_n. \end{aligned}$$

定義

Consider the subfield $F = E(e_1, \ldots, e_n) \subseteq K$. We observe that $x_1, \ldots, x_n$ are the roots of the polynomial:

$$f(t) = \prod_{i=1}^{n} (t - x_i) = t^n - e_1 t^{n-1} + e_2 t^{n-2} - \cdots + (-1)^n e_n.$$

The coefficients of $f(t)$ lie in F. Thus, K is the splitting field of $f(t)$ over F. Since the variables x_i are distinct indeterminates, $f(t)$ has no repeated roots, implying K/F is a Galois extension.
The symmetric group S_n acts naturally on K by permuting the variables:

$$\sigma \cdot f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Clearly, this action leaves the elementary symmetric polynomials fixed (i.e., $\sigma(e_k) = e_k$). Thus $S_n \subseteq \mathrm{Gal}(K/F)$. Since the Galois group embeds into the permutation group of the roots, and the roots are $x_1, \ldots, x_n$, we have $\mathrm{Gal}(K/F) \subseteq S_n$. Therefore:

$$\mathrm{Gal}(K/F) \cong S_n.$$

This setup leads to the Fundamental Theorem of Symmetric Polynomials, which asserts that the elementary symmetric polynomials form a polynomial basis for all symmetric expressions.

Theorem 3.3. ***Fundamental Theorem of Symmetric Polynomials.***

1. The fixed field of the symmetric group acting on the rational function field is the field generated by the elementary symmetric polynomials:
$$E(x_1, \ldots, x_n)^{S_n} = E(e_1, \ldots, e_n).$$
2. Every symmetric polynomial $f \in E[x_1, \ldots, x_n]$ (i.e., fixed by S_n)

can be written uniquely as a polynomial in the elementary symmetric polynomials:

$$f(x_1, \ldots, x_n) = g(e_1, \ldots, e_n),$$

for a unique $g \in E[y_1, \ldots, y_n]$.

定理

Part (i).

This follows from the Galois correspondence. We established that $\mathrm{Gal}(K/F) \cong S_n$. By the Fundamental Theorem of Galois Theory, the fixed field of the full Galois group is the base field $F = E(e_1, \ldots, e_n)$.

証明終

Existence.

We proceed by induction on the number of variables n. The case $n = 1$ is trivial since $e_1 = x_1$. Assume the result holds for $n - 1$ variables. Let $f(x_1, \ldots, x_n)$ be a symmetric polynomial. Consider the evaluation at $x_n = 0$. Let

$$\bar{f} = f(x_1, \ldots, x_{n-1}, 0).$$

The polynomial $\bar{f}$ is symmetric in variables $x_1, \ldots, x_{n-1}$. By the inductive hypothesis, there exists a polynomial Q such that $\bar{f} = Q(\bar{e}_1, \ldots, \bar{e}_{n-1})$, where $\bar{e}_k$ are the elementary symmetric polynomials in $n - 1$ variables. Note that for $k < n$, $\bar{e}_k = e_k(x_1, \ldots, x_{n-1}, 0)$. Define a candidate polynomial $g_0 = Q(e_1, \ldots, e_{n-1})$ in the original n variables. Consider the difference $h = f - g_0$. Evaluating at $x_n = 0$:

$$h(x_1, \ldots, x_{n-1}, 0) = \bar{f} - Q(\bar{e}_1, \ldots, \bar{e}_{n-1}) = 0.$$

Thus x_n divides h. Since h is symmetric (being the difference of symmetric polynomials), x_i must divide h for all $i = 1, \ldots, n$. Since the x_i are irreducible in the unique factorisation domain $E[x_1, \ldots, x_n]$, their product $e_n = x_1 \cdots x_n$ divides h. So we can write $h = e_n \cdot k$, where k is symmetric. Since $\deg k = \deg f - n < \deg f$, we can proceed by induction on the degree of the polynomial to express k, and hence f, in terms of e_i.

証明終

Uniqueness.

It suffices to show that the elementary symmetric polynomials are algebraically independent over E. Suppose there is a non-trivial relation:

$$\sum_{(i)} c_{(i)} e_1^{i_1} \cdots e_n^{i_n} = 0.$$

We induct on n. For $n = 1$, $e_1 = x_1$ is an indeterminate, so indepen-

dence holds. Assume independence for $n-1$. Setting $x_n = 0$ in the relation gives:

$$\sum_{(i)} c_{(i)} \bar{e}_1^{i_1} \cdots \bar{e}_{n-1}^{i_{n-1}} (0)^{i_n} = 0.$$

Terms with $i_n > 0$ vanish. The remaining sum is a relation among $\bar{e}_1, \ldots, \bar{e}_{n-1}$. By the inductive hypothesis, the coefficients $c_{(i)}$ for $i_n = 0$ must be zero. Thus, every term in the original relation contains a factor of e_n. We can factor out e_n and repeat the argument (induction on total degree) to conclude all coefficients are zero.

証明終

This theorem allows us to determine the Galois group of the "general" polynomial equation. This is the equation where the coefficients are not specific numbers, but independent variables.

Theorem 3.4. ***The Generic Polynomial.***
Let $t_1, \ldots, t_n$ be indeterminates over a field E. Let $F = E(t_1, \ldots, t_n)$. The polynomial

$$f(x) = x^n - t_1 x^{n-1} + t_2 x^{n-2} - \cdots + (-1)^n t_n \in F[x]$$

is irreducible and separable. Its Galois group over F is the symmetric group S_n.

定理

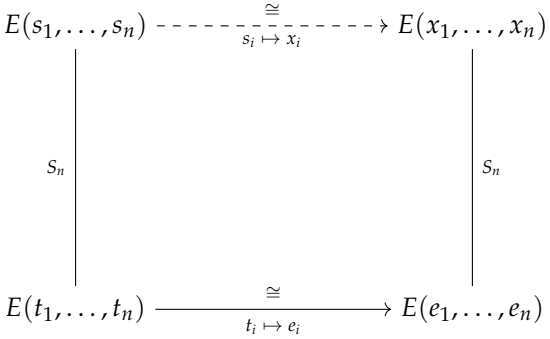


Figure 3.2: Isomorphism between the splitting field of the generic polynomial and the field of rational functions.

Proof

Let $s_1, \ldots, s_n$ be the roots of $f(x)$ in a splitting field K. Then

$$f(x) = \prod_{i=1}^{n} (x - s_i).$$

Comparing coefficients, we see that $t_k = e_k(s_1, \ldots, s_n)$, where e_k are the elementary symmetric polynomials evaluated at the roots. Thus $K = E(s_1, \ldots, s_n)$ and $F = E(e_1(s), \ldots, e_n(s))$.
Consider the field $\tilde{K} = E(x_1, \ldots, x_n)$ of rational functions in independent variables x_i, and let $\tilde{F} = E(e_1(x), \ldots, e_n(x))$. We defined a

map $\varphi : F \to \tilde{F}$ by $t_i \mapsto e_i(x)$. Since the t_i are independent indeterminates, this map is a ring isomorphism, which extends to the fields of fractions. Similarly, the map $\psi : K \to \tilde{K}$ defined by $s_i \mapsto x_i$ is a field isomorphism compatible with φ. Since $\mathrm{Gal}(\tilde{K}/\tilde{F}) \cong S_n$ (by the previous discussion), the isomorphism of fields implies:

$$\mathrm{Gal}(K/F) \cong \mathrm{Gal}(\tilde{K}/\tilde{F}) \cong S_n.$$

Since the Galois group S_n acts transitively on the roots s_i, the polynomial $f(x)$ is irreducible. Since the characteristic is arbitrary but the s_i map to distinct indeterminates x_i, the roots are distinct, so $f(x)$ is separable.

■

Remark.

This result indicates that the "general" equation of degree n has the maximum possible symmetry. Any algebraic relation between the roots of a specific polynomial (with numeric coefficients) corresponds to a reduction in the Galois group to a proper subgroup of S_n.

3.2 *Examples of Galois Extensions*

We now explore concrete examples of Galois extensions. These serve as archetypes for more complex field theoretic structures.

Cyclotomic Extensions

Let F be a field and n a positive integer. Assume that the characteristic of F does not divide n (if $\mathrm{char}(F) = p > 0$, then $p \nmid n$). This ensures the polynomial $x^n - 1$ is separable, as its derivative nx^{n-1} is nonzero at the roots.

Definition 3.4. ***Cyclotomic Extension.***
The splitting field of the polynomial $x^n - 1$ over F is called the **n-th cyclotomic extension** of F, denoted by $F(\zeta_n)$, where ζ_n is a primitive n-th root of unity.

定義

We define the **n-th cyclotomic polynomial** as

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} (x - \zeta_n^k),$$

so that $F(\zeta_n)$ is the splitting field of $\Phi_n(x)$ and $\deg \Phi_n(x) = \varphi(n)$ matches the function $\Phi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ introduced in Chapter 0.

The cyclic subgroup generated by ζ_n will be denoted by C_n whenever a group notation is convenient.
The roots of $x^n - 1$ form a cyclic group of order n under multiplication. A generator of this group is a primitive root ζ_n. Thus $K = F(\zeta_n)$ contains all n roots: $\{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\}$. Since K is the splitting field of a separable polynomial, K/F is Galois.
An automorphism $\sigma \in \mathrm{Gal}(K/F)$ is completely determined by its action on the generator ζ_n. Since $\sigma(\zeta_n)$ must also be a primitive n-th root of unity (to preserve the multiplicative order), we must have:

$$\sigma(\zeta_n) = \zeta_n^a, \quad \text{where } \gcd(a, n) = 1.$$

This defines an injective group homomorphism:

$$\Psi : \mathrm{Gal}(K/F) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times, \quad \sigma \mapsto a \pmod{n}.$$

Consequently, the Galois group is abelian and has order dividing $\varphi(n)$.

Example 3.3. Cyclotomic Extensions of $\mathbb{Q}$. Consider $F = \mathbb{Q}$ and $n = p^m$ for a prime p. The primitive n-th roots of unity are roots of the n-th cyclotomic polynomial:

$$\Phi_{p^m}(x) = \frac{x^{p^m} - 1}{x^{p^{m-1}} - 1} = \sum_{k=0}^{p-1} x^{kp^{m-1}}.$$

Substituting $x \mapsto x + 1$ and applying Eisenstein's Criterion with the prime p shows that $\Phi_{p^m}(x)$ is irreducible over $\mathbb{Q}$. Thus, the degree of the extension is:

$$[\mathbb{Q}(\zeta_{p^m}) : \mathbb{Q}] = \deg \Phi_{p^m}(x) = p^m - p^{m-1} = \varphi(p^m).$$

Since the size of the Galois group equals the degree of the extension, the injection Ψ must be an isomorphism:

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^m})/\mathbb{Q}) \cong (\mathbb{Z}/p^m\mathbb{Z})^\times.$$

範例

Remark.

It is a standard result in number theory (often proved using the irreducibility of $\Phi_n(x)$ for composite n) that for any n, $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Proposition 3.2. ***Subfields of*** $\mathbb{Q}(\zeta_p)$**.**
Let p be an odd prime. The Galois group $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is cyclic of order $p - 1$.

1. The unique element of order 2 in G corresponds to complex conjugation $\sigma : \zeta_p \mapsto \zeta_p^{-1}$.

2. The fixed field of the subgroup $\{1, \sigma\}$ is the maximal real subfield $K^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$.
3. Since G is cyclic, for every divisor d of $p-1$, there is a unique subfield of degree d over $\mathbb{Q}$.

命題

Proof

The map $\sigma(\zeta_p) = \zeta_p^{-1} = \bar{\zeta}_p$ corresponds to the residue -1 in $(\mathbb{Z}/p\mathbb{Z})^\times$. Since $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of even order, it contains a unique element of order 2. Consider the element $\alpha = \zeta_p + \zeta_p^{-1} = 2\cos(2\pi/p)$. This is clearly real and fixed by σ. The polynomial satisfied by ζ_p over $\mathbb{Q}(\alpha)$ is:

$$x^2 - \alpha x + 1 = (x - \zeta_p)(x - \zeta_p^{-1}).$$

Thus $[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\alpha)] = 2$. By the Fundamental Theorem, the fixed field of $\langle\sigma\rangle$ has index 2 in $\mathbb{Q}(\zeta_p)$. Since $\mathbb{Q}(\alpha)$ is contained in this fixed field and has the correct index, they must be equal.

■

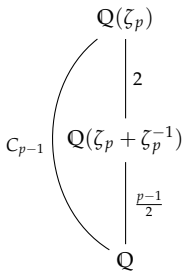


Figure 3.3: The real subfield of a cyclotomic extension.

Finite Fields

The theory of finite fields, discussed in Chapter 1, can be elegantly restated in Galois theoretic terms. Let $F = \mathbb{F}_q$ where $q = p^f$. Let K be an extension of degree n, so $K \cong \mathbb{F}_{q^n}$. K is the splitting field of $x^{q^n} - x$ over F, hence Galois.

Theorem 3.5. ***Galois Group of Finite Fields.***
The Galois group of a finite extension of finite fields is cyclic. Specifically:

$$\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong C_n.$$

It is generated by the q-power Frobenius automorphism $\sigma_q : x \mapsto x^q$.

定理

Proof

Write $q = p^f$. This is the same argument as *theorem 1.4*, with $\sigma_q = \sigma_p^f$ and base field $\mathbb{F}_q$.

■

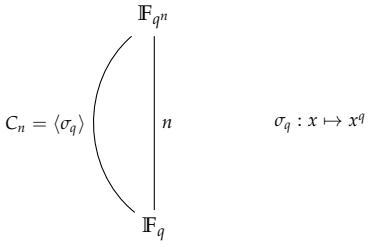


Figure 3.4: The Galois group of a finite field extension is cyclic, generated by Frobenius.

3.3 *Exercises*

1. **Cubic Discriminant and Roots.** Let F be a subfield of $\mathbb{R}$. Let $f(x)$ be an irreducible cubic polynomial in $F[x]$ with discriminant $D(f)$.
   (a) Prove that if $D(f) > 0$, then $f(x)$ has three real roots.
   (b) Prove that if $D(f) < 0$, then $f(x)$ has exactly one real root.

2. **Galois Groups in Characteristic 2.** Let F be a field of characteristic 2. Determine the Galois group of $f(x)$ over F for the following polynomials:
   (a) $f(x) = x^3 + x + 1$
   (b) $f(x) = x^3 + x^2 + 1$

3. **Calculating Galois Groups.** Determine the Galois group of the polynomial $f(x)$ over the field F in each of the following cases:
   (a) $f(x) = x^4 - 5$ over $F = \mathbb{Q}$, $F = \mathbb{Q}(\sqrt{5})$, and $F = \mathbb{Q}(\sqrt{-5})$.
   (b) $f(x) = x^4 - 10x^2 + 4$ over $F = \mathbb{Q}$.

4. **Affine Group Embedding.** Let p be a prime and $a \in \mathbb{Q}$. Suppose $x^p - a$ is irreducible in $\mathbb{Q}[x]$. Prove that the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ of the splitting field is isomorphic to a subgroup of the affine group over $\mathbb{F}_p$, specifically the matrix group:
$$\left\{ \begin{bmatrix} k & l \\ 0 & 1 \end{bmatrix} \middle| \, k \in \mathbb{F}_p^\times, l \in \mathbb{F}_p \right\} \subseteq \mathrm{GL}_2(\mathbb{F}_p).$$

5. **Specific Quartic Extension.** Let $K = \mathbb{Q}(\alpha)$ where $\alpha = \sqrt[4]{2}(1+i)$.
   (a) Prove that $K/\mathbb{Q}$ is a quartic extension.
   (b) Determine the Galois group $\mathrm{Gal}(K/\mathbb{Q})$.

   Adjoin a primitive pth root of unity ζ_p, track $\sigma(\zeta_p)$ and $\sigma(\sqrt[p]{a})$, and use that σ permutes the roots $\zeta_p^i \sqrt[p]{a}$.

6. **Inverse Galois Problem (Finite Fields).** Prove that every finite group is the Galois group of some separable polynomial over some field.

   Consider Cayley's theorem embedding G into S_n and construct a generic polynomial.
   Let G act on $E(x_1, \ldots, x_n)$ by permuting variables; use *Fundamental Theorem of Symmetric Polynomials* and the fixed field.

7. **Binomials and Roots of Unity.** Let F be a field, $c \in F$, and p a prime.
   (a) If $\mathrm{char}(F) = p$, prove that $x^p - c$ is irreducible in $F[x]$ if and only if it has no root in F.
   (b) If $\mathrm{char}(F) \neq p$ and F contains a primitive p-th root of unity, prove that $x^p - c$ is irreducible if and only if it has no root in F.

8. **Kummer Extensions.** Let F contain a primitive n-th root of unity. Let $K = F(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})$. Describe the structure of the Galois group $\mathrm{Gal}(K/F)$.

   Show each automorphism sends $\sqrt[n]{a_i}$ to $\zeta_n^{m_i} \sqrt[n]{a_i}$ and use relations among the a_i.

9. **Splitting Field of $x^4 - 2$.** Let E be the splitting field of $x^4 - 2$ over

$\mathbb{Q}$.

(a) Find all intermediate fields of the extension $E/\mathbb{Q}$.
(b) Identify which intermediate fields are Galois extensions of $\mathbb{Q}$.
(c) Identify pairs of intermediate fields that are conjugate but not equal.

10. Modular Splitting Field. Let E be the splitting field of $x^4 - 2$ over the finite field $\mathbb{F}_5$. Determine the Galois group $\mathrm{Gal}(E/\mathbb{F}_5)$ and list all intermediate fields.

11. Cyclotomic Subfields. For $n \in \{8, 9, 12\}$:

(a) Determine the structure of the group $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.
(b) List all subgroups of G.
(c) Determine the fixed field corresponding to each subgroup.

12. Maximal Real Subfield. Let $n \geq 3$. Prove that the intersection $\mathbb{Q}(\zeta_n) \cap \mathbb{R}$ is the field $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Determine its degree over $\mathbb{Q}$.

13. Gauss Sums. Let p be an odd prime and $\zeta_p = e^{2\pi i/p}$. Let $(\frac{a}{p})$ denote the Legendre symbol, where $(\frac{a}{p}) = 1$ if a is a square modulo p, -1 if not, and 0 when $a \equiv 0$. Define the Gauss sum:

$$g = \sum_{a \in \mathbb{F}_p} \left(\frac{a}{p}\right) \zeta_p^a.$$

Prove the following:

(a)
$$\sum_{a \in \mathbb{F}_p} \zeta_p^a = 0.$$

(b) $g\bar{g} = p$.
(c) $g^2 = (-1)^{(p-1)/2} p$.
(d) Consequently, $\mathbb{Q}(\zeta_p)$ contains a unique quadratic subfield

$$K = \mathbb{Q}(\sqrt{(-1)^{(p-1)/2} p}).$$

Expand $g\bar{g}$ and use the orthogonality of additive characters.
Relate g^2 to $g\bar{g}$ by evaluating $\sum_a (\frac{a}{p}) \zeta_p^{ka}$ for k a square or nonsquare.

4
Solvability by Radicals

The historical impetus for the development of Galois theory was the search for a general formula to find the roots of polynomial equations of degree $n \geq 5$. While quadratic, cubic, and quartic equations admit solutions expressible via arithmetic operations and n-th roots (radicals), this pattern appeared to break down for higher degrees. In this chapter, we utilise the Fundamental Theorem of Galois Theory to translate this problem into group theory. We establish the precise relationship between the existence of a radical formula and the algebraic structure of the Galois group.

4.1 Radical Extensions

We begin by formalising the notion of "solving by radicals". This corresponds to constructing a field extension by successively adjoining n-th roots of elements.

Definition 4.1. ***Radical Extension.***
Let F be a field.

1. A **simple radical extension** is an extension K/F such that $K = F(d)$, where $d^n = a$ for some $a \in F$ and integer $n \geq 1$. We often write $K = F(\sqrt[n]{a})$.
2. An extension K/F is a **radical extension** (or solvable by radicals) if there exists a finite tower of fields

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = K,$$

where each F_i/F_{i-1} is a simple radical extension. This tower is called a **radical tower**.

定義

Definition 4.2. ***Radical Solvability of Equations.***
Let $f(x) \in F[x]$ be a monic polynomial of degree $n \geq 1$. The equation $f(x) = 0$ is **radically solvable** over F if the splitting field K of $f(x)$ is contained in some extension E which possesses a radical tower over

F:

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = E, \quad \text{with } K \subseteq E.$$

定義

Note

The splitting field K need not be a radical extension itself; it suffices that K is contained in one. This accounts for auxiliary roots of unity required to express solutions (e.g., the cubic formula requires $\sqrt{-3}$).

The solvability of an equation corresponds to a specific property of its Galois group.

Definition 4.3. ***Solvable Group.***
A finite group G is **solvable** if there exists a chain of subgroups (a subnormal series)

$$\{1\} = G_k \triangleleft G_{k-1} \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G,$$

such that each quotient group G_i/G_{i+1} is abelian.

定義

Remark.

By the classification of finite abelian groups, one can refine this series such that each factor G_i/G_{i+1} is a cyclic group of prime order. Key properties of solvable groups include:

1. Subgroups and quotient groups of solvable groups are solvable.
2. If $N \triangleleft G$, then G is solvable if and only if both N and G/N are solvable.
3. The symmetric group S_n is solvable for $n \leq 4$, but **not solvable** for $n \geq 5$ (as A_n is simple and non-abelian for $n \geq 5$).

This group-theoretic distinction is the obstruction to solving general quintic equations.

4.2 *Galois' Criterion*

We now state the main equivalence theorem. Throughout this section, we assume $\mathrm{char}(F) = 0$ to avoid separability issues.

Theorem 4.1. ***Galois' Solvability Theorem.***
Let F be a field of characteristic 0 and $f(x) \in F[x]$. Let K be the splitting field of f over F. The equation $f(x) = 0$ is radically solvable over F if and only if $\mathrm{Gal}(K/F)$ is a solvable group.

定理

An immediate consequence of this theorem, combined with the

known structure of the symmetric group, is the Abel–Ruffini theorem.

Theorem 4.2. ***Unsolvability of the General Quintic.***
Let $n \geq 5$ and let $t_1, \ldots, t_n$ be independent indeterminates over a field F of characteristic 0. The general equation

$$f(x) = x^n - t_1 x^{n-1} + \cdots + (-1)^n t_n = 0$$

is not radically solvable over the field $L = F(t_1, \ldots, t_n)$.

定理

Proof

By *theorem 3.4*, the Galois group of the general polynomial over L is isomorphic to the symmetric group S_n. For $n \geq 5$, S_n is not a solvable group (the alternating group A_n is the unique non-trivial normal subgroup and is simple non-abelian). By *theorem 4.1*, the equation is not solvable by radicals.

■

4.3 *Proof of the Solvability Theorem*

To prove *theorem 4.1*, we require several auxiliary results connecting cyclic extensions to simple radical extensions. This connection is mediated by roots of unity.

Kummer Extensions

Lemma 4.1. ***Kummer Extensions.***
Let F be a field containing a primitive p-th root of unity ζ_p, where p is a prime. Let K/F be a cyclic extension of degree p. Then K is a radical extension of the form $K = F(\sqrt[p]{a})$ for some $a \in F$.

引理

Proof

Let $\mathrm{Gal}(K/F) = \langle \sigma \rangle \cong C_p$. Choose an element $c \in K \setminus F$. We construct a "Lagrange resolvent" to diagonalise the action of σ. Define the elements $d_i \in K$ for $i = 0, \ldots, p-1$ by:

$$d_i = c + \zeta_p^i \sigma(c) + \zeta_p^{2i} \sigma^2(c) + \cdots + \zeta_p^{(p-1)i} \sigma^{p-1}(c).$$

Applying σ to d_i:

$$\begin{aligned} \sigma(d_i) &= \sigma(c) + \zeta_p^i \sigma^2(c) + \cdots + \zeta_p^{(p-2)i} \sigma^{p-1}(c) + \zeta_p^{(p-1)i} c \\ &= \zeta_p^{-i} \left(\zeta_p^i \sigma(c) + \cdots + c \right) \\ &= \zeta_p^{-i} d_i. \end{aligned}$$

Thus, $\sigma(d_i^p) = (\sigma(d_i))^p = (\zeta_p^{-i} d_i)^p = (\zeta_p^p)^{-i} d_i^p = d_i^p$. Since d_i^p is fixed by the generator σ, it is fixed by the entire group, so $d_i^p = a_i \in F$.
It remains to show that for some i, $d_i \notin F$. We can write the definition of the d_i as a matrix-vector product. Let $c_k = \sigma^k(c)$ for $k = 0, \dots, p-1$.

$$\begin{bmatrix} d_0 \\ d_1 \\ \vdots \\ d_{p-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \zeta_p & \zeta_p^2 & \dots & \zeta_p^{p-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_p^{p-1} & \zeta_p^{2(p-1)} & \dots & \zeta_p^{(p-1)(p-1)} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{p-1} \end{bmatrix}.$$

The matrix is a Vandermonde matrix in the variables $1, \zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}$. Since ζ_p is a primitive root, these values are distinct, so the determinant is non-zero. Since $c \notin F$, the vector $(c_0, \dots, c_{p-1})$ is not a multiple of $(1, \dots, 1)$. Specifically, $K = F(c)$, so not all d_i can lie in F (otherwise c would be a linear combination of elements in F). Thus there exists some $d = d_i$ such that $K = F(d)$ and $d^p \in F$.

■

Preservation of Solvability

We establish that solvability properties are robust under base change and closure.
We use the notation in *Figure 4.1*.

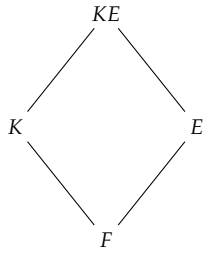


Figure 4.1: The compositum KE

Definition 4.4. ***Normal Closure.***
Let E/F be a finite extension. The **normal closure** of E over F is the smallest normal extension of F containing E (in the sense of *definition 2.8*). This is the same field as the Galois Closure.

定義

Lemma 4.2. ***Galois Group under Base Change.***
Let K be the splitting field of a polynomial $f(x) \in F[x]$. Let E/F be any field extension. Then the splitting field of $f(x)$ over E is KE, and there is an injective homomorphism:

$$\mathrm{Gal}(KE/E) \hookrightarrow \mathrm{Gal}(K/F), \quad \sigma \mapsto \sigma|_K.$$

引理

Proof
Let $K = F(\alpha_1, \dots, \alpha_n)$ where α_i are the roots of f. Then $KE = E(\alpha_1, \dots, \alpha_n)$ is clearly the splitting field over E. For any

$\sigma \in \mathrm{Gal}(KE/E)$, σ permutes the roots α_i. Since K is generated by these roots, $\sigma(K) = K$. Thus the restriction $\sigma|_K$ is an automorphism of K. Since σ fixes E, it fixes F, so $\sigma|_K \in \mathrm{Gal}(K/F)$. The map is a homomorphism. If $\sigma|_K = \mathrm{id}$, then σ fixes all α_i. Since σ also fixes E, it fixes the generating set $E \cup \{\alpha_i\}$ of KE. Thus $\sigma = \mathrm{id}$.

■

Lemma 4.3. ***Normal Closure of Radical Towers.***
Let E/F be a finite extension. If E is contained in a radical tower over F, then the normal closure N of E over F is also contained in a radical tower over F.

引理

Proof

Let $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m$ be a radical tower with $E \subseteq F_m$. Let $F_i = F_{i-1}(d_i)$ with $d_i^{n_i} \in F_{i-1}$. We proceed by induction on the length of the tower. Let M be the normal closure of F_m over F. M is generated over F by all conjugates of the elements in F_m. Let $f_i(x)$ be the minimal polynomial of d_i over F. Let the roots of f_i in M be $\{d_{i,j}\}$. If F_{i-1} is contained in a normal radical tower M_{i-1}, then adjoining all conjugates $d_{i,j}$ to M_{i-1} results in a radical extension. Specifically, if $d_i^{n_i} = a \in F_{i-1}$, then for any $\sigma \in \mathrm{Gal}(M/F)$, $(\sigma d_i)^{n_i} = \sigma a \in \sigma F_{i-1} \subseteq M_{i-1}$. Thus we can construct a tower for M by successively adjoining roots of conjugates.

■

See 4.2 for the field diagram used in the proof.

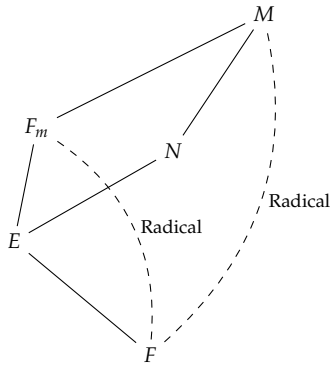


Figure 4.2: Radical solvability lifts to the normal closure

Proof of theorem 4.1

We are now equipped to prove the main theorem.

Sufficiency ($\Longrightarrow$)

Suppose $f(x)$ is radically solvable. Let K be the splitting field. By definition and *lemma 4.3*, there exists a radical tower $F = F_0 \subseteq \cdots \subseteq F_m$ such that $K \subseteq F_m$ and F_m/F is Galois (replacing the top field with its normal closure). We define a refined tower by adjoining primitive roots of unity. Let N be the least common multiple of the exponents appearing in the radical tower. Let ζ be a primitive N-th root of unity. Consider the tower:

$$F \subseteq F(\zeta) = F_0' \subseteq F_1' \subseteq \cdots \subseteq F_m' = F_m(\zeta).$$

- The extension $F(\zeta)/F$ is cyclotomic, hence abelian (and solvable).
- Each step $F_i' = F_{i-1}'(d_i)$ is a radical extension where the base field F_{i-1}' contains the requisite roots of unity. By standard Kummer theory arguments (converse of *lemma 4.1*), such extensions are

abelian.
Thus $\mathrm{Gal}(F_m(\zeta)/F)$ is a solvable group (being an extension of abelian groups by abelian groups). Since $K \subseteq F_m \subseteq F_m(\zeta)$, $\mathrm{Gal}(K/F)$ is a quotient of a subgroup of a solvable group. Thus $\mathrm{Gal}(K/F)$ is solvable.

証明終

Necessity ($\Longleftarrow$)

Suppose $G = \mathrm{Gal}(K/F)$ is solvable. Let $[K : F] = n$. Let ζ be a primitive n-th root of unity. Consider the extension $K(\zeta)/F(\zeta)$. By *lemma 4.2*, its Galois group H injects into G. Since G is solvable, H is solvable. Let

$$\{1\} = H_k \triangleleft H_{k-1} \triangleleft \cdots \triangleleft H_0 = H$$

be a composition series where factors are cyclic of prime order. By the Fundamental Theorem of Galois Theory, this corresponds to a tower of fields:

$$F(\zeta) = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_k = K(\zeta).$$

Since H_i/H_{i+1} is cyclic of prime order p and E_i contains primitive roots of unity (as $p \mid |H| \mid n$), *lemma 4.1* implies that each step E_{i+1}/E_i is a simple radical extension. Finally, $F(\zeta)/F$ is a radical extension (adjoining roots of unity). Thus $F \subseteq F(\zeta) \subseteq \cdots \subseteq K(\zeta)$ is a radical tower containing K.

証明終

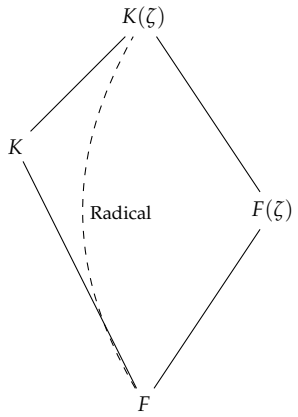


Figure 4.3: Adjoining roots of unity

4.4 *Proofs of the Main Theorems*

In this final section, we provide the rigorous proofs for the fundamental structural results of Galois theory. While we have utilised these theorems to explore examples and solvability, their proofs reveal the deep interplay between linear algebra and field theory that underpins the subject.

The Primitive Element Theorem

We first supply the complete proof for the existence of a single generator for finite separable extensions.

Proof of the Primitive Element Theorem

We prove *Primitive Element Theorem* from Chapter 2; see *theorem 2.2* for the statement. Let $K = F(\alpha_1, \ldots, \alpha_n)$ be a finite separable extension. If F is a finite field, the multiplicative group $K^\times$ is cyclic (*Finite Subgroups of Fields*). Let γ be a generator; then $K = F(\gamma)$.

Assume F is infinite. By induction, it suffices to consider the case $K = F(\alpha, \beta)$. Let $f(x)$ and $g(x)$ be the minimal polynomials of α and β over F, respectively. Let E be a splitting field for $f(x)g(x)$ containing K. Let $\alpha_1, \ldots, \alpha_r$ be the distinct roots of $f(x)$ in E (with $\alpha_1 = \alpha$), and let $\beta_1, \ldots, \beta_s$ be the distinct roots of $g(x)$ in E (with $\beta_1 = \beta$). The roots are distinct because the extension is separable. We seek an element of the form $\gamma = \alpha + c\beta$ with $c \in F$. For this γ to generate K, we essentially need to ensure that the linear combination distinguishes the roots. Specifically, we require that for any $j \neq 1$, $\alpha_i + c\beta_j \neq \alpha + c\beta$. Consider the linear equations:

$$\alpha_i + x\beta_j = \alpha + x\beta.$$

For each pair (i, j) with $j \neq 1$, there is at most one solution for x in E:

$$x = \frac{\alpha_i - \alpha}{\beta - \beta_j}.$$

Since F is infinite, we can choose $c \in F$ distinct from these finitely many ratios. Let $\gamma = \alpha + c\beta$. Clearly $F(\gamma) \subseteq F(\alpha, \beta)$. To show the reverse inclusion, notice that β satisfies $g(\beta) = 0$, and also satisfies the polynomial $h(x) = f(\gamma - cx)$ (since $h(\beta) = f(\alpha) = 0$). Thus β is a common root of $g(x)$ and $h(x)$ in the ring $F(\gamma)[x]$. In $E[x]$, the roots of $g(x)$ are $\beta_1, \ldots, \beta_s$. The roots of $h(x) = f(\gamma - cx)$ are values ξ such that $\gamma - c\xi = \alpha_k$ for some k, i.e., $\xi = (\gamma - \alpha_k)/c = (\alpha + c\beta - \alpha_k)/c$. If β were a common root other than β_1, then for some $j \neq 1$, we would have $\beta_j = (\alpha + c\beta - \alpha_k)/c$, implying $\alpha + c\beta = \alpha_k + c\beta_j$. This contradicts our choice of c. Therefore, $\gcd(g(x), h(x)) = x - \beta$. Since the GCD of two polynomials can be computed in the field containing their coefficients, $x - \beta \in F(\gamma)[x]$. Thus $\beta \in F(\gamma)$, and consequently $\alpha = \gamma - c\beta \in F(\gamma)$. Hence $F(\alpha, \beta) = F(\gamma)$.

■

Linear Independence of Automorphisms

The engine driving the correspondence between fields and groups is the linear independence of characters.

Definition 4.5. ***Linear Independence of Characters.***
Let G be a group and K a field. A set of distinct homomorphisms $\chi_1, \ldots, \chi_n : G \to K^\times$ is **linearly independent** over K if the equation

$$a_1\chi_1(g) + \cdots + a_n\chi_n(g) = 0 \quad \text{for all } g \in G$$

implies $a_1 = \cdots = a_n = 0$.

定義

Lemma 4.4. ***Dedekind's Lemma.***
Distinct field automorphisms are linearly independent. That is, if $\sigma_1, \ldots, \sigma_n$ are distinct automorphisms of K, they are linearly independent over K.

引理

Proof

Suppose there exists a non-trivial relation $\sum_{i=1}^{m} a_i \sigma_i(x) = 0$ for all $x \in K$. We choose a relation with the minimal number of non-zero coefficients m. Clearly $m \geq 2$. By dividing by a_1, we may assume $a_1 = 1$. Since $\sigma_1 \neq \sigma_m$, there exists $y \in K$ such that $\sigma_1(y) \neq \sigma_m(y)$. Substitute yx into the relation:

$$\sum_{i=1}^{m} a_i \sigma_i(y)\sigma_i(x) = 0.$$

Multiply the original relation by $\sigma_m(y)$:

$$\sum_{i=1}^{m} a_i \sigma_m(y)\sigma_i(x) = 0.$$

Subtracting these gives a new relation:

$$\sum_{i=1}^{m-1} a_i(\sigma_i(y) - \sigma_m(y))\sigma_i(x) = 0.$$

The coefficient for σ_1 is $\sigma_1(y) - \sigma_m(y) \neq 0$. Thus we have found a non-trivial relation with fewer terms, contradicting minimality.

■

This leads to the crucial inequality relating the degree of an extension to the size of the automorphism group. This result is often referred to as **Artin's Lemma**.

Theorem 4.3. ***Artin's Theorem on Invariant Fields.***
Let G be a finite subgroup of $\mathrm{Aut}(K)$. Let $F = K^G$ be the fixed field. Then:

$$[K : F] = |G|.$$

定理

Let $n = |G|$ and $G = \{\sigma_1 = \mathrm{id}, \ldots, \sigma_n\}$.

Proof that $[K : F] \leq n$.

Suppose for contradiction that $[K : F] > n$. Let $u_1, \ldots, u_{n+1}$ be linearly independent elements of K over F. Consider the system of

linear equations in unknowns x_j:

$$\sum_{j=1}^{n+1} \sigma_i(u_j)x_j = 0, \quad \text{for } i = 1, \dots, n.$$

This is a homogeneous system of n equations in $n + 1$ variables with coefficients in K. It must have a non-trivial solution $(c_1, \dots, c_{n+1})$ in K. Let us choose a solution with the minimal number of non-zero entries. By reordering, let $c_1 \neq 0$. Normalising, we may set $c_1 = 1$. The equation for $\sigma_1 = \text{id}$ is $\sum u_j c_j = 0$. Since the u_j are independent over F, not all c_j can lie in F. Suppose $c_k \notin F$. Since $c_k \notin K^G$, there exists $\sigma_r \in G$ such that $\sigma_r(c_k) \neq c_k$. Applying σ_r to the system:

$$\sum_j \sigma_r(\sigma_i(u_j))\sigma_r(c_j) = 0.$$

As σ_i ranges over G, so does $\sigma_r\sigma_i$. Thus $(\sigma_r(c_1), \dots, \sigma_r(c_{n+1}))$ is also a solution to the system (permuted). Subtracting this from the original solution:

$$\sum_{j=1}^{n+1} \sigma_i(u_j)(c_j - \sigma_r(c_j)) = 0.$$

The first component is $1 - \sigma_r(1) = 0$. The k-th component is $c_k - \sigma_r(c_k) \neq 0$. Thus we have constructed a non-trivial solution with strictly fewer non-zero entries, a contradiction. Hence $[K : F] \leq |G|$.

証明終

Proof that $[K : F] \geq n$.

Let $G = \text{Gal}(K/F)$. We have already established in *proposition* 0.6 that $|G| \leq [K : F]$ for any finite extension. However, proving $[K : F] \geq |G|$ is immediate from the Primitive Element Theorem if K/F is separable. Let $K = F(\gamma)$.
Let

$$h(x) = \prod_{\sigma \in G} (x - \sigma(\gamma)).$$

The coefficients of h are fixed by G, so $h \in F[x]$. Since γ is a root, the minimal polynomial $m(x)$ divides $h(x)$. Thus $[K : F] = \deg m \leq \deg h = |G|$.
Combining with the first part, if $F = K^G$, we must have $[K : F] = |G|$.

証明終

Corollary 4.1. *Galois Extensions are Normal and Separable.* If $F = K^G$ for a finite group G, then K is a separable normal extension of F.

推論

Proof

For any $\beta \in K$, let $\mathcal{O} = \{\sigma(\beta) \mid \sigma \in G\} = \{\beta_1, \ldots, \beta_r\}$ be its orbit. The polynomial $g(x) = \prod_{i=1}^{r}(x - \beta_i)$ is separable and invariant under G, so $g(x) \in F[x]$. Since β is a root, the minimal polynomial of β divides $g(x)$, hence splits completely in K with distinct roots. Thus the extension is normal and separable.

■

Proof of the Fundamental Theorem

We now assemble these results to prove *theorem* 2.4. Let K/F be a Galois extension with group G.

Proof of the Fundamental Theorem of Galois Theory

The Correspondence: Let $H \leq G$ be a subgroup. Let $L = K^H$. By *theorem* 4.3, $[K : L] = |H|$. Conversely, let L be an intermediate field. Let $H = \mathrm{Gal}(K/L)$. By definition, $L \subseteq K^H$. Since K/F is Galois, K is the splitting field of a separable polynomial over F, and thus also over L. Hence K/L is Galois. By the equality of degree and group order: $[K : L] = |H|$. Also $[K : K^H] = |H|$ by Artin's Theorem. Thus $[K : L] = [K : K^H]$, implying $L = K^H$. Therefore, the maps $H \mapsto K^H$ and $L \mapsto \mathrm{Gal}(K/L)$ are inverses.

Degrees: We have $[K : L] = |H|$. By the Tower Law and Lagrange's Theorem:

$$[L : F] = \frac{[K : F]}{[K : L]} = \frac{|G|}{|H|} = (G : H).$$

Conjugation: Let $H \leftrightarrow L$. The field corresponding to the conjugate subgroup $\sigma H \sigma^{-1}$ is:

$$K^{\sigma H \sigma^{-1}} = \{x \in K \mid \sigma h \sigma^{-1}(x) = x \quad \forall h \in H\}.$$

Let $y = \sigma^{-1}(x)$. The condition becomes $h(y) = y$, i.e., $y \in L$. Thus $x \in \sigma(L)$. So $\sigma H \sigma^{-1} \leftrightarrow \sigma(L)$.

Normality: L/F is normal $\iff$ $\sigma(L) = L$ for all $\sigma \in G$ (since any embedding into an algebraic closure corresponds to restriction of an automorphism of K). By the conjugation relation, $\sigma(L) = L \iff \sigma H \sigma^{-1} = H$. Thus L/F is normal $\iff H \triangleleft G$. In this case, the map $G \to \mathrm{Gal}(L/F)$ given by restriction $\sigma \mapsto \sigma|_L$ is a surjective homomorphism with kernel H. By the First Isomorphism Theorem:

$$\mathrm{Gal}(L/F) \cong G/H.$$

■

4.5 *Exercises*

1. **Explicit Radicals.** Express the following trigonometric values in terms of radicals:
   (a) $\cos 20^\circ$ (Note: While not constructible, it is radically solvable).
   (b) $\cos \frac{360^\circ}{7}$.

2. **Cardano's Formula.** Let F be a field of characteristic o and $f(x) = x^3 - t_1x^2 + t_2x - t_3 \in F(t_1, t_2, t_3)[x]$. Derive the explicit formula for the roots x_1, x_2, x_3 in terms of the coefficients and the cube roots of unity ω. Define $p = t_2 - t_1^2/3$ and $q = t_1t_2/3 - 2t_1^3/27 - t_3$. Let

$$\alpha = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}, \quad \beta = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

   Verify that $x_1 = t_1/3 + \alpha + \beta$ is a root, provided $\alpha\beta = -p/3$.

3. **Solving Equations.** Find all complex roots of the following polynomials:
   (a) $x^3 - 2x + 4 = 0$
   (b) $x^3 - 15x + 4 = 0$
   (c) $x^4 - 2x^3 - 8x - 3 = 0$

4. **Inseparability and Solvability.** Let $F = \mathbb{F}_p(t)$. Consider the equation $x^p - x - t = 0$.
   (a) Prove that the Galois group of the splitting field is cyclic (hence solvable).
   (b) Prove that the equation is **not** solvable by radicals over F.
   (c) Explain why this does not contradict Galois' Solvability Theorem (check the characteristic).

5. **Invariant Fields of Rational Functions.** Let $E = \mathbb{C}(t)$. Let $\sigma, \tau \in \mathrm{Aut}(E)$ be defined by $\sigma(t) = \omega t$ (where $\omega = e^{2\pi i/3}$) and $\tau(t) = t^{-1}$.
   (a) Prove that the subgroup $H = \langle \sigma, \tau \rangle$ has order 6 and is isomorphic to S_3.
   (b) Determine the fixed field E^H. Show it is $\mathbb{C}(t^3 + t^{-3})$.

6. **Artin-Schreier Invariants.** Let F be a field of characteristic p. Let $\sigma \in \mathrm{Aut}(F(x))$ be defined by $\sigma(x) = x + 1$. Let $H = \langle \sigma \rangle$.
   (a) Prove $|H| = p$.
   (b) Determine the fixed field $F(x)^H$.

7. **Artin-Schreier Galois Groups.** Let F be a field of characteristic p and $a \in F$. Suppose $f(x) = x^p - x - a$ is irreducible. Let α be a root. Prove that $F(\alpha)/F$ is a Galois extension and determine its Galois group.

8. **Galois Translation Theorem.** Let L and M be subfields of a larger field E. Suppose L is a finite Galois extension of $L \cap M$. Prove that LM is a Galois extension of M and that there is a natural isomorphism:

$$\mathrm{Gal}(LM/M) \cong \mathrm{Gal}(L/L \cap M).$$

9. **Normal Closures and Intersections.** Let E/F be a finite Galois extension with intermediate fields N, M such that $F \subseteq M \subseteq N \subseteq E$. Suppose N is the normal closure of M over F. Prove that:

$$\mathrm{Gal}(E/N) = \bigcap_{\sigma \in \mathrm{Gal}(E/F)} \sigma \mathrm{Gal}(E/M)\sigma^{-1}.$$

10. **Prime Degree Extensions.** Let E/F be a finite Galois extension. Suppose that for every intermediate field K with $F \subsetneq K \subseteq E$, the degree $[K : F]$ is the same. Prove that $[E : F]$ must be a prime number.

11. **Multiquadratic Extensions.**
    (a) Prove that $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ is a Galois extension of $\mathbb{Q}$ and determine its Galois group.
    (b) Find the minimal polynomial of $\alpha = \sqrt{6} + \sqrt{10} + \sqrt{15}$ over $\mathbb{Q}$.
    (c) Prove that $\sqrt{6} \in \mathbb{Q}(\alpha)$.
    (d) Find the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over the field $\mathbb{Q}(\alpha)$.

5
R-Modules

We have previously explored fields and vector spaces, where scalars can be inverted. We now generalise this structure to rings, where scalars need not be invertible. The resulting object, an R-module, is the fundamental tool for algebraic number theory and homological algebra.

5.1 Definitions and Examples

Definition 5.1. ***R*-Module.**
Let R be a ring. An R**-module** M is a set equipped with two operations:

$$+_M : M \times M \to M, \qquad \cdot_M : R \times M \to M,$$

satisfying the following axioms for all $r, r' \in R$ and $m, m' \in M$:

1. $(M, +_M)$ is an abelian group with identity 0_M.
2. Distributivity over vector addition: $r \cdot (m + m') = rm + rm'$.
3. Distributivity over scalar addition: $(r + r') \cdot m = rm + r'm$.
4. Associativity of scalars: $(rr') \cdot m = r \cdot (r'm)$.
5. Identity: $1_R \cdot m = m$.

定義

The structure of a module can be reinterpreted through the lens of ring homomorphisms.

Remark.

For an abelian group M, let $\mathrm{End}(M)$ denote the set of group endomorphisms (homomorphisms from M to M). Under pointwise addition and composition, $\mathrm{End}(M)$ forms a (generally non-commutative) ring. The scalar multiplication on an R-module M is equivalent to a ring homomorphism $\phi : R \to \mathrm{End}(M)$, defined by $\phi(r)(m) = r \cdot m$. The axioms ensure that this map respects the ring structure of R.

Example 5.1. Basic Module Structures.

- The ring R is naturally an R-module over itself, using its internal addition and multiplication.
- Any ideal $I \subseteq R$ is an R-module under the operations restricted from R.
- If R is a field, the axioms of an R-module are identical to those of a vector space. Thus, R-modules over a field are simply vector spaces.

範例

Example 5.2. Abelian Groups. Let $R = \mathbb{Z}$. Any abelian group M admits a unique $\mathbb{Z}$-module structure. The axiom $1 \cdot m = m$ combined with additivity forces the definition:

$$n \cdot m = \begin{cases} \underbrace{m + \cdots + m}_{n \text{ times}} & \text{if } n > 0, \\ 0_M & \text{if } n = 0, \\ \underbrace{(-m) + \cdots + (-m)}_{|n| \text{ times}} & \text{if } n < 0. \end{cases}$$

Thus, the study of abelian groups is equivalent to the study of $\mathbb{Z}$-modules.

範例

Example 5.3. Change of Rings. Let $f : R \to S$ be a ring homomorphism.

- The ring S becomes an R-module via the action $r \cdot s = f(r)s$. Here, the scalar multiplication uses the map f to interpret elements of R as elements of S.
- More generally, if M is an S-module, it inherits an R-module structure via restriction of scalars:

$$r \cdot m = f(r) \cdot_S m.$$

- In particular, if I is an ideal of R, the quotient map $\pi : R \to R/I$ allows any R/I-module to be viewed as an R-module. In this case, I acts trivially: for any $r \in I$, $r \cdot m = 0$. We say I **annihilates** M.
- Conversely, if M is an R-module annihilated by I, it admits a well-defined R/I-module structure defined by $(r + I) \cdot m = rm$. This is well-defined because if $r + I = r' + I$, then $r - r' \in I$, so $(r - r')m = 0$, implying $rm = r'm$.

範例

Example 5.4. Function Modules. Let S be a set and let M_S be the set of all functions $f : S \to R$. We define addition and scalar multiplication pointwise:

$$(f+g)(s) = f(s) + g(s), \qquad (r \cdot f)(s) = r \cdot f(s).$$

This makes M_S into an R-module. Consider the subset of functions with finite support:

$$\mathcal{F}_S = \{f \in M_S \mid f(s) = 0 \text{ for all but finitely many } s \in S\}.$$

This subset is closed under the module operations and forms the **free R-module on the set S**.

範例

5.2 *Submodules and Quotients*

Just as we analyse groups via subgroups and rings via ideals, we investigate modules through submodules.

Definition 5.2. ***Submodule.***
Let M be an R-module. A subset $N \subseteq M$ is an **R-submodule** if it is closed under addition and scalar multiplication:

1. For all $n, n' \in N$, $n + n' \in N$ (i.e., N is a subgroup of M).
2. For all $r \in R$ and $n \in N$, $rn \in N$.

定義

Note that the ideals of R are precisely the R-submodules of R when viewed as a module over itself.

Definition 5.3. ***Generated Submodules.***
Let S be a subset of an R-module M. The submodule **generated** by S is the set of all finite linear combinations of elements of S with coefficients in R:

$$\langle S \rangle = \left\{ \sum_{i=1}^{k} r_i s_i \;\middle|\; r_i \in R, s_i \in S, k \in \mathbb{N} \right\}.$$

This is the smallest submodule of M containing S. If there exists a finite set S such that $\langle S \rangle = M$, we say M is a **finitely generated** R-module.

定義

Quotient Modules

Given a submodule $N \subseteq M$, we can construct a quotient structure.

Definition 5.4. ***Quotient Module.***
Let N be a submodule of M. We define a congruence relation on M by:

$$m \equiv m' \pmod{N} \iff m - m' \in N.$$

The equivalence classes are the cosets $m + N$. The set of these classes, denoted M/N, forms an R-module under the operations:

$$(m + N) + (m' + N) = (m + m') + N,$$

$$r \cdot (m + N) = (rm) + N.$$

This is called the **quotient** of M by N.

定義

The well-definedness of scalar multiplication follows from the submodule property: if $m - m' \in N$, then $r(m - m') = rm - rm' \in N$, so $rm \equiv rm' \pmod{N}$. The natural map $\pi : M \to M/N$ given by $m \mapsto m + N$ is a module homomorphism.

Direct Sums

Definition 5.5. ***Direct Sum.***
Let M_1 and M_2 be R-modules. The **direct sum** $M_1 \oplus M_2$ is the set of ordered pairs (m_1, m_2) with component-wise operations:

$$(m_1, m_2) + (m_1', m_2') = (m_1 + m_1', m_2 + m_2'),$$

$$r \cdot (m_1, m_2) = (rm_1, rm_2).$$

定義

Example 5.5. Quotients by Ideals. Let M be an R-module and I an ideal of R. We can form the submodule IM generated by products of scalars in I and vectors in M:

$$IM = \left\{ \sum_{j=1}^{k} i_j m_j \;\middle|\; i_j \in I, m_j \in M \right\}.$$

The quotient M/IM is an R-module. Since every element of I annihilates this quotient (mapping elements to the zero coset), M/IM naturally carries the structure of an R/I-module. The scalar multiplication is defined by:

$$(r + I) \cdot (m + IM) = rm + IM.$$

To verify this is well-defined, suppose $r - r' \in I$ and $m - m' \in IM$. Then:

$$rm - r'm' = r(m - m') + (r - r')m'.$$

The first term is in IM because $m - m' \in IM$ and IM is a submodule. The second term is in IM because $r - r' \in I$ implies $(r - r')m' \in IM$. Thus the difference lies in IM.

範例

5.3 *Homomorphisms and Free Modules*

Having established the structural definitions of submodules and quotients, we turn our attention to the maps between modules that preserve this structure.

Module Homomorphisms

Definition 5.6. ***Module Homomorphism.***
Let M and N be R-modules. A map $f : M \to N$ is an **R-module homomorphism** (or simply an R-linear map) if it satisfies:
1. Additivity: $f(m + m') = f(m) + f(m')$ for all $m, m' \in M$.
2. R-linearity: $f(rm) = rf(m)$ for all $r \in R, m \in M$.

The set of all such homomorphisms is denoted $\mathrm{Hom}_R(M, N)$.

定義

Remark.

It is crucial to distinguish between ring homomorphisms and module homomorphisms. A ring homomorphism $\phi : R \to R$ must satisfy multiplicative splitting $\phi(rr') = \phi(r)\phi(r')$, whereas an R-module homomorphism $f : R \to R$ treats the first scalar as a coefficient: $f(rr') = rf(r')$.

The structural kernels and images behave exactly as they do in group theory.

Definition 5.7. ***Kernel and Image.***
Let $f : M \to N$ be an R-module homomorphism.
- The **kernel** of f is $\ker f = \{m \in M \mid f(m) = 0\}$.
- The **image** of f is $\mathrm{im}\, f = \{n \in N \mid \exists m \in M, f(m) = n\}$.

定義

It is a standard verification that $\ker f$ is a submodule of M and $\mathrm{im}\, f$ is a submodule of N. Consequently, we may construct the quotient $M/\ker f$.

Proposition 5.1. ***Universal Property of the Quotient.***
Let N be a submodule of M and let $\pi : M \to M/N$ be the canonical projection. Let $f : M \to M'$ be an R-module homomorphism such

that $N \subseteq \ker f$. Then there exists a unique homomorphism $\bar{f} : M/N \to M'$ such that $\bar{f} \circ \pi = f$.

命題

Proof

The proof is identical to that for quotient rings. We define $\bar{f}(m+N) = f(m)$. This is well-defined because if $m - m' \in N$, then $f(m-m') = 0$, so $f(m) = f(m')$. Linearity follows from the linearity of f.

■

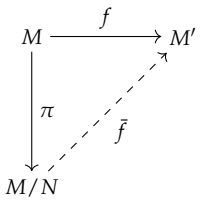


Figure 5.1: The universal property of the quotient module.

Free Modules

In vector spaces, the existence of a basis is guaranteed (assuming the Axiom of Choice), allowing any vector space to be non-canonically identified with a direct sum of copies of the field. For modules over arbitrary rings, bases need not exist. Modules that do admit a basis are termed *free*.

Definition 5.8. ***Basis and Free Modules.***
Let M be an R-module. A subset $S \subseteq M$ is a **basis** if:

1. S generates M: Every $m \in M$ can be written as a finite sum $m = \sum r_i s_i$ with $r_i \in R, s_i \in S$.
2. S is linearly independent: If $\sum r_i s_i = 0$ for distinct $s_i \in S$, then $r_i = 0$ for all i.

An R-module possessing a basis is called **free**. The cardinality of the basis is the **rank** of M.

定義

Remark.

If R is a field, every module is free. For general rings, this is false. For example, the $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$ (for $n > 1$) has no basis. Any single element x satisfies $nx = 0$, violating linear independence.

Example 5.6. Standard Free Modules.

- The ring R is a free module of rank 1 with basis $\{1_R\}$. Indeed, any unit $u \in R^\times$ constitutes a basis.
- Recall the module $\mathcal{F}_S$ of functions $S \to R$ with finite support introduced in the previous section. For each $s \in S$, define the characteristic function $e_s \in \mathcal{F}_S$ by:

$$e_s(t) = \delta_{st} = \begin{cases} 1 & \text{if } t = s, \\ 0 & \text{if } t \neq s. \end{cases}$$

The set $\{e_s\}_{s \in S}$ forms a basis for $\mathcal{F}_S$. Any $f \in \mathcal{F}_S$ is non-zero at finitely many points $s_1, \ldots, s_n$. Setting $r_i = f(s_i)$, we have $f =$

$\sum r_i e_{s_i}$, proving generation. For independence, if $\sum r_i e_{s_i} = 0$ (the zero function), evaluating at s_j yields $r_j = 0$. Thus $\mathcal{F}_S$ is the **free module on the set** S.

範例

Free modules behave well under direct sums.

Proposition 5.2. ***Direct Sums of Free Modules.***
Let F_1 and F_2 be free R-modules with bases S_1 and S_2 respectively. Then $F_1 \oplus F_2$ is free with basis

$$S = \{(s, 0) \mid s \in S_1\} \cup \{(0, s') \mid s' \in S_2\}.$$

If F_1, F_2 have finite ranks n_1, n_2, then $F_1 \oplus F_2$ has rank $n_1 + n_2$.

命題

Proof

Let $(m, m') \in F_1 \oplus F_2$. Since S_1 spans F_1 and S_2 spans F_2, we can write $m = \sum r_i s_i$ and $m' = \sum r'_j s'_j$. Then

$$(m, m') = \sum r_i (s_i, 0) + \sum r'_j (0, s'_j).$$

Thus S spans. For independence, suppose $\sum r_i (s_i, 0) + \sum r'_j (0, s'_j) = (0, 0)$. This implies $\sum r_i s_i = 0$ in F_1 and $\sum r'_j s'_j = 0$ in F_2. By the linear independence of S_1 and S_2, all coefficients vanish.

■

The defining characteristic of free modules is their universal mapping property: to define a map out of a free module, it suffices to specify the images of the basis elements arbitrarily.

Proposition 5.3. ***Universal Property of Free Modules.***
Let $\mathcal{F}_S$ be the free R-module on a set S. For any R-module M and any set map $f : S \to M$, there exists a unique R-module homomorphism $\phi_f : \mathcal{F}_S \to M$ such that $\phi_f(e_s) = f(s)$ for all $s \in S$.

命題

Proof

We construct ϕ_f by extending linearly: for $g = \sum_{s \in S} r_s e_s \in \mathcal{F}_S$ (where the sum is finite), define

$$\phi_f(g) = \sum_{s \in S} r_s f(s).$$

This map is clearly R-linear. Uniqueness follows because any homomorphism is determined by its action on a basis: $\phi(\sum r_s e_s) = \sum r_s \phi(e_s) = \sum r_s f(s)$.

■

Corollary 5.1. *Classification by Rank.* Let M be a free R-module with basis T. If S is a set with the same cardinality as T, then $M \cong \mathcal{F}_S$. Consequently, any two free modules of the same rank are isomorphic.

推論

Proof

Let $g : T \to S$ be a bijection. Using the universal property, the map $T \to \mathcal{F}_S$ sending $t \mapsto e_{g(t)}$ extends to a homomorphism $\phi : M \to \mathcal{F}_S$. Similarly, $e_s \mapsto g^{-1}(s)$ induces an inverse homomorphism.

■

Generators and Relations

While not all modules are free, every module is a quotient of a free module. Let M be an R-module generated by a finite set $S = \{s_1, \ldots, s_n\}$. The universal property yields a surjective homomorphism:

$$\psi : \mathcal{F}_S \to M, \quad \psi\left(\sum_{i=1}^{n} m_i e_{s_i}\right) = \sum_{i=1}^{n} m_i s_i.$$

The kernel $K = \ker \psi$ consists of the linear dependencies among the generators. Elements of K are called **relations**.

$$\sum_{i=1}^{n} m_i e_{s_i} \in K \iff \sum_{i=1}^{n} m_i s_i = 0 \text{ in } M.$$

Since K is a submodule of a free module (which, over general rings, is not necessarily free, though it is for PIDs), we can often find a generating set $T = \{t_1, \ldots, t_m\}$ for K. This gives a surjection $\mathcal{F}_T \to K$. Composing with the inclusion $K \hookrightarrow \mathcal{F}_S$, we obtain a sequence of maps:

$$\mathcal{F}_T \xrightarrow{\phi} \mathcal{F}_S \xrightarrow{\psi} M \to 0.$$

Here $\operatorname{im} \phi = K = \ker \psi$. By the First Isomorphism Theorem, $M \cong \mathcal{F}_S / \operatorname{im} \phi$. This description is called a **presentation** of M. If S and T are both finite, M is **finitely presented**.

Definition 5.9. ***Cokernel.***
Let $f : A \to B$ be an R-module homomorphism. The **cokernel** of f is the quotient module

$$\operatorname{coker} f = B / \operatorname{im} f.$$

定義

Definition 5.10. ***Presentation Matrix.***
Let M be finitely presented with generators $s_1, \ldots, s_n$ and relations $t_1, \ldots, t_m$. The map $\phi : R^m \to R^n$ is determined by the images of the basis vec-

tors of R^m. Writing $\phi(e_{t_j}) = \sum_{i=1}^{n} a_{ij} e_{s_i}$, we form the $n \times m$ matrix $A = (a_{ij})$. The module M is isomorphic to the cokernel of the linear map defined by A:

$$M \cong R^n / AR^m.$$

The matrix A is the **presentation matrix**.

定義

Example 5.7. Simple Presentations.

- Let $R = \mathbb{Z}$ and $M = \mathbb{Z}/n\mathbb{Z}$. M is generated by 1, so $\mathcal{F}_S \cong \mathbb{Z}$. The kernel is the ideal $n\mathbb{Z}$, generated by n. The presentation matrix is the 1×1 matrix (n).
- Let $R = \mathbb{Z}[\sqrt{-5}]$. Consider the ideal $I = (2, 1 + \sqrt{-5})$. We treat I as an R-module generated by $s_1 = 2$ and $s_2 = 1 + \sqrt{-5}$. We seek the relations $r_1 s_1 + r_2 s_2 = 0$. Observe that:

$$(1 + \sqrt{-5})s_1 - 2s_2 = 2(1 + \sqrt{-5}) - 2(1 + \sqrt{-5}) = 0.$$

$$3s_1 - (1 - \sqrt{-5})s_2 = 6 - (1 - \sqrt{-5})(1 + \sqrt{-5}) = 6 - (1 - (-5)) = 0.$$

It can be shown that these two relations generate the kernel of the map $R^2 \to I$. Thus, we define $\phi : R^2 \to R^2$ sending the basis of the relation module to these linear combinations. The presentation matrix is:

$$A = \begin{bmatrix} 1 + \sqrt{-5} & 3 \\ -2 & -1 + \sqrt{-5} \end{bmatrix}.$$

The columns correspond to the relations, and the rows to the generators s_1, s_2.

範例

The presentation matrix is not unique. If A presents M, then for any invertible matrices $B \in \mathrm{GL}_n(R)$ and $C \in \mathrm{GL}_m(R)$, the matrix BAC also presents M. This corresponds to changing the basis of the free modules $\mathcal{F}_S$ and $\mathcal{F}_T$.

5.4 *Exercises*

1. **Ideals as Submodules.** Let R be a ring, viewed as a left R-module over itself.
   (a) Show that any ideal $I \subseteq R$ is an R-submodule of R.
   (b) Conversely, show that any R-submodule $N \subseteq R$ is an ideal of R.
   (c) Conclude that the ideals of R are exactly the submodules of R viewed as an R-module.

2. **Function Modules and Free Modules.** Let S be a set and R a ring. Let $\mathcal{F}_S$ be the set of functions $f : S \to R$ with finite support (i.e., $f(s) \neq 0$ for only finitely many s).
   (a) Prove that $\mathcal{F}_S$ is an R-module under pointwise operations.
   (b) For each $s \in S$, define $e_s \in \mathcal{F}_S$ by $e_s(t) = 1$ if $t = s$ and 0 otherwise. Show that every $f \in \mathcal{F}_S$ can be uniquely written as a finite linear combination $\sum r_s e_s$.
   (c) Deduce that $\{e_s\}_{s \in S}$ is a basis for $\mathcal{F}_S$, making it a free R-module.

3. **Generating Modules.** Let M be an R-module and $S \subseteq M$. Prove the equivalence of the following statements:
   (a) Every element of M is an R-linear combination of elements of S.
   (b) For any R-module N and homomorphisms $f, g : M \to N$, if $f|_S = g|_S$ then $f = g$.
   (c) For any R-module L and homomorphism $h : L \to M$, if $S \subseteq \operatorname{im} h$, then h is surjective.

4. **Finite Generation.** An R-module M is finitely generated if it is generated by a finite set. Prove that if M is finitely generated, then for any chain of submodules $N_1 \subseteq N_2 \subseteq \dots$ such that $\bigcup N_i = M$, there exists k such that $N_k = M$.

5. **$\mathbb{Z}$-Modules and Abelian Groups.**
   (a) Prove that every abelian group A admits a unique structure of a $\mathbb{Z}$-module.
   (b) Prove that for abelian groups A, B, $\operatorname{Hom}_{\mathbb{Z}}(A, B)$ is exactly the set of group homomorphisms.
   (c) Explain why the axiom $1 \cdot m = m$ forces the definition of integer multiplication.

6. **Products and Coproducts.** Let $\{M_i\}_{i \in I}$ be a family of R-modules. Let $P = \prod_{i \in I} M_i$ (direct product) and $S = \bigoplus_{i \in I} M_i$ (direct sum).
   (a) Prove the universal property of the product: A homomorphism $f : L \to P$ corresponds uniquely to a family of homomorphisms $f_i : L \to M_i$.
   (b) Prove the universal property of the direct sum: A homomorphism $g : S \to N$ corresponds uniquely to a family of homomorphisms $g_i : M_i \to N$.

7. **Submodules of $\mathbb{Z}^2$.** View $\mathbb{Z}^2$ as a $\mathbb{Z}$-module. For each subset, determine if it is a submodule. If so, find a finite generating set.
   (a) $N_1 = \{(n, 2n) \mid n \in \mathbb{Z}\}$
   (b) $N_2 = \{(2a, 3b) \mid a, b \in \mathbb{Z}\}$

(c) $N_3 = \{(a,b) \in \mathbb{Z}^2 \mid a+b \text{ is even}\}$
(d) $N_4 = \{(a,b) \in \mathbb{Z}^2 \mid a \equiv b \pmod 3\}$

8. Quotients of $\mathbb{Z}^2$. Let $M = \mathbb{Z}^2$ and N be the submodule generated by $(2,0)$ and $(1,3)$.

(a) Describe the quotient module M/N as an abelian group (e.g., as a direct sum of cyclic groups).
(b) Find the annihilator ideal $\text{Ann}_{\mathbb{Z}}(M/N) = \{r \in \mathbb{Z} \mid r \cdot (M/N) = 0\}$.

9. Hom-sets. Let M, N be R-modules.

(a) Show that $\text{Hom}_R(M,N)$ is an abelian group under pointwise addition.
(b) If R is commutative, show $\text{Hom}_R(M,N)$ is an R-module via $(r \cdot f)(m) = r \cdot f(m)$.
(c) Prove there is an isomorphism of R-modules $\text{Hom}_R(R,M) \cong M$ given by $f \mapsto f(1)$.

10. Isomorphism Theorems. Let $f : M \to N$ be an R-module homomorphism.

(a) Prove $\ker f$ is a submodule of M and $\text{im}\, f$ is a submodule of N.
(b) Construct an isomorphism $M/\ker f \cong \text{im}\, f$.
(c) Show f is injective $\iff \ker f = 0$ and surjective $\iff \text{im}\, f = N$.

11. Homomorphisms of Cyclic Modules.

(a) Show that any group homomorphism $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is determined by $f(1)$.
(b) Prove that $nf(1) = 0$ in $\mathbb{Z}/m\mathbb{Z}$ is a necessary and sufficient condition.
(c) Deduce that $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/\gcd(n,m)\mathbb{Z}$.

12. Non-Free Modules. Consider the $\mathbb{Z}$-module $M = \mathbb{Z}/n\mathbb{Z}$ with $n > 1$.

(a) Prove that M cannot have a basis. (Show any element is linearly dependent).
(b) Conclude M is finitely generated but not free.
(c) Give another example of a finitely generated non-free $\mathbb{Z}$-module.

13. Presentation of Modules. Let M be generated by $m_1, \ldots, m_n$.

(a) Define $\psi : R^n \to M$ by $(r_1, \ldots, r_n) \mapsto \sum r_i m_i$. Show ψ is surjective.
(b) Let $K = \ker \psi$ be the relation module. Prove $M \cong R^n/K$.

6
Noetherian Rings and Modules

We now introduce the Noetherian condition, a finiteness property that tames the complexity of rings and modules. This concept generalises the property of Principal Ideal Domains where every ideal is generated by a single element, to rings where ideals are generated by finitely many elements. This finiteness is the cornerstone of algebraic geometry and algebraic number theory.

6.1 Definitions and Basic Properties

The Noetherian property can be stated in two equivalent ways: as a condition on chains of submodules (the ascending chain condition), or as a condition on generators.

Definition 6.1. ***Noetherian Modules and Rings.***
Let R be a ring.

1. An R-module M is **Noetherian** if every increasing sequence of submodules stabilizes. That is, for any chain
$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$$
of submodules of M, there exists an integer N such that $M_n = M_N$ for all $n \geq N$.
2. The ring R is **Noetherian** if it is Noetherian as a module over itself. Since the submodules of R are its ideals, this means every ascending chain of ideals $I_1 \subseteq I_2 \subseteq \dots$ stabilizes.

定義

The equivalence between the chain condition and finite generation is fundamental.

Theorem 6.1. ***Finite Generation Criterion.***
An R-module M is Noetherian if and only if every submodule of M is finitely generated.

定理

($\Longrightarrow$)

Suppose M is Noetherian. Let N be a submodule of M. We construct a generating set for N inductively. If $N = \{0\}$, it is generated by the empty set. Otherwise, choose $n_1 \in N$. Let $N_1 = \langle n_1 \rangle$. If $N_1 = N$, we are done. If not, choose $n_2 \in N \setminus N_1$ and set $N_2 = \langle n_1, n_2 \rangle$. Iterating this, if N is not finitely generated, we can choose a sequence $n_1, n_2, \ldots$ such that $n_{k+1} \in N \setminus N_k$ where $N_k = \langle n_1, \ldots, n_k \rangle$. This yields a strictly ascending chain of submodules:

$$N_1 \subsetneq N_2 \subsetneq N_3 \subsetneq \ldots$$

This contradicts the Noetherian hypothesis. Thus the process must terminate, implying $N = N_k$ for some k, so N is finitely generated.

証明終

($\Longleftarrow$)

Suppose every submodule of M is finitely generated. Let $M_1 \subseteq M_2 \subseteq \ldots$ be an ascending chain. Let $N = \bigcup_{i=1}^{\infty} M_i$. It is easily verified that the union of an ascending chain of submodules is itself a submodule. By assumption, N is finitely generated, say by $x_1, \ldots, x_k$. Since each $x_j \in N$, there exists an index i_j such that $x_j \in M_{i_j}$. Let $n = \max\{i_1, \ldots, i_k\}$. Then all generators $x_1, \ldots, x_k$ lie in M_n, so $N \subseteq M_n$. Since $M_n \subseteq M_{n+1} \subseteq \cdots \subseteq N$, we must have $M_n = M_{n+1} = \cdots = N$. The chain stabilizes.

証明終

Corollary 6.1. *PIDs are Noetherian.* Every Principal Ideal Domain (PID) is a Noetherian ring.

推論

Proof

In a PID, every ideal is generated by a single element, hence finitely generated.

■

Example 6.1. Examples of Noetherian and Non-Noetherian Rings.

- Any field F is Noetherian (its only ideals are (0) and (1)).
- The ring of integers $\mathbb{Z}$ is Noetherian (it is a PID).
- The polynomial ring in infinitely many variables $R = \mathbb{C}[x_1, x_2, \ldots]$ is *not* Noetherian. The chain of ideals

  $$(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \ldots$$

  never stabilizes. Similarly, the ideal generated by all variables is not finitely generated.

範例

6.2 *Finitely Generated Modules over Noetherian Rings*

We now investigate how the Noetherian property behaves under standard module operations. The main goal is to show that over a Noetherian ring, "finitely generated" is equivalent to "Noetherian".

Proposition 6.1. ***Inheritance of Noetherian Property.***
Let M be a Noetherian R-module. Then:
1. Every submodule $N \subseteq M$ is Noetherian.
2. Every quotient module M/N is Noetherian.

命題

Proof

(i) Since M is Noetherian, every submodule of M is finitely generated. A submodule of N is a submodule of M, hence finitely generated. Thus N is Noetherian.
(ii) Let Q be a submodule of M/N. Let $\pi : M \to M/N$ be the projection. The preimage $\pi^{-1}(Q)$ is a submodule of M, hence finitely generated by some $x_1, \ldots, x_k$. The images $\pi(x_1), \ldots, \pi(x_k)$ generate Q. Since every submodule of the quotient is finitely generated, M/N is Noetherian.

■

A crucial property is that extensions of Noetherian modules are Noetherian.

Definition 6.2. ***Short Exact Sequence.***
A sequence of R-module homomorphisms

$$0 \longrightarrow A \xrightarrow{\iota} B \xrightarrow{\pi} C \longrightarrow 0$$

is **short exact** if it is exact at each term, that is, ι is injective, π is surjective, and $\operatorname{im} \iota = \ker \pi$.

定義

Proposition 6.2. ***Extensions of Noetherian Modules.***
Let $0 \to N \to M \to M/N \to 0$ be a short exact sequence of R-modules. If N and M/N are Noetherian, then M is Noetherian.

命題

Proof

Let $P \subseteq M$ be a submodule. We show P is finitely generated. The intersection $P \cap N$ is a submodule of N. Since N is Noetherian, $P \cap N$ is finitely generated, say by $a_1, \ldots, a_s$. The image of P in the quotient, $(P + N)/N \cong P/(P \cap N)$, is a submodule of the Noetherian module M/N. Thus it is finitely generated, say by the cosets of $b_1, \ldots, b_t \in P$. We claim $\{a_1, \ldots, a_s, b_1, \ldots, b_t\}$ generates P. Let

$x \in P$. Its image in M/N can be written as $\sum r_j(b_j + N)$. Thus $x - \sum r_j b_j \in N$. Since $x \in P$ and $\sum r_j b_j \in P$, the difference lies in $P \cap N$. Thus:

$$x - \sum_{j=1}^{t} r_j b_j = \sum_{i=1}^{s} q_i a_i$$

for some $q_i \in R$. Hence $x = \sum q_i a_i + \sum r_j b_j$, proving finite generation.

■

Corollary 6.2. *Direct Sums.* If M and N are Noetherian R-modules, then their direct sum $M \oplus N$ is Noetherian.

推論

Proof

We have an exact sequence $0 \to M \to M \oplus N \to N \to 0$. Since M and N are Noetherian, so is $M \oplus N$.

■

Corollary 6.3. *Finite Rank Free Modules.* If R is a Noetherian ring, then any free R-module of finite rank R^n is Noetherian.

推論

Proof

By induction on n. For $n = 1$, R is Noetherian by definition. Since $R^n \cong R \oplus R^{n-1}$, the result follows from the previous corollary.

■

We conclude with the central theorem linking the ring structure to its modules.

Theorem 6.2. ***Modules over Noetherian Rings.***
Let R be a Noetherian ring. An R-module M is Noetherian if and only if M is finitely generated.

定理

($\Longrightarrow$)

If M is Noetherian, then M is a submodule of itself, hence finitely generated.

証明終

($\Longleftarrow$)

Suppose M is finitely generated by $x_1, \ldots, x_n$. There exists a surjective homomorphism from the free module R^n to M:

$$\phi : R^n \to M, \quad e_i \mapsto x_i.$$

Since R is Noetherian, R^n is a Noetherian module. The image of a Noetherian module under a homomorphism is isomorphic to a quotient, hence Noetherian. Thus $M \cong R^n / \ker \phi$ is Noetherian.

証明終

6.3 *Exercises*

1. **Ideals in Noetherian Rings.** Let R be a ring. Prove that the following are equivalent:
   (a) R is Noetherian (i.e., every ascending chain of ideals stabilizes).
   (b) Every ideal of R is finitely generated.

2. **Submodules of Finitely Generated Modules.** Let R be a Noetherian ring and M a finitely generated R-module. Prove that every submodule $N \subseteq M$ is finitely generated.

   Use the fact that finitely generated modules over a Noetherian ring are Noetherian.

   (a) Prove the statement above using the Noetherian property.
   (b) Let $f : M \to M$ be a surjective R-module homomorphism. Prove that f is injective.

   Use the ascending chain $\ker f \subseteq \ker f^2 \subseteq \dots$.

   (c) Give an example showing that the conclusion of (b) can fail if M is not Noetherian.

3. **Infinite Direct Sums.** Let R be a Noetherian ring (e.g., $\mathbb{Z}$). Consider the module $M = \bigoplus_{n=1}^{\infty} R$ with standard basis $e_1, e_2, \dots$.
   (a) Let $M_k = \langle e_1, \dots, e_k \rangle$. Show that $M_1 \subsetneq M_2 \subsetneq \dots$ is a strictly ascending chain.
   (b) Deduce that M is not a Noetherian R-module, even though R is Noetherian.
   (c) Conclude that "finitely generated" is essential in the theorem relating Noetherian rings to Noetherian modules.

4. **Polynomial Rings in Infinite Variables.** Let k be a field and $R = k[x_1, x_2, \dots]$ be the polynomial ring in countably many variables.
   (a) Prove that the chain of ideals $(x_1) \subsetneq (x_1, x_2) \subsetneq \dots$ is strictly ascending.
   (b) Conclude R is not a Noetherian ring.
   (c) Show that the ideal $I = (x_1, x_2, \dots)$ is not finitely generated.

5. **Quotients of Noetherian Rings.** Let R be a ring and I an ideal.
   (a) If R is Noetherian, prove that R/I is Noetherian.
   (b) Conversely, suppose R/I is Noetherian and I is finitely generated as an ideal. Prove that R is Noetherian.

   Use the short exact sequence $0 \to I \to R \to R/I \to 0$.

   (c) Deduce that R is Noetherian if and only if R/I is Noetherian for every finitely generated ideal I.

7
Polynomial Rings and Factorisation

Having established the general theory of Noetherian rings and modules, we now apply these concepts to the specific setting of polynomial rings. This study yields two cornerstones of commutative algebra: the Hilbert Basis Theorem, which guarantees that polynomial rings over Noetherian rings retain the Noetherian property, and the extension of unique factorisation from a ring to its polynomial ring via Gauss's Lemma.

7.1 The Hilbert Basis Theorem

Our primary goal is to prove that if a ring R satisfies the ascending chain condition on ideals, so does $R[X]$. This result is fundamental to algebraic geometry, as it implies that algebraic sets defined by infinitely many polynomial equations can actually be defined by finitely many.

We begin by analysing the structure of ideals in $R[X]$ through the leading coefficients of their elements. Let $P(X) = \sum_{i=0}^{n} b_i X^i \in R[X]$ with $b_n \neq 0$. We call b_n the **leading coefficient** of $P(X)$.

Lemma 7.1. ***Ideal of Leading Coefficients.***
Let R be a Noetherian ring and let $I \subseteq R[X]$ be an ideal. Let $J \subseteq R$ be the set of leading coefficients of all polynomials in I, together with 0. Then J is an ideal of R.

引理

Proof

Let $a \in J$. If $a = 0$, the closure properties are trivial. Assume $a \neq 0$. Then there exists $P(X) \in I$ of degree n with leading coefficient a. For any $r \in R$, if $ra \neq 0$, then ra is the leading coefficient of $rP(X)$, which lies in I. Thus $ra \in J$. Suppose $a, b \in J$ are nonzero leading coefficients of $P(X) \in I$ (degree n) and $Q(X) \in I$ (degree m). Without loss of generality, assume $n \geq m$. Consider the polynomial $S(X) = P(X) + X^{n-m}Q(X)$. This polynomial lies in I. Its term of

degree n is $(a+b)X^n$. If $a+b \neq 0$, it is the leading coefficient of $S(X)$, so $a+b \in J$. If $a+b = 0$, the condition holds trivially. Thus J is an ideal.

■

The Noetherian property of R ensures J is finitely generated. We use these generators to reduce the degree of polynomials in I.

Lemma 7.2. ***Degree Reduction.***
Let $I \subseteq R[X]$ be an ideal and J its ideal of leading coefficients. Let $a_1, \ldots, a_s$ generate J, and let $P_1, \ldots, P_s \in I$ be polynomials such that the leading coefficient of P_i is a_i. Let $N = \max_i(\deg P_i)$. For any $Q(X) \in I$ with $\deg Q \geq N$, there exist polynomials $R_1, \ldots, R_s \in R[X]$ such that

$$\deg\left(Q(X) - \sum_{i=1}^{s} R_i(X)P_i(X)\right) < N.$$

引理

Proof

We proceed by induction on $d = \deg Q$. The base case is implicit in the inductive step. Let a be the leading coefficient of $Q(X) = aX^d + \ldots$. Since $a \in J$, we may write $a = \sum_{i=1}^{s} r_i a_i$ for some $r_i \in R$. Consider the polynomial:

$$H(X) = \sum_{i=1}^{s} r_i X^{d-\deg P_i} P_i(X).$$

Since $d \geq N \geq \deg P_i$, the powers of X are non-negative. The leading term of $H(X)$ is $(\sum r_i a_i)\, X^d = aX^d$. Consequently, the polynomial $Q(X) - H(X)$ has degree strictly less than d. Since $H(X)$ is an $R[X]$-linear combination of the P_i, if the degree of the difference is still $\geq N$, we repeat the process. By induction, we eventually reduce the degree below N.

■

Theorem 7.1. ***Hilbert Basis Theorem.***
Let R be a Noetherian ring. Then the polynomial ring $R[X]$ is Noetherian.

定理

Proof

Let $I \subseteq R[X]$ be an ideal. We define J, a_i, P_i, and N as in the previous lemmas. Let $M = R[X]_{\leq N}$ be the R-submodule of polynomials of degree at most N. As an R-module, M is generated by $\{1, X, \ldots, X^N\}$. Since R is Noetherian and M is finitely generated, M is a Noetherian R-module. Consider the submodule

$I_{\leq N} = I \cap M$. Being a submodule of a Noetherian module, $I_{\leq N}$ is finitely generated over R. Let $T_1, \ldots, T_k$ be generators of $I_{\leq N}$. We claim that the set $\{P_1, \ldots, P_s, T_1, \ldots, T_k\}$ generates I as an ideal in $R[X]$. Let $Q \in I$. By the Degree Reduction Lemma, there exist $H_i \in R[X]$ such that

$$Q'(X) = Q(X) - \sum_{i=1}^{s} H_i(X) P_i(X)$$

has degree strictly less than N. Thus $Q' \in I \cap R[X]_{\leq N} = I_{\leq N}$. We can therefore write Q' as an R-linear combination of $T_1, \ldots, T_k$:

$$Q'(X) = \sum_{j=1}^{k} r_j T_j(X).$$

Substituting back, $Q(X)$ is expressed as a linear combination of the P_i and T_j. Thus I is finitely generated.

■

By induction on the number of variables, we immediately obtain:

Corollary 7.1. *Multivariate Polynomial Rings.* If R is Noetherian, then $R[X_1, \ldots, X_n]$ is Noetherian. In particular, since fields and PIDs are Noetherian, $\mathbb{Q}[X_1, \ldots, X_n]$ and $\mathbb{Z}[X_1, \ldots, X_n]$ are Noetherian rings.

推論

This leads naturally to the study of finitely generated algebras.

Definition 7.1. ***Finitely Generated Algebra.***
Let R be a ring. An R**-algebra** is a ring S equipped with a ring homomorphism $\phi : R \to S$. We say S is **finitely generated** as an R-algebra if there exists a finite set $s_1, \ldots, s_n \in S$ such that the evaluation homomorphism

$$\psi : R[X_1, \ldots, X_n] \to S, \quad X_i \mapsto s_i$$

is surjective. Equivalently, $S \cong R[X_1, \ldots, X_n] / \ker \psi$.

定義

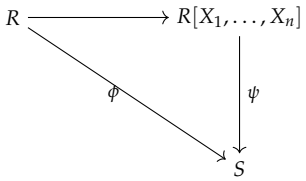


Figure 7.1: Structure of a finitely generated R-algebra.

Corollary 7.2. *Noetherian Algebras.* If R is a Noetherian ring, then any finitely generated R-algebra is Noetherian.

推論

Proof

Since R is Noetherian, $R[X_1, \ldots, X_n]$ is Noetherian. Any quotient of a Noetherian ring is Noetherian.

■

7.2 *Factorisation in Polynomial Rings*

While $\mathbb{Z}$ is a unique factorisation domain (UFD), the ring $\mathbb{Z}[X]$ is not a PID. For instance, the ideal $\langle 2, X \rangle$ is not principal. However, $\mathbb{Z}[X]$ remains a UFD. To prove this generally, we relate factorisation in $R[X]$ to factorisation in $K[X]$, where K is the field of fractions of R.

Gauss's Lemma

Let R be a UFD and K its field of fractions. Factorisation in $K[X]$ is well-understood because $K[X]$ is a Euclidean domain (and thus a PID and UFD). The difficulty lies in the fact that a polynomial irreducible in $R[X]$ might become reducible in $K[X]$, or vice versa.

Example 7.1. Irreducibility Dependence. The polynomial $3X + 15$ factorises as $3(X + 5)$ in $\mathbb{Z}[X]$. Both factors are non-units. However, in $\mathbb{Q}[X]$, 3 is a unit, so $3X + 15$ is associated to $X + 5$, which is irreducible.

範例

To handle coefficients, we define the **content** of a polynomial $P \in R[X]$ as the greatest common divisor (GCD) of its coefficients. A polynomial is **primitive** if its content is a unit (i.e., the GCD of coefficients is 1).

Theorem 7.2. ***Gauss's Lemma.***
Let R be a UFD and K its field of fractions. Let $P(X) \in R[X]$. If $P(X) = Q(X)T(X)$ is a factorisation in $K[X]$, then there exists $\alpha \in K^\times$ such that $\alpha Q(X) \in R[X]$ and $\alpha^{-1}T(X) \in R[X]$ is a factorisation in $R[X]$. In particular, if a primitive polynomial in $R[X]$ is reducible in $K[X]$, it is reducible in $R[X]$.

定理

Proof

Since $Q, T \in K[X]$, we can clear denominators. Choose $e_1, e_2 \in R$ such that $e_1 Q(X)$ and $e_2 T(X)$ are in $R[X]$. Further, we may factor out the content of these polynomials to ensure they are primitive. Thus, there exists $d \in R$ and primitive polynomials $Q'(X), T'(X) \in R[X]$ such that:

$$dP(X) = Q'(X)T'(X).$$

We claim that if $P(X)$ is primitive, then d must be a unit. Suppose d is not a unit. Let q be an irreducible factor of d in R. Since R is a UFD, the ideal $\langle q \rangle$ is prime, so $R/\langle q \rangle$ is an integral domain. Consider the reduction homomorphism $\pi : R[X] \to (R/\langle q \rangle)[X]$.

Applying this to the equation:

$$\overline{0} = \pi(dP) = \pi(Q')\pi(T').$$

Since $(R/\langle q \rangle)[X]$ is an integral domain, either $\pi(Q') = 0$ or $\pi(T') = 0$. If $\pi(Q') = 0$, all coefficients of Q' are divisible by q. This contradicts the construction of Q' as a primitive polynomial. Thus d must be a unit. The scalar α is constructed by redistributing the units and the cleared denominators.

■

This leads to a precise criterion for irreducibility.

Proposition 7.1. ***Irreducibility Criterion.***
Let $P(X) \in R[X]$ be a primitive polynomial. Then $P(X)$ is irreducible in $R[X]$ if and only if it is irreducible in $K[X]$.

命題

($\Longleftarrow$)

If P is irreducible in $K[X]$, it cannot factor into polynomials of lower degree in $R[X]$. The only possible factorisation in $R[X]$ would involve scalars, but since P is primitive, the only scalar divisors are units.

証明終

($\Longrightarrow$)

Suppose P is reducible in $K[X]$, so $P = QT$ with $\deg Q, \deg T < \deg P$. By Gauss's Lemma, we can modify this to a factorisation $P = (\alpha Q)(\alpha^{-1}T)$ in $R[X]$. Since degrees are preserved, P is reducible in $R[X]$.

証明終

R[X] is a UFD

We now combine these results to establish the main theorem.

Theorem 7.3. ***Polynomial Rings over UFDs.***
If R is a unique factorisation domain, then $R[X]$ is a unique factorisation domain.

定理

Existence.

Let $P(X) \in R[X]$. Let d be the content of P, so $P(X) = dQ(X)$ where Q is primitive. Since R is a UFD, d factors uniquely into irreducibles in R. These are also irreducible in $R[X]$. Next, consider $Q(X)$ as an element of $K[X]$. Since $K[X]$ is a UFD (being a PID), $Q(X) = F_1(X) \cdots F_k(X)$ where F_i are irreducible in $K[X]$. By Gauss's Lemma, we can scale these factors to be in $R[X]$ and

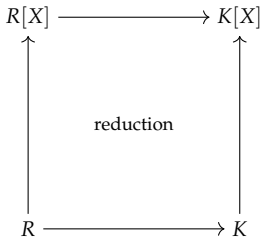


Figure 7.2: Comparison of factorisations.

primitive. Let these be $G_i(X)$. Since G_i is primitive and irreducible in $K[X]$, it is irreducible in $R[X]$. Thus $P(X) = dG_1(X) \cdots G_k(X)$ is a factorisation into irreducibles.

証明終

Uniqueness.

Suppose $P(X)$ has two factorisations into irreducibles. We separate the irreducible factors into two types: constant factors (irreducibles in R) and non-constant factors (primitive polynomials in $R[X]$).

$$P = c_1 \dots c_m \cdot q_1(X) \dots q_n(X) = d_1 \dots d_r \cdot t_1(X) \dots t_s(X).$$

The product $c = \prod c_i$ must equal $d = \prod d_j$ up to units, as these represent the content of P. Since R is a UFD, the constant factors match unique to units. The primitive parts $\prod q_i$ and $\prod t_j$ must be equal. Viewed in $K[X]$, these are irreducible factorisations. Since $K[X]$ is a UFD, $n = s$, and after reordering, q_i is associated to t_i in $K[X]$. So $q_i = \frac{a}{b} t_i$. Since both are primitive, a/b must be a unit in R. Thus they are associates in $R[X]$.

証明終

Corollary 7.3. *Multivariate UFDs.* If R is a UFD, then $R[X_1, \dots, X_n]$ is a UFD. Consequently, $\mathbb{Z}[X_1, \dots, X_n]$ and $F[X_1, \dots, X_n]$ (where F is a field) are UFDs.

推論

Remark.

It is important to note that while $R[X]$ inherits the UFD property, quotient rings generally do not. For example, $\mathbb{Z}[X]$ is a UFD, but $\mathbb{Z}[X]/\langle X^2 + 5 \rangle \cong \mathbb{Z}[\sqrt{-5}]$ is not, as evidenced by the non-unique factorisation $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

7.3 *Irreducibility Criteria*

We turn to the practical problem of determining whether a given polynomial is irreducible. While no single algorithm solves this efficiently for all rings, several powerful criteria exist.

Elementary Criteria and Finite Fields

For polynomials of low degree, irreducibility is determined simply by the existence of roots.

Proposition 7.2. ***Degree 2 and 3.***
Let K be a field and $P(X) \in K[X]$ a polynomial of degree 2 or 3. Then $P(X)$ is irreducible if and only if $P(X)$ has no roots in K.

命題

Proof

If $P(X)$ is reducible, it can be written as $P(X) = A(X)B(X)$ with $\deg A, \deg B \geq 1$. Since $\deg P \leq 3$, at least one factor must have degree 1. A linear factor in $K[X]$ corresponds to a root in K. Conversely, if $P(X)$ has a root α, then $(X - \alpha)$ divides $P(X)$.

■

For finite fields, we can leverage the structure of the Frobenius automorphism to formulate a precise criterion. Let $\mathbb{F}_q$ denote the finite field with $q = p^s$ elements.

Lemma 7.3. ***Factorisation of*** $X^{q^r} - X$**.**
The polynomial $X^{q^r} - X \in \mathbb{F}_q[X]$ is the product of all monic irreducible polynomials in $\mathbb{F}_q[X]$ whose degree divides r.

引理

Proof

Let $P(X)$ be a monic irreducible polynomial of degree d. Let α be a root of $P(X)$ in a splitting field. Then $\mathbb{F}_q(\alpha) \cong \mathbb{F}_{q^d}$. The elements of $\mathbb{F}_{q^d}$ are precisely the roots of $X^{q^d} - X$. Furthermore, $\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^r}$ if and only if $d \mid r$. Thus, α is a root of $X^{q^r} - X$ if and only if $d \mid r$. Since $P(X)$ is the minimal polynomial of α, $P(X)$ divides $X^{q^r} - X$ if and only if $d \mid r$.
It remains to show that $X^{q^r} - X$ is square-free, ensuring each irreducible factor appears with multiplicity 1. The formal derivative is:

$$\frac{d}{dX}(X^{q^r} - X) = q^r X^{q^r - 1} - 1 = -1 \quad (\text{since } \operatorname{char}(\mathbb{F}_q) = p \mid q).$$

Since the derivative is a non-zero constant, it is coprime to the polynomial. Thus $X^{q^r} - X$ has no repeated roots.

■

Corollary 7.4. *Irreducibility in* $\mathbb{F}_q[X]$*.* Let $P(X) \in \mathbb{F}_q[X]$ have degree d. Then $P(X)$ is irreducible if and only if

$$\gcd(P(X), X^{q^r} - X) = 1 \quad \text{for all } 1 \leq r < d.$$

推論

Proof

If $P(X)$ is reducible, it has an irreducible factor $Q(X)$ of degree r where $1 \leq r \leq d/2 < d$. By the previous lemma, $Q(X)$ divides $X^{q^r} - X$. Thus the GCD is divisible by $Q(X) \neq 1$. Conversely, if $P(X)$ is irreducible, its only divisors are units and associates of

$P(X)$. Since $\deg P = d > r$, $P(X)$ cannot divide $X^{q^r} - X$.

■

Criteria over UFDs

We now consider the case where coefficients lie in a unique factorisation domain R, such as $\mathbb{Z}$. Let K be the field of fractions of R. Recall that determining the irreducibility of $P(X) \in K[X]$ is often equivalent to checking irreducibility in $R[X]$. Specifically, we can transform monic polynomials in $K[X]$ to monic polynomials in $R[X]$.

Remark.

Let $P(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_0 \in K[X]$. For any $r \in R$, define

$$Q_r(X) = r^n P(X/r) = X^n + rc_{n-1}X^{n-1} + \cdots + r^n c_0.$$

Clearly $P(X)$ is irreducible in $K[X]$ if and only if $Q_r(X)$ is. By choosing r to be a common multiple of the denominators of the c_i, we can ensure $Q_r(X) \in R[X]$. Thus, we focus on monic polynomials in $R[X]$.

The most common technique is reduction modulo a prime ideal.

Proposition 7.3. ***Reduction Modulo*** $\mathfrak{p}$**.**
Let R be a UFD and $\mathfrak{p}$ a prime ideal of R. Let $Q(X)$ be a monic polynomial in $R[X]$. Let $\overline{Q}(X) \in (R/\mathfrak{p})[X]$ denote the reduction of $Q(X)$ modulo $\mathfrak{p}$. If $\overline{Q}(X)$ is irreducible in $(R/\mathfrak{p})[X]$, then $Q(X)$ is irreducible in $R[X]$.

命題

Proof

Suppose $Q(X)$ is reducible in $R[X]$. Since Q is monic, we factor it as $Q(X) = A(X)B(X)$ where A, B are monic polynomials of positive degree. Reducing modulo $\mathfrak{p}$ preserves the degree of monic polynomials. Thus $\overline{Q}(X) = \overline{A}(X)\overline{B}(X)$ is a factorisation into monic polynomials of positive degree in $(R/\mathfrak{p})[X]$. This contradicts the irreducibility of $\overline{Q}(X)$.

■

Example 7.2. Application to $\mathbb{Z}[X]$. Consider $f(X) = X^2 + aX + b \in \mathbb{Z}[X]$ where a, b are odd integers. Reducing modulo 2, we obtain:

$$\overline{f}(X) = X^2 + X + 1 \in (\mathbb{Z}/2\mathbb{Z})[X] = \mathbb{F}_2[X].$$

This polynomial has no roots in $\mathbb{F}_2$ ($\overline{f}(0) = 1, \overline{f}(1) = 1$), so it is irreducible. Thus $f(X)$ is irreducible in $\mathbb{Z}[X]$ (and by Gauss's Lemma, in $\mathbb{Q}[X]$).

範例

Note

This criterion is sufficient but not necessary. The polynomial $X^4 + 1$ is irreducible in $\mathbb{Z}[X]$ (and $\mathbb{Q}[X]$), yet it is reducible modulo p for every prime p. For $p = 2$, $X^4 + 1 = (X + 1)^4$. For odd primes, it can be shown via elementary number theory that $X^4 + 1$ divides $X^{p^2-1} - 1$, which splits completely in $\mathbb{F}_{p^2}$.

A specific case of modular reduction provides a very powerful sufficient condition known as Eisenstein's Criterion.

Proposition 7.4. ***Eisenstein's Criterion.***
Let R be a UFD and $\mathfrak{p}$ a prime ideal. Let $Q(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ be a monic polynomial in $R[X]$. Suppose that:
1. $a_i \in \mathfrak{p}$ for all $0 \leq i \leq n-1$,
2. $a_0 \notin \mathfrak{p}^2$.

Then $Q(X)$ is irreducible in $R[X]$.

命題

Proof

Suppose $Q(X)$ is reducible. Since it is monic, we may write $Q(X) = A(X)B(X)$ with $A, B \in R[X]$ monic of positive degree. Reduce modulo $\mathfrak{p}$. By the first condition, $\overline{Q}(X) = X^n$. Since $R/\mathfrak{p}$ is an integral domain (as $\mathfrak{p}$ is prime), the unique factorisation of X^n implies that $\overline{A}(X) = X^s$ and $\overline{B}(X) = X^t$ for some $s, t > 0$ with $s + t = n$. Consequently, the constant terms satisfy $\overline{A}(0) = 0$ and $\overline{B}(0) = 0$. This means $A(0) \in \mathfrak{p}$ and $B(0) \in \mathfrak{p}$. However, the constant term of $Q(X)$ is $a_0 = A(0)B(0)$. Since both factors lie in $\mathfrak{p}$, their product lies in $\mathfrak{p}^2$. Thus $a_0 \in \mathfrak{p}^2$, contradicting the second condition. ■

Example 7.3. Irreducibility of $X^4 + 1$. Although modular reduction failed for $X^4 + 1$, we can apply Eisenstein's criterion after a linear substitution. Let $Q(X) = X^4 + 1$. If $Q(X)$ were reducible, then $Q(X + 1)$ would also be reducible.

$$Q(X+1) = (X+1)^4 + 1 = X^4 + 4X^3 + 6X^2 + 4X + 2.$$

We apply Eisenstein's criterion with the prime $p = 2$. The coefficients $4, 6, 4, 2$ are all divisible by 2. The constant term 2 is not divisible by $2^2 = 4$. Thus $Q(X + 1)$ is irreducible, implying $X^4 + 1$ is irreducible.

範例

Multivariate Polynomials

For polynomial rings in several variables, such as $F[X, Y, Z]$, we can view the ring as polynomials in one variable with coefficients in a ring of fewer variables:

$$F[X, Y, Z] \cong (F[X, Y])[Z].$$

Since $F[X, Y]$ is a UFD, we can apply the techniques developed above.

Example 7.4. Using the Discriminant. Consider $P(X, Y) = X^4 + X^2Y^2 + Y^2 + XY \in \mathbb{C}[X, Y]$. We view this as a polynomial in Y with coefficients in $R = \mathbb{C}[X]$. Let $K = \mathbb{C}(X)$ be the field of rational functions.

$$P(X, Y) = (X^2 + 1)Y^2 + XY + X^4.$$

Since the GCD of coefficients in $\mathbb{C}[X]$ is 1, P is irreducible in $\mathbb{C}[X, Y]$ if and only if it is irreducible in $K[Y]$. Being quadratic in Y, it is irreducible if and only if it has no roots in K, which occurs if and only if the discriminant is not a square in K.

$$\Delta = X^2 - 4(X^2 + 1)(X^4) = X^2 - 4X^6 - 4X^4 = X^2(1 - 4X^2 - 4X^4).$$

The factor $(1 - 4X^2 - 4X^4)$ has simple roots in $\mathbb{C}$, so it is not a square in $\mathbb{C}[X]$. Thus Δ is not a square in K, so $P(X, Y)$ is irreducible.

範例

Example 7.5. Reduction Modulo an Ideal. Consider $P(X, Y, Z) = Z^5 + X^3Y^4Z + 2X^2YZ^3 - XYZ + Y^3 \in \mathbb{C}[X, Y, Z]$. We view this as a monic polynomial in Z over the UFD $R = \mathbb{C}[X, Y]$. Let $\mathfrak{p} = \langle X \rangle$ be the ideal generated by X. This is a prime ideal since $R/\mathfrak{p} \cong \mathbb{C}[Y]$ is an integral domain. The reduction modulo X is:

$$\overline{P}(Y, Z) = Z^5 + Y^3 \in \mathbb{C}[Y][Z].$$

We check if $Z^5 + Y^3$ is irreducible in $\mathbb{C}[Z][Y]$ (viewing as a polynomial in Y). It is $Y^3 + Z^5$. This is irreducible if $-Z^5$ is not a cube in $\mathbb{C}[Z]$. By unique factorisation in $\mathbb{C}[Z]$, Z^5 is not a cube. Thus $\overline{P}$ is irreducible, implying $P(X, Y, Z)$ is irreducible.

範例

7.4 *Exercises*

1. **Noetherianity of Formal Power Series.** Let R be a Noetherian ring. The ring of formal power series $R[[X]]$ consists of expressions of the form $f = \sum_{i=0}^{\infty} a_i X^i$ where $a_i \in R$. Unlike polynomials,

these sums need not be finite.

(a) Define the *order* of a non-zero power series f, denoted $\operatorname{ord}(f)$, as the smallest n such that $a_n \neq 0$. The coefficient $a_{\operatorname{ord}(f)}$ is the *lowest coefficient* of f. Show that f is a unit in $R[[X]]$ if and only if a_0 is a unit in R.

(b) Generalise the logic of the *Hilbert Basis Theorem* to prove that if R is Noetherian, then $R[[X]]$ is Noetherian.

For (b): Instead of leading coefficients and degree reduction, consider the ideal J_k of lowest coefficients of series in I with order k. Show that $J_0 \subseteq J_1 \subseteq J_2 \subseteq \dots$ and use the ascending chain condition on R and the J_k.

2. **The Content Identity.** Let R be a UFD. For $f \in R[X]$, let $c(f)$ denote its content.

(a) Prove that for any $f, g \in R[X]$, $c(fg) = c(f)c(g)$ up to units in R.

(b) Let $f \in \mathbb{Z}[X]$. Suppose there exists a prime p such that p does not divide the leading coefficient of f. If the reduction $\overline{f} \in \mathbb{F}_p[X]$ has no repeated factors, prove that any factorisation of f in $\mathbb{Z}[X]$ must reduce to the factorisation of $\overline{f}$.

3. **The Failure of the PID Property.** While $K[X]$ is a PID for any field K, we have seen that $R[X]$ is rarely a PID if R is not a field.

(a) Let R be an integral domain. Prove that $R[X]$ is a PID if and only if R is a field.

(b) Consider the ideal $I = \langle 2, X \rangle \subset \mathbb{Z}[X]$. Prove that I is not a principal ideal.

(c) Show that I is a maximal ideal by identifying the quotient $\mathbb{Z}[X]/I$.

(d) Generalise this: if K is a field, show that the ideal $\langle X, Y \rangle \subset K[X, Y]$ is maximal but not principal.

4. **Cyclotomic Irreducibility.** Let p be a prime number. The p-th cyclotomic polynomial is defined as

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

(a) Show that pascals identity implies the binomial coefficient $\binom{p}{k}$ is divisible by p for $1 \leq k \leq p - 1$.

(b) Apply the substitution $X = Y + 1$ to $\Phi_p(X)$. Show that the resulting polynomial in Y satisfies the conditions of *Eisenstein's Criterion* for the prime p.

(c) Conclude that $\Phi_p(X)$ is irreducible in $\mathbb{Q}[X]$.

5. **Multivariate Fermat Polygons.** We investigate the irreducibility of $f(X, Y) = X^n + Y^n - 1$ over various fields.

(a) Prove that $X^n + Y^n - 1$ is irreducible in $\mathbb{C}[X, Y]$ for all $n \geq 1$.

(b) For which n is $X^n + Y^n - 1$ irreducible in $\mathbb{F}_p[X, Y]$? Consider specifically $p = 2, n = 2$.

For (a): View this as a polynomial in X with coefficients in $\mathbb{C}[Y]$. Use *Eisenstein's Criterion* with a prime ideal $\mathfrak{p} = \langle Y - \alpha \rangle$ for some suitable $\alpha \in \mathbb{C}$.