PMATH 348 WINTER 2021

Fields and Galois Theory

Instructor: Yu-Ru Liu

Lecture Notes

by Justin Li

Contents

1. Ring Theory

1.1 Review of ring theory

Definition 1.1.1 — Commutative Ring with 1. A set R equipped with addition $(+)$ and multiplication $(\cdot)$ such that:

1. R is an abelian group (under $+$) with identity 0.
2. Multiplication is commutative and associative. There exists $1 \in R$, such that $\forall r \in R$, $1r = r$
3. For all r, s, $t \in R$, $r(s+t) = rs + rt$

In the following, we use the word **ring** to mean a commutative ring with 1.

Definition 1.1.2 — Field.
A **field** $\mathbb{F}$ is a ring in which every $a \in \mathbb{F} \setminus \{0\}$ is a unit. i.e. $ab = 1$ for some $b \in \mathbb{F}$

Definition 1.1.3 — Intergral Domain.
A ring R is an **integral domain** if for a, $b \in R$, $ab = 0$ implies that $a = 0$ or $b = 0$

■ **Example 1.1** The set of integers $\mathbb{Z}$ is an integral domain. The sets $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}_p$ are all fields. ■

Proposition 1.1.1
Every subring of a field is an integral domain.

Definition 1.1.4 — Ideal.
An **ideal** in a ring R is a subset I containing 0 such that for $a, b \in I$ and $r \in R$, $a = b \in I$ and $ra \in I$

■ **Example 1.2** The only ideals of a field $\mathbb{F}$ are $\{0\}$ and $\mathbb{F}$ ■

Definition 1.1.5 — Principal Ideal Domains (PID).
An integral domain R is a **principal ideal domains(PID)** if every ideal is generated by one element.

In the following two examples, we will list common properties of $\mathbb{Z}$ and $\mathbb{F}[x]$, the set of polynomials in x over a field $\mathbb{F}$

■ **Example 1.3** The set of integers $\mathbb{Z}$ is an integral domain and the units of $\mathbb{Z}$ are $\{\pm 1\}$.
Division Algorithm in $\mathbb{Z}$: for $a, b \in \mathbb{Z}$, $a \neq 0$, we can write $b = qa + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r \leq |a|$.
Using the Division Algorithm in $\mathbb{Z}$, we can prove that an ideal I of $\mathbb{Z}$ is of the form $I - \langle n \rangle = n\mathbb{Z}$
Thus $\mathbb{Z}$ is a PID. Note that if $n > 0$, then the generator n in unique.
Consider all fields containing $\mathbb{Z}$. Their intersection (the smallest field containing $\mathbb{Z}$) is the set of rational numbers

$$\mathbb{Q} = \left\{ \frac{a}{b} : \ a, \ b \in \mathbb{Z} \ and \ b \neq 0 \right\}$$

■

■ **Example 1.4** Let $\mathbb{F}$ be a field. Define

$$\mathbb{F}[x] = \{f(x) = a_0 + a_1 x + \ldots + a_m x^m, \ a_i \in \mathbb{F} \ \ \forall \ 0 \leq i \leq m\}$$

If $a_m = 1$, we say $f(x)$ is **monic**
If $a_m \neq 0$, the **degree** of $f(x)$ is m, also $\deg(0) = -\infty$
For $f(x), g(x) \in \mathbb{F}[x]$, $\deg(fg) = \deg(f) + \deg(g)$ (to preserve this degree formula we define $\deg(0) = \pm\infty$)
The set $\mathbb{F}[x]$ is an n integral domain and the units of $\mathbb{F}[x]$ are $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$
Division Algorithm in $\mathbb{F}[x]$: for $f(x), g(x) \in \mathbb{F}[x]$, $f(x) \neq 0$, we can write $g(x) = q(x)f(x) + r(x)$ where $q(x), r(x) \in \mathbb{F}[x]$ and $\deg(r) < \deg(f)$. (to preserve this degree formula we define $\deg(0) = \pm\infty$)
Using the Division Algorithm in $\mathbb{F}[x]$, we can prove that an ideal I of $\mathbb{F}[x]$ is of the form $I = \langle f(x) \rangle = f(x)\mathbb{F}[x]$. Thus $\mathbb{F}[x]$ is a PID. Note that if $f(x)$ is monic, then the generator f(x) is unique.
Consider all fields containing $\mathbb{F}[x]$, their Their intersection (the smallest field containing $\mathbb{F}[x]$) is the set of rational functions ■

Definition 1.1.6 — Quotient Ring of R modulo I.
The quotient ring of R modulo I, denoted by R/I, contains elements of the form $r + I$ ($r \in R$). The addition and multiplication on R/I are defined by

$$(r_1 + I) + (r_2 + I) = (r_1 + r_2) + R \qquad and \qquad (r_1 + I) \cdot (r_2 + I) = r_1 r_2 + I$$

■ **Example 1.5** For $n \in Z$, we have

$$\mathbb{Z}/\langle n \rangle = \{r = r + \langle n \rangle, 0 \leq r \leq |n|\}$$

For $f(x) \in \mathbb{F}[x]$, we have

$$\mathbb{F}[x]/\langle f(x) \rangle = \{r(x) = r(x) + \langle f(x) \rangle, \deg(r) < \deg(f)\}$$

■

Theorem 1.1.2 — First Isomorphism Theorem. Let $\varphi : R \to S$ be a ring homomorphism. Then $\ker(\varphi)$ is an ideal I. Moreover, there is an isomorphism

$$R/I \longrightarrow im(\varphi),\ r + I \to \varphi(r)$$

Definition 1.1.7 — Maximal Ideal.
An ideal I in a ring R is **maximal** if $I \neq R$ and there is no ideal J with $I \subsetneq J \subsetneq R$

Definition 1.1.8 — Prime Ideal.
An ideal I in a ring R is prime if $I \neq R$ and $ab \in I$ implies that $a \in I$ or $b \in I$

Proposition 1.1.3
Every maximal ideal is prime. Moreover, in PID, every prime ideal is maximal.

■ **Example 1.6** In $\mathbb{Z}$, $\langle n \rangle$ is maximal if and only if n is a prime. ■

■ **Example 1.7** In $F[x]$, $\langle f(x) \rangle$ is maximal if and only if $f(x)$ is irreducible ■

Theorem 1.1.4 — Let I be an ideal of a ring R and $I \neq R$. Then
(1) I I is a maximal ideal if and only if R/I is a field
(2) I I is a prime ideal if and only if R/I is an integral domain

1.2 Eisenstein's Criterion

In this section, we will apply Gauss' Lemma (proved in PMATH 347) to prove Eisenstein's Criterion. We will need this criterion in Chapter 2

Lemma 1.2.1 — Gauss' Lemma. (for $\mathbb{Z}[x]$)
Let $f(x) \in \mathbb{Z}[x]$ with $\deg(f) \geq 1$. If $f(x)$ is irreducible in $\mathbb{Z}[x]$, then it's irreducible in $\mathbb{Q}[x]$

■ **Remark 1.1** The converse of the above result is not true. For example, the ploynomial $2x + 8$ is irreducible in $\mathbb{Q}[x]$, but $2x + 8 = 2(x + 4)$ is reducible in $\mathbb{Z}[x]$ ■

Theorem 1.2.2 — Eisenstein's Criterion. (for $\mathbb{Z}[x]$)
Let $f(x) = a_n x_n + a_{n+1}x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$ with $n \geq 1$. Let $p \in \mathbb{Z}$ be a prime. If $p \nmid a_n$, $p \mid a_i$ for all $0 \leq i \leq (n-1)$ and $p^2 \nmid a_0$, then $f(x)$ is **irreducible** in $\mathbb{Q}[x]$

Proof. Consider The map $\mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$ defined by

$$f(x) \longmapsto \overline{f}(x) = \overline{a_n}x^n + \overline{a_{n-1}}x^{n-1} + \ldots + \overline{a_0} \pmod{p}$$

where $\overline{a_i} \in \mathbb{Z}_p$ with $\overline{a_i} \equiv a_i \pmod{p}$ for $0 \leq i \leq n$. Since $p \nmid a_i$ for all $0 \leq i \leq (n-1)$, we have

$\overline{f}(x) = \overline{a_n}x^n$ with $\overline{a_n} \neq 0$. If $f(x)$ is reducible in $\mathbb{Q}[x]$, by **Lemma 1.2.1-Gasuss' Lemma** for $\mathbb{Z}[x]$ for $\mathbb{Z}[x]$, $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{Z}[x]$ and $\deg(g), \deg(h) \geq 1$. It follows that $\overline{a_n}x^n = \overline{g}(x)\overline{h}(x)$. Since $\mathbb{Z}_p$ is a unique factorization domain, from which we see that $\overline{g}(x) = bx^m$ and $\overline{h}(x) = cx^k$ for some $b, c \in \mathbb{Z}_p$. In other words, $\overline{g}(x)$ and $\overline{h}(x)$ have 0 constant in $\mathbb{Z}_p$. Since the constants of both $g(x)$ and $h(x)$ are divisible by p, this implies that $p^2 \mid a_0$, which leads to a **contradiction**. Thus $f(x)$ is irreducible in $\mathbb{Q}[x]$ ■

■ **Example 1.8** The polynomial $2x^7+3x^4+6x^2+12$ is irreducible in $\mathbb{Q}[x]$, as we can apply **Eisenstein's Criterion** with $p = 3$ ■

Definition 1.2.1 — Primitive. (in ring theory)
A polynomial is primitive if its coefficients are coprime

Fact 1.2.3 $f(x)$ is irreducible in $\mathbb{Q}[x] \iff f(x+1)$ is irreducible in $\mathbb{Q}[x]$

■ **Example 1.9** Let p be a prime and

$$\zeta_p = e^{\frac{2\pi i}{p}} = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$$

be a $p-$th root of 1. It's a root of the $p-$th cyclotomic polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$$

Eisenstein's Criterion does not imply the irreducibility of $\Phi_p(x)$ immediately. However, we can consider

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \ldots + \binom{p}{p-2}x + \binom{p}{p-1} \in \mathbb{Z}[x]$$

Since p is a prime, $p \nmid 1$, $p \mid \binom{p}{i}$ for all $1 \leq i \leq (p-1)$ and $p^2 \nmid \binom{p}{p-1}$. Thus by **Eisenstein's Criterion** for $\mathbb{Z}[x]$, $\Phi_p(x+1)$ is irreducible in $\mathbb{Q}[x]$. This implies that $\Phi_p(x)$ is also irreducible in $\mathbb{Q}[x]$. Since $\Phi_p(x)$ is primitive, so $\Phi_p(x)$ is also irreducible in $\mathbb{Z}[x]$ ■

■ **Remark 1.2** The above results can be generalized to unique factorization domains ■

Lemma 1.2.4 — Gauss' Lemma. (for **PID**)
Let R be a unique factorization domain with the field of fractions $\mathbb{F}$. Let $g(x) \in R[x]$ with $\deg(g) \geq 1$. If $g(x)$ is irrducible in $R[x]$, then it is irreducible in $\mathbb{F}[x]$. Applying the same proof in **Theorem 1.2.1 for** $\mathbb{Z}[x]$, we can prove the following result.

Theorem 1.2.5 — Eisenstein's Criterion. (for **PID**)

Let R be a unique factorization domain with the field of F and

$$f(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0 \in R[x]$$

with $n \geq 1$. Let $l \in R$ be an irreducible element. If $l \nmid b_n$, $l \mid b_i$ for all $0 \leq i \leq (n-1)$ and $l^2 \nmid b_0$, then $f(x)$ is irreducible in $\mathbb{F}[x]$.

■ **Remark 1.3** The above results also can be generalized to unique factorization domains, but the proof need to be modified. ■

Lemma 1.2.6 — Gauss' Lemma. (for **UFD**)
Let S be a unique factorization with the field of fractions E. Let $h(x) \in S[x]$ with $\deg(h) \geq 1$. If $h(x)$ is irreducible in $S[x]$, then it is irreducible in $E[x]$

Theorem 1.2.7 — Eisenstein's Criterion. (for **UFD**) Let S be a unique factorization domain with the field of fractions E. Let $h(x) = c_n x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0 \in S[x]$ with $n \geq 1$. Let $l \in S$ be an irreducible element. If $l \nmid c_n$, $l \mid c_i$ for all $0 \leq i \leq (n-1)$ and $l^2 \nmid c_0$, then $h(x)$ is irreucible in $E[x]$

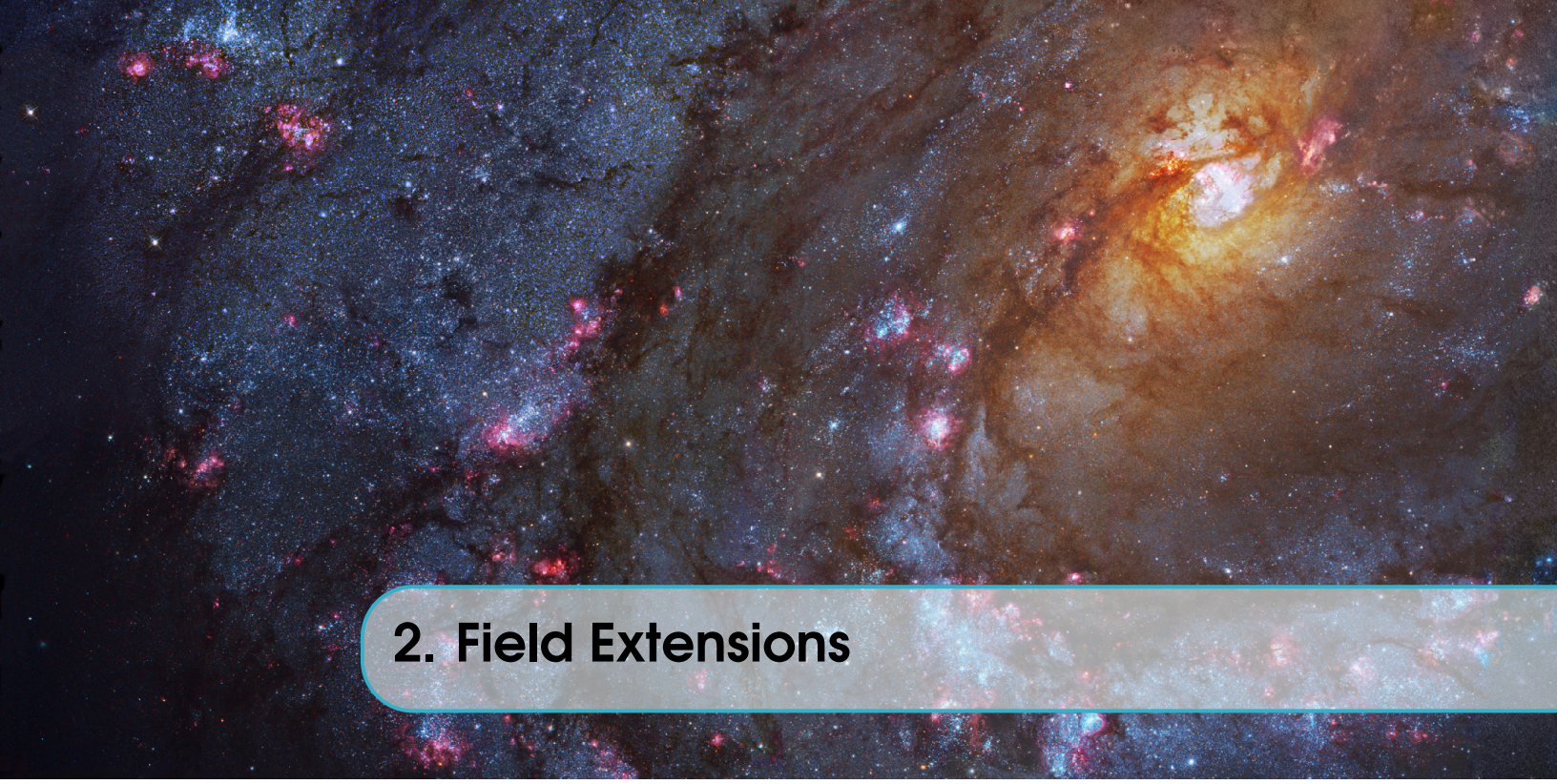
Proof. We prove by contradiction. If $h(x0$ is reducible in $E[x]$, by **Gauss' Lemma** for **UFD**, there exists $s(x), r(x) \in S[x]$ of degree ≥ 1 such that $h(x) = s(x)r(s)$. We write

$$s(x) = a_0 + a_1 x + \ldots + a_m x^m \quad \text{and} \quad r(x) = b_0 + b_1 x + \ldots + b_k x^k$$

where $1 \leq m, k < n$. Since $h(x) = s(x)r(x)$, we have

$$c_0 = a_0 b_0 \quad c_1 = a_0 b_1 + a_1 b_0 \quad c_2 = a_0 b_2 + a_1 b_1 + a_2 b_2, \quad \ldots$$

Consider the constant term. Since $l \mid c_0$, we have $l \mid a_0 b_0$. Since l is irreducible, $l \mid a_0$ or $l \mid b_0$. **WLOG** we suppose $l \mid a_0$. Since $l^2 \mid c_0$ we have $l \mid b_0$. If we consider the coefficient of x, since $l \mid c_1$, we have $l \mid (a_0 b_1 + a_1 b_0)$. Since $l \mid a_0$, we have $l \mid a_1 b_0$. Since $l \mid b_0$ so we have $l \mid a_1$ By repeating the above argument, the conditions on coefficient of $h(x)$ imply that $l \mid a_i$ for all $0 \leq i \leq (m-1)$ and $l \mid a_m$. Consider the reduction $\overline{h}(x) = \overline{s}(x)\overline{r}(x) \in S/\langle l \rangle[x]$. By the assunmption on the coefficients of h, $\overline{h}(x) = \overline{c_n} x^n$. However, since $\overline{s}(x) = \overline{a_m} x^m$ and $l \nmid b_0$,$\overline{s}(x)\overline{r}(x)$ contain the term $\overline{a_m b_0} x^m$, which leads to a contradiction, Som $h(x)$ is irreducible in $E[x]$ which completes the proof. ■



2. Field Extensions

2.1 Degree of Extensions

Definition 2.1.1 — Field Extension.
If E is a field containing another field F, we say E is a **field extension** of F, denoted by E/F

Note: the notation E/F is not used to denote a quotient ring as the field E has no ideals other than $\{0\}$ and E.

If E/F is a field extension, we can view E as a vector space over F:
(1) Addition: for $e_1, e_2 \in E$, $e_1 + e_2 \coloneqq e_1 + e_2$ (addition of E)
(2) Scalar multiplication: For $c \in F$, $e \in E$, $ce \coloneqq ce$ (multiplication of E)

Definition 2.1.2 — Degree Finite Extension.
The dimension of E over F (viewed as a vector space) is called the **degree** of E over F, denoted by $[E : F]$. If $[E : F] < \infty$, we say E/F is a **finite extension**. Otherwise, E/F is an **infinite extension**

■ **Example 2.1** $[\mathbb{C} : \mathbb{R}] = 2$ is a finite extension since $\mathbb{C} \cong \mathbb{R} + \mathbb{R}i$ where $i^2 = -1$ ■

■ **Example 2.2** Let F be a field. Let

$$F[x] = \{f(x) = a_0 + a_1 x + \ldots + a_n x^n \textbf{ where } a_0, a_1, \ldots a_n \in F \textbf{ and } n \in \mathbb{N} \cup \{0\}\}$$

and

$$F(x) = \left\{ \frac{f(x)}{g(x)} : \ f(x), g(x) \in F[x] \textbf{ and } g(x) \neq 0 \right\}$$

Then $[F(x) : F]$ is ∞ since $\{1, x, x^2, \ldots\}$ are linearly independent over F ■

Theorem 2.1.1
If E/K and K/F are finite field extensions, then E/F is a finite field extension and

$$[E : F] = [E : K] \cdot [K : F]$$

In particular, if K is an intermediate field of a finite extension E/F, then $[K : F] \mid [E : F]$

Proof: Suppose $[E : K] = m$ and $[K : F] = n$. Let $\{a_1, a_2, \ldots, a_m\}$ be a basis of E/K and $\{b_1, b_2, \ldots, b_n\}$ be a basis of K/F. It suffices to show $\{a_i b_j,\ 1 \le i \le m,\ 1 \le j \le n\}$ is a basis of E/F

Claim: Every element of E is a linear combination of $\{a_i b_j\}$ over F
For $e \in E$, we have

$$e = \sum_{i=1}^{m} k_i a_i \quad \textbf{where } k_i \in K$$

For $k_i \in K$, we have

$$k_i = \sum_{j=1}^{n} c_{ij} b_j \quad \textbf{where } c_{ij} \in K$$

Thus we have

$$e = \sum_{i=1}^{m} \sum_{j=1}^{n} c_{ij} b_j a_i$$

Claim: The set $\{a_i b_j,\ 1 \le i \le m,\ 1 \le j \le n\}$ is linearly independent over F
Suppose that

$$\sum_{i=1}^{m} \sum_{j=1}^{n} c_{ij} b_j a_i = 0 \quad \textbf{where } c_{ij} \in F$$

Since $\sum_{j=1}^{n} c_{ij} b_j \in K$ and $\{a_1, a_2, \ldots, a_m\}$ is independent over K, we have

$$\sum_{j=1}^{n} c_{ij} b_j = 0$$

Since $\{b_1, b_2, \ldots, b_n\}$ is independent over F, so we have $c_{ij} = 0$.
Thus $\{a_i b_j,\ 1 \le i \le m,\ 1 \le j \le n\}$ is a basis of E/F and we have

$$[E : F] = [E : K] \cdot [K : F]$$

which completes the proof of the theorem.

2.2 Algebraic and Transcendental Extensions

Definition 2.2.1 — Algebraic Over & Transcendental Over.
Let E/F be a field extension and $\alpha \in E$. We say α is **algebraic over** F if there exists $f(x) \in F[x] \setminus \{0\}$ with $f(\alpha) = 0$. Otherwise, α is **transcendental over** F.

■ **Example 2.3** $\frac{c}{d} \in \mathbb{Q}$, $\sqrt{2}$, $\sqrt{2} + \sqrt{-2}$ are algebraic over $\mathbb{Q}$ (See Assignment 2), but e and π are transcendental over $\mathbb{Q}$ ■

■ **Remark 2.1** Let E/F be a field extension and $\alpha \in E$. Let $F[\alpha]$ denote the smallest subring of E containning F and α and $F(\alpha)$ is the smallest subfield of E containnig F and α. For $\alpha, \beta \in E$, we define $F[\alpha, \beta]$ and $F(\alpha, \beta)$ similarly. ■

Definition 2.2.2 — Simple Extension.
If $E = F(\alpha)$ for some $\alpha \in E$, we say E is a **simple extension** of F.

Note: The degree of simple extension $F(\alpha)/F$ is either infinite of finite. In this section, we will show that this depends on if α in transcendental of algebraic

Definition 2.2.3 — F-homomorphism.
Let R and R_1 be two rings which contain a field F. A ring homomorphism $\psi : R \to R_1$ is said an$F$**-homomorphism** if $\psi|_F = 1_F$

Theorem 2.2.1
Let E/F be a field extension and $\alpha \in E$. If α is transcendental over F, then

$$F[a] \cong F[x] \quad \textbf{and} \quad F(\alpha) \cong F(x)$$

In particular, $F[\alpha] \neq F(\alpha)$

Proof: Let $\psi : F(x) \to F(\alpha)$ be unique F-homomorphism defined by $\psi(x) = \alpha$. Thus, for $f(x), g(x) \in F[x]$, $g(x) \neq 0$, we have

$$\psi(f/g) = f(\alpha)/g(\alpha) \in F(\alpha)$$

Note that since α is transcendental, we have $g(\alpha) \neq 0$. Thus the map is well-defined. Since $F[x]$ is a field and $\ker \psi$ is an ideal of $F(x)$, we have $\ker(\psi) = F(x)$ or 0. Thus $\psi = 0$ or ψ is injective. Since $\psi(x) = \alpha \neq 0$, ψ is injective. Also, since $F(x)$ is a field, $\operatorname{Im} \psi$ contains a field generated by F amd α. i.e. $F(\alpha) \subseteq \operatorname{Im} \psi$. Thus $\operatorname{Im} \psi = F(\alpha)$ and ψ is surjective. It follows that ψ is an isomorphism and we have

$$F[a] \cong F[x] \quad \textbf{and} \quad F(\alpha) \cong F(x)$$

as desired.

Theorem 2.2.2
Let E/F be a field extension and $\alpha \in E$. If α is algebraic over F, there exists a unique monic irreducible polynomial $p(x) \in F[x]$ such that there exists a F-isomorphism

$$\psi : F[x]/\langle p(x)\rangle \to F[\alpha] \quad \textbf{with} \quad \psi(x) = a$$

From which we conclude $F[\alpha] = F(\alpha)$

Proof: We first remark that since α is algebraic, the map in the proof of **Theorem 2.2.1** $f/g \mapsto f(\alpha)/g(\alpha)$ is not defined. Consider the unique F-homorphism $\psi : F[x] \to F(\alpha)$ defined by $\psi(x) = \alpha$. Thus for $f(x) \in F[x]$, we have $\psi(f) = f(\alpha) \in F[a]$. Since $F[x]$ is a ring, $\operatorname{Im}\psi$ contains a ring generated by F and α. i.e. $F[a] \subseteq \operatorname{Im}\psi\mathrm{m}$, thus $\operatorname{Im}\psi = F[a]$. Let

$$I = \ker\psi = \{f(x) \in F[x],\ f(\alpha) = 0\}$$

Since α is algebraic, $I \neq \{0\}$. We have $F[x]/I \cong \operatorname{Im}\psi$, a subring of a field $F(\alpha)$. Thus $F[x]/I/$ is an integral domain and I is prime ideal. It follows that $I = \langle p(x)\rangle$ where $p(x)$ is irreducible. If we assume that $p(x)$ is monic, then it's unique. It follows that

$$F[x]/\langle p(x) \cong F[\alpha]$$

Since $p(x)$ is irreducible, $F[x]/\langle p(x)\rangle$ is a field. Thus $F[a]$ is a field. Also, since the $F(\alpha)$ is the smallest field containing $F[\alpha]$, we have

$$F[\alpha] = F(\alpha)$$

which completes the proof.

Definition 2.2.4 — Minimal Polynomial.
If α is algebraic over a field F, the unique monic irreducible polynomial $p(x)$ in **Theorem 2.2.2** is called the **minimial polynomial of α over F**. From the proof of **Theorem 2.2.2**, we see that If $f(x) \in F[x]$ with $f(\alpha) = 0$, then $p(x) \mid f(x)$

As a direct consequence of **Theorem 2.2.1 and 2.2.2**. we have

Theorem 2.2.3
Let E/F be a field extension and $\alpha \in E$
(1) α is transcendental over $F \iff [F(\alpha) : F] = \infty$
(2) α is algebraic over $F \iff [F(\alpha) : F] < \infty$

Moreover, if $p(x)$ is the minimal polynomial of α over F, we have $[F(\alpha) : F] = \deg(p)$ and $\left\{1, \alpha, \alpha^2, \ldots, \alpha^{\deg(p)-1}\right\}$ is a basis of $F(\alpha)/F$ (This is why we call $[F(\alpha) : F]$ the degree of field extension)

Proof: It suffices to show ($\Longrightarrow$) for (1) and (2) (since ($\Longleftarrow$) of (1) is ($\Longrightarrow$) of (2) and vice

versa.)

For (1) $\Longrightarrow$, by **Theorem 2.2.1** if α is transcendental over F, $F(\alpha) \cong F(x)$. In $F(x)$, the elements $\{1, x, x^2, \ldots\}$ are linearly independent over F, thus we have $[F(\alpha) : F] = \infty$

For (2) $\Longrightarrow$, by **Theorem 2.2.2**, if α is algebraic over F, $F(\alpha) \cong F[x]/\langle p(x)\rangle$ with $x \mapsto \alpha$. Note that

$$F[x]/\langle p(x)\rangle = \{r(x) \in F[x] : \ \deg(r) < \deg(p)\}$$

Thus $\{1, x, x^2, \ldots, x^{\deg(p)-1}\}$ forms a basis of $F[x]/\langle p(x)\rangle$. It follows that $[F(\alpha) : F] = \deg(p)$ and $\{1, \alpha, \alpha^2, \ldots, \alpha^{\deg(p)-1}\}$ is a basis of $F(\alpha)$ over F

■ **Example 2.4** Let p be prime and $\zeta_p = e^{\frac{2\pi i}{p}}$, a p-th root of 1. We have seen in **Chapter 1** that ζ_p is a root of the p-th cyclotomic polynomial $\Phi_p(x)$, which is irreducible. Thus, by **Theorem 2.2.3** $\Phi_p(x)$ is the minimal polynomial of ζ_p over $\mathbb{Q}$ and

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$$

The field $\mathbb{Q}(\zeta_p)$ is called the **p-th cyclotomic extension of** $\mathbb{Q}$ ■

Theorem 2.2.4

Let E/F be a field extension. If $[E : F] < \infty$, there exists $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$ such that

$$F \subsetneq F(\alpha_1) \subsetneq F(\alpha_1, \alpha_2) \subsetneq \ldots \subsetneq F(\alpha_1, \alpha_2, \ldots, \alpha_n) = E$$

Thus, to understand a finite extension, it suffices to understand a finite simple extension.

Proof: We will prove this theorem by induction on $[E : F]]$. If $[E : F] = 1$, so $E = F$ we are done. Suppose $[E : F] > 1$ and the statement holds for all field extension $\tilde{E}/\tilde{F}$ with $[\tilde{E} : \tilde{F}] < [E : F]$. Let $\alpha_1 \in E/F$, by **Theorem 2.1.1**

$$[E : F] = [E : F(\alpha_1)] \cdot [F(\alpha_1) : F]$$

Since $[F : F(\alpha_1)] > 1$, we have $[E : F(\alpha_1)] < [E : F]$. By induction hypothesis, there exist $\alpha_2, \alpha_3, \ldots, \alpha_n$ such that

$$F(\alpha_1) \subsetneq F(\alpha_1)(\alpha_2) \subsetneq F(\alpha_1)(\alpha_2, \alpha_3) \subsetneq \ldots \subsetneq F(\alpha_1)(\alpha_2, \ldots, \alpha_n) = E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

Therefore, we have

$$F \subsetneq F(\alpha_1) \subsetneq F(\alpha_1, \alpha_2) \subsetneq \ldots \subsetneq F(\alpha_1, \alpha_2, \ldots, \alpha_n) = E$$

which completes the proof.

Definition 2.2.5 — Algebraic Extension & Transcendental Extension.

A field extension E/F is **algebraic** if every $\alpha \in E$ is a **algebraic** over F. Otherwise, it is

transcendental

Theorem 2.2.5
Let E/F be a field extension, if $[E:F] < \infty$, then E/F is **algebraic**

Proof: Suppose $[E:F] = n$. for $\alpha \in E$, the elements $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ are not linearly independent over F. Thus there exist $c_i \in F$ $(0 \leq i \leq n)$ is not 0, such that

$$\sum_{i=1}^{n} c_i \alpha^i = 0$$

Thus α is a root of the polynomial $\sum_{i=0}^{n} c_i x^i \in F[x]$, thus it is **algebraic** over F

Theorem 2.2.6
Let E/F be a field extension, we define

$$L = \{\alpha \in E : \ [F(\alpha):F] < \infty\}$$

Then L is an **intermediate** field of E/F

Proof: If $\alpha, \beta \in L$, we need to show $\alpha \pm \beta$, $\alpha\beta$, $\frac{\alpha}{\beta}(\beta \neq 0)$ are in L. By definition of L, we have $[F(\alpha):F] < \infty$ and $[F(\beta):F] < \infty$. Consider the field $F(\alpha, \beta)$. Since the minimal polynomial of α over $F(\beta)$ divides the minimal polynomial of α over F (the minimal polynomial of α over F, say $p(x) \in F[x]$, it is also a polynomial over $F(\beta)$ i.e. $p(x) \in F(\beta)[x]$ such that $p(\alpha) = 0$), we have $[F(\alpha, \beta) : F(\beta)] \leq [F(\alpha):F]$. Combining this with **Theorem 2.1.1** we have

$$[F(\alpha, \beta):F] = [F(\alpha, \beta) : F(\beta)] \cdot [F(\beta):F] \leq [F(\alpha):F] \cdot [F(\beta):F] < \infty$$

Since $\alpha + \beta \in F(\alpha, \beta)$, it follows that

$$[F(\alpha + \beta):F] \leq [F(\alpha, \beta):F] < \infty$$

i.e. $(\alpha + \beta) \in L$. Similarly, we can show $\alpha - \beta$,$\alpha\beta$, $\frac{\alpha}{\beta}(\beta \neq 0)$ are in L. Therefore, L is a field, which completes the proof.

Definition 2.2.6 — Algebraic Closure.
Let E/F be a field extension, the set

$$L = \{\alpha \in E : \ [F(\alpha) : F] < \infty\}$$

is called **algebraic closure** of F in E

Definition 2.2.7 — Algebraically Closed.
A field F is **algebraically closed** if for any algebraic extension E/F, we have $E = F$

■ **Example 2.5**
By fundamental theorem of algebra, $\mathbb{C}$ is algebraically closed. Moreover, $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$ in $\mathbb{C}$ and we have $[\mathbb{C} : \mathbb{R}] = 2$ ■

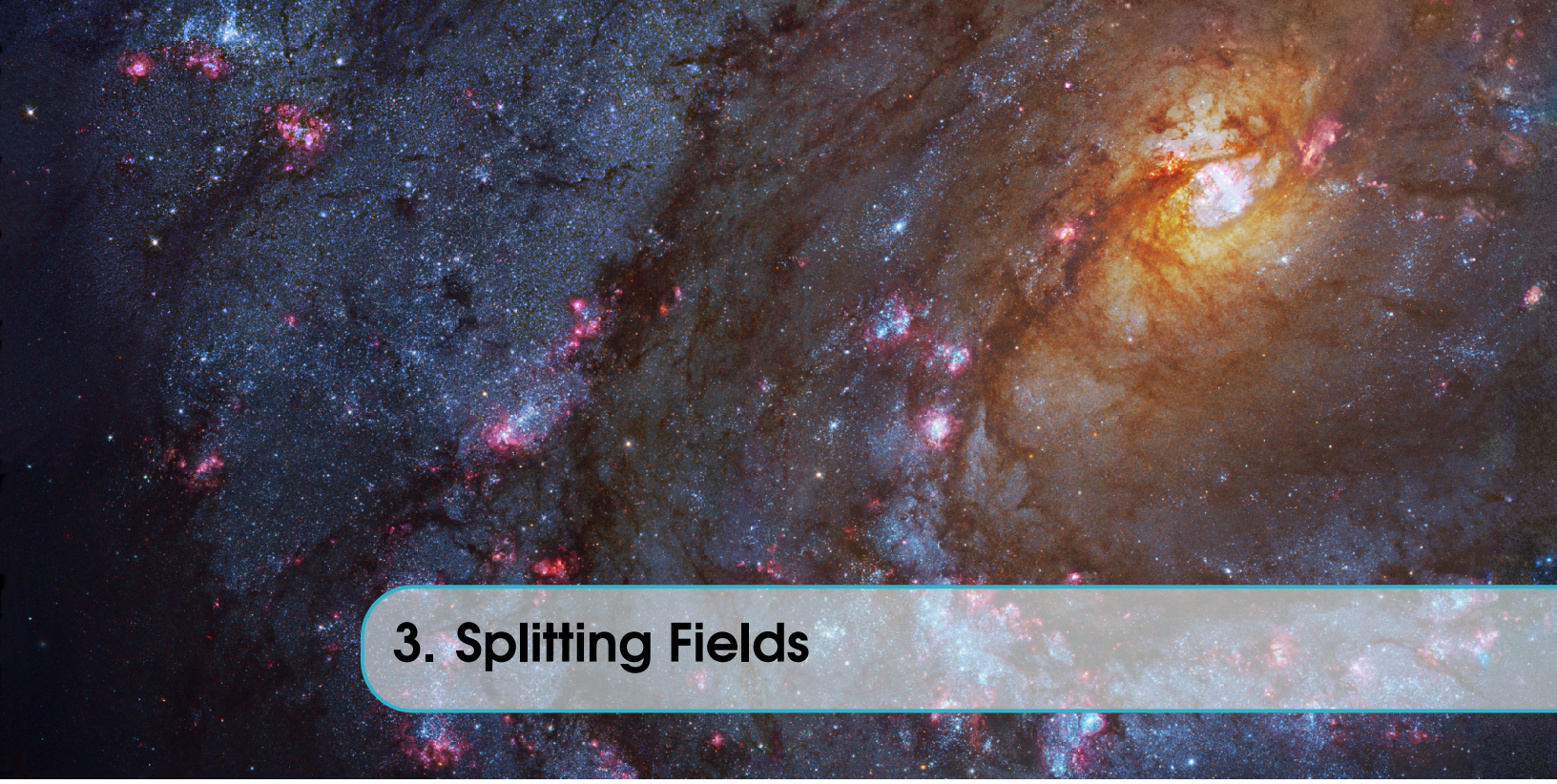
■ **Example 2.6**
Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. i.e.

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \ \alpha \textbf{ is algebraic over } \mathbb{Q}\}$$

Since $\zeta_p \in \overline{\mathbb{Q}}$, we have

$$[\overline{\mathbb{Q}} : \mathbb{Q}] \geq [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$$

As $p \to \infty$, we have $[\overline{\mathbb{Q}} : \mathbb{Q}] \to \infty$. We have seen in **Theorem 2.2.5** that if E/F is finite, then E/F is algebraic. However, this example shows that the converse of **Theorem 2.2.5** is false. ■



3. Splitting Fields

3.1 Existence of Splitting Fields

Definition 3.1.1
Let E/F be a field extension. We say $f(x) \in F[x]$ **splits over** E if E contains all roots for $f(x)$. i.e. $f(x)$ is a product of linear factors in $E[x]$

Definition 3.1.2
Let $\widetilde{E}/F$ be a field extension, $f(x) \in F[x]$, and $F \subseteq E \subseteq \widetilde{E}$. If

(1) $f(x)$ splits over E;
(2) There is no proper subfield of E such that $f(x)$ splits over;
then we say E is a **splitting field** of $f(x) \in F[x]$ in E

To show the existence of a splitting field of $f(x)$, we first find a field extension of F which contains at least one root of $f(x)$

Theorem 3.1.1
Let $p(x) \in F[x]$ be **irreducible**. The **quotient ring** $F[x]/\langle p(x)\rangle$ is a field containing F and a root of $f(x)$

Proof: Since $p(x)$ is irreducible the ideal $I = \langle p(x)\rangle$ is maximal. Thus $E = F[x]/I$ is a field. We consider the map

$$\psi : F \to F, \qquad a \mapsto a + I$$

Since F is a field and $\psi \neq 0$, so ψ is injective. Thus, by identifying F with $\psi(F)$, F can be viewed as a subfield of E.

Claim: Let $\alpha = x + I \in E$, then α is a root of $p(x)$. Write

$$\begin{aligned} p(x) &= a_0 + a_1 x + \cdots + a_n x^n \\ &= (a_0 + I) + (a_1 + I)x + \cdots + (a_n + I)x^n \\ &\in E[x] \end{aligned}$$

Then we have

$$\begin{aligned} p(\alpha) &= (a_0 + I) + (a_1 + I)\alpha + \cdots + (a_n + I)\alpha^n \\ &= (a_0 + I) + (a_1 + I)(x + I) + \cdots + (a_n + I)(x + I)^n \\ &= (a_0 + a_1 x + \cdots + a_n x^n) + I \qquad \textbf{since } (x + I)^i = x^i + I \textbf{ for } 0 \leq i \leq n \\ &= p(x) + I \\ &= 0 + I \\ &= I \end{aligned}$$

Thus, we have $\alpha = x + I \in E$ is a root of $p(x)$.

Theorem 3.1.2 — Kronecker Theorem.
Let $f(x) \in F[x]$, there exist a field E containing F such that $f(x)$ splits over E

Proof: We prove this theorem by induction on $\deg(f)$. If $\deg(f) = 1$, we let $E = F$ and we are done. Suppose $\deg(f) > 1$ and the statement holds for all $g(x)$ with $\deg(g) < \deg(f)$ ($g(x)$ is not necessarily in $F[x]$). Write $f(x) = p(x)h(x)$, where $p(x), h(x) \in F[x]$ and $p(x)$ is irreducible. By **Theorem 3.1.1**, there exists a field K such that K containing a root of $p(x)$, say α. Then we have

$$p(x) = (x - \alpha)q(x) \qquad \textbf{and} \qquad f(x) = (x - \alpha)h(x)q(x)$$

where $q(x) \in K[x]$. Since $\deg(hq) < \deg(f)$, by induction, there exist a field E containing K over which $h(x)q(x)$ splits. It follows that $f(x)$ splits over E.

Theorem 3.1.3
Every $f(x) \in F[x]$ has a splitting field, which is a finite extension of F

Proof: For $f(x) \in F[x]$, by **Theorem 3.1.2** there exists a field extension E/F over which $f(x)$ splits. We say $\alpha_1, \alpha_2, ..., \alpha_n$ are roots of $f(x)$ in E. Consider $F(\alpha_1, \alpha_2, ..., \alpha_n)$ This is the smallest subfield of E containing all roots of $f(x)$. So $f(x)$ does not split over any proper subfield of it. Thus $F(\alpha_1, \alpha_2, ..., \alpha_n)$ is the splitting field of $f(x)$ in E. In addition, since α_i are all algebraic, so $F(\alpha_1, \alpha_2, ..., \alpha_n)/F$ is finite.

3.2 Uniqueness of Splitting Fields

We have seen from **Theorem 3.1.3** that for a fixed field extension E/F, a splitting field of $f(x) \in F[x]$ in E is of the form $F(\alpha_1, \alpha_2, ..., \alpha_n)$ where α_i are roots of $f(x)$ in E. Thus, it's unique within E
Question: If we change E/F to a different field extension, say E_1/F, what's the relation between the splitting field of $f(x)$ in E and the one in E_1?

Definition 3.2.1 Let $\phi : R \to R_1$ be a ring homomorphism, and $\Phi : R[x] \to R_1[x]$ be the unique ring homomorphism satisfying $\Phi \mid_R = \phi$ and $\Phi(x) = x$. In this case, we say Φ **extends** ϕ. More generally, if $R \subseteq S$, $R_1 \subseteq S_1$ and $\Phi : S \to S_1$ is a ring homomorphism with $\Phi \mid_R = \phi$, we say Φ **extends** ϕ.

Theorem 3.2.1
Let $\phi : F \to F_1$ be an isomorphism of fields and $f(x) \in F[x]$. Let $\Phi : F[x] \to F_1[x]$ be unique ring isomorphism which extends ϕ. Let $f_1(x) = \Phi(f(x))$ and E/F and E_1/F_1 be splitting fields of $f(x)$ and $f_1(x)$ respectively. Then there exists an isomorphism $\psi : E \to E_1$ which extends ϕ.

Proof: We prove this theorem by induction on $[E : F]$. If $[E : F] = 1$, then $f(x)$ is a product of linear factors in $F[x]$, and so $f_1(x) \in F_1[x]$. Thus, we have $E = F$ and $E_1 = F_1$. Take $\psi = \phi$ and we are done.
Now suppose $[E : F] > 1$ and the statement is true for all field extensions $\widetilde{E}/\widetilde{F}$ with $[\widetilde{E} : \widetilde{F}] < [E : F]$. Let $p(x) \in F[x]$ be an irreducible factor of $f(x)$ with $\deg(p) \geq 2$ and let $p_1(x) = \Phi(p(x))$ (such $p(x)$ exists as if all irreducible factors of $f(x)$ are degree 1. Then $[E : F] = 1$) Let $\alpha \in E$ and $\alpha_1 \in E_1$ be roots of $p(x)$ and $p_1(x)$ respectively. From **Theorem 2.2.2**, we have an $F-$isomorphism

$$F(\alpha) \cong F[x]/\langle p(x)\rangle \qquad \alpha \mapsto x + \langle p(x)\rangle$$

Similarly, there is an F_1-isomorphism

$$F_1(\alpha_1) \cong F_1[x]/\langle p_1(x)\rangle \qquad \alpha_1 \mapsto x + \langle p_1(x)\rangle$$

Consider the isomorphism $\Phi : F[x] \to F_1[x]$ which extends ϕ. Since $p_1(x) = \Phi(p(x))$, there exists a field isomorphism

$$\widetilde{\Phi} : F[x]/\langle p(x)\rangle \to F_1[x]/\langle p_1(x)\rangle \quad x + \langle p(x)\rangle \mapsto x + \langle p_1(x)\rangle$$

which extends ϕ. It follows that there exists a field isomorphism

$$\widetilde{\phi} : F(\alpha) \to F_1(\alpha_1) \qquad \alpha \to \alpha_1$$

which extends ϕ. Note that since $\deg(p) \geq 2$, $[E : F(\alpha)] < [E : F]$. Since E (resp E_1) is the splitting field of $f(x) \in F(\alpha)[x]$ (resp $f_1(x) \in F_1(\alpha_1)[x]$) over $F(\alpha)$ (resp $F_1(\alpha_1)$) By induction, there exists $\psi : E \to E_1$ which extends ϕ. Thus, ψ also extends ϕ.

Corollary 3.2.2
Any two splitting fields of $f(x) \in F[x]$ over F are $F-$isomorphic. Then, we can now say "the" splitting field of $f(x)$ over F.

Proof: Let $\phi : F \to F$ be the identity map and apply **Theorem 3.2.1**

3.3 Degrees of Splitting Fields

Theorem 3.3.1
Let F be a field and $f(x) \in F[x]$ with $\deg(f) = n \geq 1$. If E/F is the splitting field of $f(x)$, then $[E : F] \mid n!$

Proof: We prove this theorem by induction on $\deg(f)$. If $\deg(f) = 1$, choose $E = F$ and we have $[E : F] \mid 1!$. Suppose we have $\deg(f) > 1$ and the statement holds for all $g(x)$ with $\deg(g) < \deg(f)$ ($g(x)$ is not necessarily in $F[x]$), there are two cases:
Case 1: If $f(x) \in F[x]$ is irreducible and $\alpha \in E$ is a root of $f(x)$, by **Theorem 2.2.2**

$$F(\alpha) \cong F[x]/\langle f(x)\rangle \qquad \textbf{and} \qquad [F(\alpha) : F] = \deg(f) = n$$

Write $f(x) = (x-\alpha)g(x) \in F(\alpha)[x]$ with $g(x) \in F(\alpha)[x]$. Since E is the splitting field of $g(x)$ over $F(\alpha)$ and $\deg(g) = n-1$. By induction, $[E : F(\alpha)] \mid (n-1)!$. Since $[E : F] = [E : F(\alpha)][F(\alpha) : F]$, it follows that $[E : F] \mid n!$.
Case 2: If $f(x)$ is not irreducible, write $f(x) = g(x)h(x)$ with $g(x), h(x) \in F[x]$, $\deg(g) = m$, $\deg(h) = k$. $m + k = n$ and $1 \leq m, k \leq n$. Let K be the splitting field of $g(x)$ over K and $\deg(g) = m$. By induction, $[K : F] \mid m!$. Since E is the splitting field of $h(x)$ over K and $\deg(h) = k$, by induction $[E : K] \mid k!$, thus we have $[E : F] \mid m!k!$, which is a factor of $n!$ (since $n!/m!k! = \binom{n}{m} \in \mathbb{Z}$)

4. More Field Theory

4.1 Prime Field

Definition 4.1.1 — Prime Field.
The **prime field** of a field F is the intersection of all subfields of F

Theorem 4.1.1
If F is a field, then its prime field is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}_p$ for some prime p

Proof: Let F_1 be a subfield of F, we consider the ring map

$$\mathcal{X} : \mathbb{Z} \to F_1 \quad n \to n \cdot 1 \quad \textbf{where } 1 \in F_1 \subseteq F$$

Let $I = \ker \mathcal{X}$ be the kernel of $\mathcal{X}$, since $\mathbb{Z}/I \cong \operatorname{Im} \mathcal{X}$ (by the first isomorphism theorem), a subring of F_1, it is an integral domain. Thus, I is a prime ideal. Now, we have two cases:
(1) If $I = \langle 0 \rangle$, then $Z \subseteq F_1$, since F_1 is a field, then

$$\mathbb{Q} = \textbf{Frac}(\mathbb{Z}) \subseteq F_1$$

(2) If $I = \langle p \rangle$, by the first isomorphism theorem we have

$$\mathbb{Z}_p = \mathbb{Z}/\langle p \rangle \cong \operatorname{Im} \mathcal{X} \subseteq F_1$$

this completes our proof.

4.2 Formal Derivatives and Repeated Roots

Definition 4.2.1 — Formal Derivative.
If F is a field, the monomials $\{1, x, x^2, ...\}$ form an F-basis of $F[x]$. Define the linear operator $D : F[x] \to F[x]$ by $D(1) = 0$ and $D(x^i) = ix^{i-1}$ $(i \in \mathbb{N})$. Thus, for

$$f(x) = a_0 + a_1x + a_2x + ... + a_nx^n \ , \quad a_i \in F$$

we have

$$D(f)(x) = a_1 + 2a_2x + ... + na_nx^{n-1}$$

Note that
(1) $D(f + g) = D(f) + D(g)$
(2) Leibniz Rule: $D(fg) = D(f) \cdot g + f \cdot D(g)$
We call $D(f) = f'$ for the **formal derivative** of f.

Theorem 4.2.1
Let F be a field and $f(x) \in F[x]$
(1) If $ch(F) = 0$, then $f'(x) = 0$ if and only if $f(x) = c$ for some $c \in F$
(2) If $ch(F) = p$, then $f'(x) = 0$ if and only if $f(x) = g(x^p)$ for some $g(x) \in F[x]$

Proof (1): $\Longleftarrow$ is clear.
$\Longrightarrow$: For $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$, $f'(x) = a_1 + 2a_2x + ... + na_nx^{n-1} = 0$ implies that $ia_i = 0$ for $1 \leq i \leq n$. Since $ch(F) = 0$, $i \neq 0$, thus $a_i = 0$ for all $i \geq 1$. Then we have $f(x) = a_0 \in F$

Proof (2): $\Longleftarrow$ We write $g(x) = b_0 + b_1x + ... + b_mx^m$, then

$$f(x) = g(x^p) = b_0 + b_1x^p + b_2x^{2p} + ... + b_mx^{pm}$$

Then

$$f'(x) = pb_1x^{p-1} + 2pb_2x^{2p-1} + ... + pmb_mx^{pm-1}$$

Since $ch(F) = p$, we have $f'(x) = 0$
$\Longrightarrow$ For $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$, $f'(x) = a_1 + 2a_2x + ... + na_nx^{n-1} = 0$ implies that $ia_i = 0$ for $1 \leq i \leq n$. Since $ch(F) = p$, $ia_i = 0$ implies that $a_i = 0$ unless $p \mid i$, then

$$f(x) = a_0 + a_px^p + a_{2p}x^{2p} + ... + a_{mp}x^{mp} = g(x^p)$$

where $g(x) = a_0 + a_px + a_{2p}x^2 + ... + a_{mp}x^m \in F[x]$.

Definition 4.2.2 — Repeated Root.
Let E/F be a field extension and $f(x) \in F[x]$, we say $\alpha \in E$ is a **repeated root** of $f(x)$ if and only if $f(x) = (x - \alpha)^2g(x)$ for some $g(x) \in E[x]$

Theorem 4.2.2
Let E/F be a field extension, $f(x) \in F[x]$ and $\alpha \in E$. Then α is a repeated root of $f(x)$ if and

only if $(x-\alpha)$ divides both f and f' i.e. $(x-\alpha) \mid \gcd(f, f')$

Proof: $\Longrightarrow$ Suppose $f(x) = (x-\alpha)^2 g(x)$, then

$$f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x) = (x-\alpha) \cdot (2g(x) + (x-\alpha)g'(x))$$

Then $(x-\alpha)$ divides both f and f'

$\Longleftarrow$: Suppose that $(x-\alpha)$ divides both f and f'. Write $f(x) = (x-\alpha)h(x)$ where $h(x) \in E[x]$, then

$$f'(x) = h(x) + (x-\alpha)h'(x)$$

Since $f(\alpha) = 0$ we have $h(\alpha) = 0$. Then $(x-\alpha)$ is a factor of $h(x)$ and $f(x) = (x-\alpha)^2 g(x)$ for some $g(x) \in E[x]$

Corollary 4.2.3
Let F be a field and $f(x) \in F[x]$, then $f(x)$ has no repeated root in any extension of F if and only if $\gcd(f, f') = 1$

Proof: Note that $\gcd(f, f') \neq 1$ if and only if $(x-\alpha) \mid \gcd(f, f')$ for α in some extensions of F. By **Theorem 4.2.2** the result follows.

■ **Remark 4.1** We notice that the condition of repeated roots depends on the extensions of F while the gcd condition involves only F ■

4.3 Finite Fields

Given a field F, let $F^* = F \setminus \{0\}$ be the multiplicative group of nonzero elements of F

Proposition 4.3.1
Since F is a finite field, by **Theorem 4.1.1**, its prime field is Z_p. Since F is a finite dimensional vector space over $\mathbb{Z}_p$, we have $F \cong \mathbb{Z}_p \times \mathbb{Z}_p \times ..... \times \mathbb{Z}_p$ (n summands), then $|F| = p^n$

Theorem 4.3.2
Let F be a field and G be a finite subgroup of F^*, Then G is a cyclic group. In particular, if F is a finite field, then F^* is a cyclic group

Proof: **WLOG** we can assume that $G \neq \{1\}$. Since G is a finite abelian group, $G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times ..... \times \mathbb{Z}/n_r\mathbb{Z}$ where $n_1 > 1$ and $n_i \mid n_j$ for $1 \leq i \leq j \leq r$. Since $n_r(\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times ..... \times \mathbb{Z}/n_r\mathbb{Z}) = 0$, it follows that every $u \in G$ is a root of $x^{n_r} - 1 \in F[x]$. Since the polynomial has at most n_r distinct roots in F, we have $r = 1$ and $G \cong Z/n_r\mathbb{Z}$

By taking u to be a generator of the multiplicative group of F^*, we have

Corollary 4.3.3
If F is a finite field, then F is a simple extension of $\mathbb{Z}_p$. i.e. $F = \mathbb{Z}_p(u)$ for some $u \in F$

Theorem 4.3.4
1. F is a finite field with $|F| = p^n$ if and only if F is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$
2. Let F be a finite field with $|F| = p^n$, let $m \in \mathbb{N}$ with $m \mid n$. Then F contains a unique subfield K with $|K| = p^m$

Proof (1) : $\Longrightarrow$ If $|F| = p^n$, then $|F^*| = p^n - 1$. Then every $u \in F^*$ satisfies $u^{p^n} = 1$ and it's a root of $x\big(x^{p^n-1} - 1\big) = x^{p^n} - x \in \mathbb{Z}_p[x]$, Since $0 \in F$ is also a root of $x^{p^n} - x$, the polynomial $x^{p^n} - x$ has p^n distinct roots in F. i.e. it splits over F. Then F is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$
$\Longleftarrow$ Suppose that F is a splitting field of $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p$. Since $ch(F) = p$, we have $f'(x) = -1$. Since $\gcd(f, f') = 1$, by **Corollary 4.2.3** $f(x)$ has p^n distinct roots in F. Let E be the set of all roots of $f(x)$ in F and $\varphi : F \to F$ be given by $u \mapsto u^{p^n}$. For $u \in F$, u is a root of $f(x)$ if division, the set E is a subfield of F of order p^n, which contains $\mathbb{Z}_p$ (since all $u \in \mathbb{Z}_p$ satisfy $u^p = p$ and thus $u^{p^n} = u$). Since F is a splitting field, it's generated over $\mathbb{Z}_p$ by the roots of $f(x)$. i.e. the elements of E, then $F = \mathbb{Z}_p(E) = E$

Proof (2): We recall that

$$x^{ab} - 1 = (x^a - 1)(x^{ab-a} + x^{ab-2a} + ... + x^a + 1)$$

Then if $n = mk$, we have

$$x^{p^n} - x = x\big(x^{p^n-1} - 1\big) = x\big(x^{p^m-1} - 1\big)g(x) = \big(x^{p^m} - x\big)g(x)$$

for some $g(x) \in \mathbb{Z}_p[x]$. Since $\big(x^{p^n} - x\big)$ splits over F, so does $\big(x^{p^m} - x\big)$. Let

$$K = \big\{u \in F : u^{p^m} - u = 0\big\}$$

Then $|K| = p^r$ since roots of $\big(x^{p^m} - x\big)$ are distinct. Also, by **(1)** K is a field. Note that if $\widetilde{K} \subseteq F$ be any subfield with $\left|\widetilde{K}\right| = p^m$, then $\widetilde{K} \subseteq K$. It follows that $\widetilde{K} = K$, then we see that a subfield K of F with $|K| = p^m$ is unique.

A direct consequence of Theorem 4.3.4 and Corollary 3.2.2, we have

Corollary 4.3.5 — E.H. Moore.
Let p be a prime and $n \in \mathbb{N}$, then any two finite field of order p^n are isomophic. We denote such a field by F_{p^n}

4.4 Separable Polynomials

Definition 4.4.1
Let F be a field and $f(x) \in F[x] \setminus \{0\}$. If $f(x)$ is irreducible, we say $f(x)$ is **separable over** F if it has no repeated root in any extension of F. In general we say $f(x)$ is separable over F if each irreducible factor of $f(x)$ is separable over F.

■ **Example 4.1** $f(x) = (x-4)^9$ is separable in $\mathbb{Q}[x]$ ■

■ **Example 4.2** Consider the polynomial $f(x) = x^n - a \in F[x]$ with $n \geq 2$
We recall **Corollary 4.2.3** which states that if $\gcd(f, f') = 1$, then $f(x)$ has no repeated root in any extension of F. i.e. $f(x)$ is separable.
Note that if $a = 0$, the only irreducible factor of $f(x)$ is x. Since $\gcd(x, x') = 1$, $f(x)$ is separable.
Now we assume $a \neq 0$, note that $f'(x) = nx^{n-1}$. Thus, the only irreducible factor of $f'(x)$ is x, provided that $n \neq 0$
(1) If $ch(F) = 0$, since $x \nmid f(x)$, we have $\gcd(f, f') = 1$, then $f(x)$ is separable.

(2) If $ch(F) = p$ and $\gcd(n, p) = 1$, since $x \nmid f(x)$, then $\gcd(f, f') = 1$. Hence $f(x)$ is separable.

(3) If $ch(F) = p$, consider $f(x) = x^p - a$, since $f'(x) = px^{p-1} = 0$, we have $\gcd(f, f') = 1$. However, it's still possible that all irreducible factors $l(x)$ of $f(x)$ has property that $\gcd(l, l') = 1$. To decide if $f(x)$ is separable, we need to find its irreducible factors first. Define

$$F^p = \{b^p : b \in F\}$$

which is a subfield of F.

(3.1) If $a \in F^p$, say $a = b^p$ for some $b \in F$, then

$$f(x) = x^p - b^p = (x-b)^p \in F[x]$$

which is irreducible. Since each irreducible factor of $f(x)$ is linear it's separable. Thus, $f(x)$ is separable.

(3.2) Suppose $a \notin F^p$
Claim: $f(x) = x^p - a$ is irreducible in $F[x]$.
Write $x^p - a = g(x)h(x)$ where $g(x), h(x) \in F[x]$ are monic polynomials. Let E/F be an extension where $x^p - a$ has a root. We say $\beta \in E$ ($\beta^p - a = 0$). Note that $a = \beta^p \notin F^p$, $\beta \notin F$. We have

$$x^p - a = x^p - \beta^p = (x-\beta)^p$$

Thus, $g(x) = (x-\beta)^r$ and $h(x) = (x-\beta)^s$ for some $r, s \in \mathbb{N} \cup \{0\}$ and $r + s = p$. Write

$$g(x) = x^r - r\beta x^{r-1} + ...$$

then $r\beta \in F$. Since $\beta \notin F$, as an element of F, we have $r = 0$ (if $r \neq 0$, then $r^{-1} \in F$ and $r^{-1}r\beta = \beta \in F$, a contradiction). Then, as an integer, we have $r = 0$ or $r = p$. It follows that either

$g(x) = 1$ or $h(x) = 1$ in $F[x]$. Then $f(x)$ is irreducible.
Since $f(x)$ is irreducible and $f(x) = (x - \beta)^p \in E[x]$, it's not separable. In this case, since all roots of $f(x)$ are the same, we say $f(x)$ is **purely inseparable**. ∎

Definition 4.4.2 — Perfect.
A field F is **perfect** if every (irreducible) polynomial $r(x) \in F[x]$ is separable over F

Theorem 4.4.1
Let F be a field.
(1) If $ch(F) = 0$, then F is perfect.
(2) If $ch(F) = p$ and $F^p = F$, then F is perfect.

Proof: Let $r(x) \in F[x]$ be irreducible, then

$$\gcd(r, r') = \begin{cases} 1, & \textbf{if } r' \neq 0 \\ r, & \textbf{if } r' = 0 \end{cases}$$

Suppose that $r(x)$ is not separable, then by **Corollary 4.2.3**, $\gcd(r, r') \neq 1$ so that $r'(x) = 0$
For (1): If $ch(F) = 0$, from **Theorem 4.2.1 (1)**, $r'(x) = 0$ implies that $r(x) = c \in F$, a contradiction since $\deg(r) \geq 1$. Then $r(x)$ is separable and F is perfect
For (2): If $ch(F) = p$, from **Theorem 4.2.1 (2)**, $r'(x) = 0$ implies that

$$r(x) = a_0 + a_1x^p + a_2x^{2p} + \ldots\ldots\ldots + a_mx^{mp}, \quad a_i \in F$$

Since $F = F^p$, we can write $a_i = b_i^p$ with $b_i \in F$, then

$$r(x) = b_0^p + b_1^px^p + \ldots\ldots\ldots\ldots + b_m^px^{mp} = (b_0 + b_1x + \ldots\ldots + b_mx^m)^p$$

a contradiction since $r(x)$ is irreducible, then $r(x)$ is separable and F is perfect.

∎ **Remark 4.2** Let $ch(F) = p$ and $F^p \neq F$ (e.g. $F = \mathbb{F}_p(x)$). If we take $a \in F \setminus F^p$, then the polynomial $x^p - a$ is purely inseparable. Then if $ch(F) = p$, F is perfect if and only if $F^p = F$ ∎

Corollary 4.4.2
Every finite field is perfect

Proof: Every finite field $F = \mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$ for some prime p and $n \in \mathbb{N}$, then for any $a \in F$ we have

$$a = a^{p^n} = \left(a^{p^{n-1}}\right)^p$$

Since $a^{p^{n-1}} \in F$ and $F = F^p$, then by **Theorem 4.4.1 (2)**, F is perfect.

5. The Sylow Theorems

5.1 Review of Group Actions

Definition 5.1.1
An **action** of a group G on a set S is a function $G \times S \to S$, $(g, x) \to gx$ such that for all $x \in S$ and $g_1, g_2 \in G$ we have

$$ex = x \quad \textbf{and} \quad (g_1 g_2)x = g_1(g_2 x)$$

where e is the identity element of the group G. If G acts on S for $x \in S$, we denote by $G \cdot x$ the orbit of x. i.e.

$$G \cdot x = \{gx : g \in G\}$$

Also, we denote by G_x the **stabilizer** of x i.e.

$$G_x = \{g \in G : gx = x\}$$

which is a subgroup of G. We have $|G \cdot x| = |G : G_x|$

■ **Example 5.1**
Let G be a group acting on itself by conjugation i.e. $(g, x) \mapsto gxg^{-1}$. Then for $x \in G$

$$C_G(x) \coloneqq G_x = \left\{g \in G : gxg^{-1} = x\right\}$$

is the **centralizer** of x. Let $Z(G)$ be the **center** of G i.e.

$$Z(G) = \left\{g \in G : gxg^{-1} = x \ \textbf{ for all } x \in G\right\}$$

Note that for $x \in G$, we have $|G \cdot x| = 1$ if and only if $x \in Z(G)$. Thus, we have the following class equations of G:

$$|G| = |Z(G)| + \sum_{i=1}^{m} |G : C_G(x_i)|$$

where $x_i \in G \setminus Z(G)$, the orbits $G \cdot x_i = \{gx_ig^{-1} : g \in G\}$ are distinct conjugacy classes of G and $|G \cdot x_i| = |G : C_G(x_i)| > 1$ for each i ∎

Lemma 5.1.1
Given a prime p, let G be a group of order p^n which acts on a finite set S. Let

$$S_0 = \{x \in S : gx = x \text{ for all } g \in G\}$$

Then we have $|S| \equiv |S_0|$ (mod p)

Proof: For $x \in S$, $|G \cdot x| = 1$ if and only if $x \in S_0$. Thus S can be written as a disjoint union.

$$S = S_0 \cup G \cdot x_1 \cup ..... \cup G \cdot x_m$$

with $|G \cdot x_i| > 1$ for all i, thus

$$|S| = |S_0| + |G \cdot x_1| + ... + |G \cdot x_m|$$

Since $|G \cdot x_i| > 1$ and $|G \cdot x_i| = |G : G_{x_i}|$ divides $|G| = p^n$, we have $p \mid |G \cdot x_i|$ for all i. It follows that $|S| \equiv |S_0|$ (mod p)

Theorem 5.1.2 — Cauchy.
Let p be a prime and G and finite group. If $p \mid |G|$, then G contains an element of order p

Proof: (by J.Mckay) Define

$$S = \{(a_1, a_2, ..., a_p) : a_i \in G \text{ and } a_1a_2....a_p = e\}$$

Since a_p is uniquely determined by $a_1, ..., a_{p-1}$, if $|G| = n$ we have $|S| = n^{p-1}$. Since $p \mid n$ we have $|S| \equiv 0$ (mod p). Let the group $\mathbb{Z}_p$ act on S by cyclic permutation. i.e. for $k \in \mathbb{Z}_p$

$$k(a_1, ..., a_p) = (a_{k+1}, a_{k+2}, ..., a_k)$$

One can verify that this action is well-defined (ex). Also $(a_1, a_2, ..a_p) \in S_0$ if and only if $a_1 = a_2 = ... = a_p$. Clearly, $(e, e, e, ..., e) \in S_0$ and hence $|S_0| \geq 1$. By **LEmma 5.1.1** we have $|S_0| \equiv |S| \equiv 0$ (mod p). Since $|S_0| \geq 1$ and $|S_0| = 0$ (mod p), we have $|S_0| \geq p$. Thus there exists $a \neq e$ such that $(a, a, a....., a) \in S_0$, which implies that $a^p = e$. Since p is a prime, the order of a is p

5.2 The Sylow Theorems

Definition 5.2.1 — p-group.
Let p be a prime. A group in which every element has order of a non-negative power of p is called a **p-group**

As a direct corollary of Theorem 5.1.2 we have

Corollary 5.2.1
A finite group G is a p-group if and only if $|G|$ is a power of p

Lemma 5.2.2
The center $Z(G)$ of a non-trivial finite p-group G contains more than one element.

Proof: Since G is a p-group, by **Corollary 5.2.1** $|G|$ is a power of p. We recall the class equation of

$$|G| = |Z(G)| + \sum_{i=1}^{m} |G : C_G(x_i)|$$

where $|G : C_G(x_i)| > 1$. Since $|G|$ is a power of p, $|G : C_G(x_i)| \mid |G|$ and $|G : C_G(x_i)| > 1$, we see that $p \mid |G : C_G(x_i)|$. It follows that $p \mid |Z(G)|$. Since $|Z(G)| \geq 1$, $Z(G)$ has at least p elements.

We recall that if H is a subgroup of G, then

$$N_G(H) = \left\{ g \in G : gHg^{-1} = H \right\}$$

is the **normalizer** of H in G. In particular, we have $H \lhd N_G(H)$

Lemma 5.2.3
If H is a p-subgroup of a finite group G, then $|N_G(H) : H| \equiv |G : H| \pmod{\text{p}}$.

Proof: Let S be a set of all left cosets of H in G and let H acts on S by left multiplication. Then $|S| = |G : H|$. For $x \in G$, we have

$$\begin{aligned} xH \in S_0 &\iff hxH = xH \quad \textbf{for all } h \in H \\ &\iff x^{-1}hxH = H \quad \textbf{for all } h \in H \\ &\iff x^{-1}Hx = H \quad \textbf{this holds since the above equality holds for all } h \in H \\ &\iff x \in N_G(H) \end{aligned}$$

Thus $|S_0|$ is the number of cosets xH with $x \in N_G(H)$, and since $|S_0| = |N_G(H) : H|$. By **LEmma 5.1.1**'

$$|N_G(H) : H| = |S_0| \equiv |S| = |G : H| \quad \textbf{(mod p)}$$

Corollary 5.2.4
Let H be a p-subgroup of a finite group G. If $p \mid |G : H|$, then $p \mid |N_G(H) : H|$ and $N_G(H) \neq H$

Proof: Since $p \mid |G : H|$, by **Lemma 5.2.3** we have

$$|N_G(H) : H| \equiv |G : H| \equiv 0 \quad \textbf{(mod p)}$$

Since $p \mid |N_G(H) : H|$ and $|N_G(H) : H| \geq 1$, we have $|N_G(H) : H| \geq p$, thus $N_G(H) \neq H$

We recall Cauchy's theorem states that if $p \mid |G|$, then $|G|$ contains an element a of order p. Thus $|\langle a \rangle| = p$. The following First Sylow Theorem can be viewed as a generalizations of Cauchy's Theorem

Theorem 5.2.5 — First Sylow Theorem.
Let G be a group of order $p^n m$,where p is a prime, $n \geq 1$ and $\gcd(p, m) = 1$. Then G contains a subgroup of order p^i for all $1 \leq i \leq n$. Moreover, every subgroup of G of order p^i $(i < n)$ is normal in some subgroup of order p^{i+1}

Proof: We prove this theorem by induction. For $i = 1$, since $p \mid |G|$, by **Theorem 5.1.2** G contains an element a of order p. Suppose that the statement holds for some $1 \leq i \leq n$, we say H is a subgroup of G order p^i. Then $p \mid |G : H|$. We have seen in the proof of **Corollary 5.2.4** that $p \mid |N_G(H) : H|$ and $|N_G(H) : H| \geq p$. Then by **Theorem 5.1.2** $N_G(H)/H$ contains a subgroup of order p. Such a group is the form H_1/H where H_1 is a subgroup of $N_G(H)$ containing H. Since $H \lhd N_G(H)$, we have $H \lhd H_1$. Finally, $|H_1| = |H| \cdot |H_1/H| = p^i \cdot p = p^{i+1}$

Definition 5.2.2 — Sylow p-subgroup.
A subgroup P of group G is called a **Sylow p-subgroup** of G if P is a maximal p-group of G. i.e. If $P \subseteq H \subseteq G$ with H is a p-group, then $P = H$

As a direct consequence of Theorem 5.2.5 we have

Corollary 5.2.6
Let G be a group of order $p^n m$, where p is a prime, $n \geq 1$ and $\gcd(p, m) = 1$. Let H be a p-subgroup of G

(1) H is a Sylow p-subgroup if and only if $|H| = p^n$
(2) Every conjugate of a Sylow p-subgroup is a Sylow p-subgroup.
(3) If there is only one Sylow p-subgroup P, then $P \lhd G$

Theorem 5.2.7 — Second Sylow Theorem.
If H is a p-subgroup of a finite group G, and P is any Sylow p-subgroup of G, then there exists $g \in G$ such that $H \subseteq gPg^{-1}$. In particularm any two Sylow p-subgroup of G are conjugate.

Proof: Let S be the set of all left cosets of P in G, and let H act on S be left multiplication. By **Lemma 5.1.1** we have $|S_0| \equiv |S| = |G : P| \pmod{\text{p}}$. Since $p \nmid |G : P|$, we have $|S_0| \neq 0$.

Then there exists $xP \in S_0$ for some $x \in G$. Note that

$$\begin{aligned} xP \in S_0 &\iff hxP = xP \quad \textbf{for all } h \in H \\ &\iff x^{-1}hxP = P \quad \textbf{for all } h \in H \\ &\iff x^{-1}Hx \subseteq P \\ &\iff H \subseteq xPx^{-1} \end{aligned}$$

If H is Sylow p-subgroup, then $|H| = |P| = \left|xPx^{-1}\right|$, then $H = xPx^{-1}$

Theorem 5.2.8 — Third Sylow Theorem.
If G is a finite group and p is a prime with $p \mid |G|$, then the number of Sylow p-subgroup of G divides G and is of the form $kp+1$ for some $k \in \mathbb{N} \cup \{0\}$

Proof: By **Theorem 5.2.7**, the number of Sylow p-subgroup of G is the number of conjugates of any one of them, say P. This number is $|G : N_G(P)|$, which is a divisor of $|G|$. Let S be the set of all Sylow p-subgroup of G and let P act on S by conjugation. Then $Q \in S_0$ if and only if $xQx^{-1} = Q$ for all $x \in P$. The latter condition holds if and only if $P \subseteq N_G(Q)$. Both P and Q are Sylow p-subgroup of G and hence of $N_G(Q)$. Thus by **Corollary 5.2.6**, they are conjugate in $N_G(Q)$. Since $Q \lhd N_G(Q)$, this can only occur if $Q = P$. Thus, $S_0 = \{P\}$ and by **Lemma 5.1.1** $|S| \equiv |S_0| \equiv 1 \pmod{\text{p}}$. Thus $|S| = kp+1$ for some $k \in \mathbb{N} \cup \{0\}$

■ **Remark 5.1** Suppose that G is a group with $|G| = p^r m$ and $\gcd(p, m) = 1$. Let n_p be the number of Sylow p-subgroup of G. By the **Theorem 5.2.8**, we see that $n_p \mid p^r m$ and $n_p \equiv 1 \pmod{\text{p}}$. Since $p \nmid n_p$, we have $n_p \mid m$ ■

■ **Example 5.2** **Claim**: Every group of order 15 is cyclic.
Let G be a group of order $15 = 3 \cdot 5$. Let n_p be the number of Sylow p-subgroup of G. By the **Theorem 5.2.8**, we have $n_3 \mid 5$ and $n_3 \equiv 1 \pmod 3$. Thus $u_3 = 1$. Similarly, we have $n_5 \mid 3$ and $n_5 \equiv 1 \pmod 5$. Thus $n_5 = 1$. It follows that there is only one Sylow 3-subgroup and 5-subgroup in G, say P_3 and P_5 respectively. Thus $P_3 \lhd G$ and $P_5 \lhd G$. Consider $|P_3 \cap P_5|$, which divides 3 and 5, thus $|P_3 \cap P_5| = 1$. Also, $|P_3P_5| = 15 = |G|$. It follows that

$$G \cong P_3 \times P_5 \cong \mathbb{Z}/\langle 3\rangle \times \mathbb{Z}/\langle 5\rangle \cong \mathbb{Z}/\langle 15\rangle$$

■

■ **Example 5.3** **Claim:** There are two isomorphism classes of groups of order 21
Let G be a group of order $21 = 3 \cdot 7$. Let n_p be the number of Sylow p-subgroup of G. By **Theorem 5.2.8**, we have $n_3 \mid 7$ and $n_3 \equiv 1 \pmod 3$. Then $n_3 = 1$ or 7. Also we have $n_7 \mid 3$ and $n_7 \equiv 1 \pmod 7$. Thus $n_7 = 1$, it follows that G has a unique Sylow 7-subgroup, say P_7. Note that $P_7 \lhd G$ and P_7 is cyclic, $P_7 = \langle x\rangle$ with $x^7 = 1$. Let H be a Sylow 3-subgroup, since $|H| = 3$, H is cyclic and $H = \langle y\rangle$ with $y^3 = 1$. Since $P_7 \lhd G$, we have $yxy^{-1} = x^i$ for $0 \le i \le 6$. It follows that

$$x = y^3xy^{-3} = y^2x^iy^{-2} = yx^{i^2}y^{-1} = x^{i^3}$$

Since $x^{i^3} = x$ and $x^7 = 1$, we have $i^3 - 1 \equiv 0 \pmod{p}$ Since $0 \leq i \leq 6$, we have $i = 1, 2, 4$
(1) If $i = 1$, then $yxy^{-1} = x$ i.e. $yx = xy$, then G is an abelian group and $G \cong \mathbb{Z}\langle 21\rangle$
(2) If $i = 2$, then $yxy^{-1} = x^2$, then $G = \left\{x^i y^j : 0 \leq i \leq 6,\ 0 \leq j \leq 2,\ yxy^{-1} = x^2\right\}$
(3) If $i = 4$, then $yxy^{-1} = x^4$. Note that

$$y^2xy^{-2} = yx^4y^{-1} = x^{16} = x^2$$

Note that y^2 is also a generator of H. Thus by replacing y by y^2, we get back to case (2). It follows that there are two isomorphism classes of groups of order 21. ∎

6. Solvable Group

Definition 6.0.1 — Solvable Group.
A group G is solvable if there exists a tower

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq G_3 ..... \supseteq G_m = \{1\}$$

with $G_{i+1} \lhd G_i$ and G_i/G_{i+1} abelian for all $0 \leq i \leq (m-1)$

■ **Remark 6.1** G_{i+1} is not necessarily a normal subgroup of G. However, if G_{i+1} is a normal subgroup of G, we get $G_{i+1} \lhd G_i$ for free. ■

■ **Example 6.1** Consider a symmetric group S_4. Let A_4 be the alternating subgroup of S_4 and $V \cong \mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle$ the Klein 4 group. Note that A_4 and V are normal subgroup of S_4. We have

$$S_4 \supseteq A_4 \supseteq V \supseteq \{1\}$$

Since $S_4/A_4 \cong \mathbb{Z}/\langle 2\rangle$ and $A_4/V \cong \mathbb{Z}\langle 3\rangle$, S_4 is solvable. ■

Before we consider properties of solvable groups, we recall the theorems from **Pmath 347**

Theorem (Second Isomorphism Theorem) If H and N are subgroup of G with $N \lhd G$, then $H/H \cap N \cong NH/N$. (If either H or N is normal subgroup of G, then $NH = HN$ and it's a subgroup of G)

Theorem (Third Isomorphism Theorem) If H and N are normal subgroup of a group G s.t. $N \subseteq H$, then H/N is a normal subgroup of G/N and $(G/N)/(H/N) \cong G/H$

Theorem 6.0.1
Let G be a solvable group

(1) If H is a subgroup of G, then H is solvable.
(2) Let N be a normal subgroup of G. Then the quotient group G/N is solvable.

Proof: Since G is a solvable group, there exists a tower

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq G_3 ..... \supseteq G_m = \{1\}$$

with $G_{i+1} \lhd G_i$ and G_i/G_{i+1} abelian for all $0 \leq i \leq (m-1)$

For (1): Define $H_i = H \cap G_i$, since $G_{i+1} \lhd G_i$, we have a tower

$$H = H_0 \supseteq H_1 \supseteq H_2 \supseteq H_3 ..... \supseteq H_m = \{1\}$$

with $H_{i+1} \lhd H_i$. Note that both H_i and G_{i+1} are subgroup of G_i and $H_{i+1} = H \cap G_{i+1} = H_i \cap G_{i+1}$. Applying the second isomorphism theorem to G_i, we have

$$H_i/H_{i+1} = H_i/(H_i \cap G_{i+1}) \cong H_i G_{i+1}/G_{i+1} \subseteq G_i/G_{i+1}$$

Since G_i/G_{i+1} is abelian, so is H_i/H_{i+1}, it follows that H is solvable.

For (2): Consider the towers:

$$G = G_0 N \supseteq G_1 N \supseteq G_2 N \supseteq G_3 N ..... \supseteq G_m N = N$$

and

$$G/N = G_0 N/N \supseteq G_1 N/N \supseteq G_2 N/N \supseteq G_3 N/N ..... \supseteq G_m N/N = \{1\}$$

Since $G_{i+1} \lhd G_i$ and $N \lhd G$, we have

$$G_{i+1}N \lhd G_i N \quad \textbf{which implies that} \quad G_{i+1}N/N \lhd G_i N/N$$

By third isomorphism theorem, we have

$$(G_i N/N)/(G_{i+1}N/N) \cong G_i N/G_{i+1}N$$

By the second isomorphism theorem, we have

$$G_i N/G_{i+1}N \cong G_i/(G_i \cap G_{i+1}N)$$

Consider the natural quotient map $G_i \to G_i/(G_i \cap G_{i+1}N)$ which is surjective. Since $G_{i+1} \subseteq (G_i \cap G_{i+1}N)$, it induces a surjective map $G_i/G_{i+1} \to G_i/(G_i \cap G_{i+1}N)$ (Universal Property of Groups: Let G, G' be groups and let $f : G \to G'$ be a group homomorphism. If $N \lhd G$ satisfies $N \subseteq \ker(f)$, then there exists a unique map $\overline{f} : G/N \to G'$ s.t. $f = \overline{f} \circ \pi$ where $\pi : G \to G/N$ is the natural quotient map.) Since G_i/G_{i+1} is abelian, so is $G_i/(G_i \cap G_{i+1}N$. Thus $(G_i N/N)/(G_{i+1}N/N)$ is abelian. It follows that G/N is solvable.

The following theorem goes in the opposite direction from **Theorem 6.0.1**

Theorem 6.0.2
Let N be a normal subfroup of group G. If both N and G/N are solvable, then G is solvable. In particular, a direct product of any finitely many solvable groups is solvable.

Proof: Since N is solvable, we have a tower

$$N = N_0 \supseteq N_1 \supseteq N_2 \supseteq N_3 ..... \supseteq N_m = \{1\}$$

with $N_{i+1} \lhd N_i$ and N_i/N_{i+1} abelian. For a subgroup $H \subseteq G$ with $N \subseteq H$, we denote by $\overline{H} = H/N$. Since G/N is solvable, we have a tower

$$G/N = \overline{G} = \overline{G_0} \supseteq \overline{G_1} \supseteq \overline{G_2} \supseteq \overline{G_3} ..... \supseteq \overline{G_r} = \{1\}$$

with $\overline{G}_{i+1} \lhd \overline{G}_i$ and $\overline{G}_i/\overline{G}_{i+1}$ abelian. Let $Sub_N(G)$ denote the subgroups of G which contains N. Consider the map

$$\sigma : Sub_N(G) \to Sub(G/N), \quad H \mapsto H/N$$

for all $i = 0, 1, 2, ..., r$. Define $G_i = \sigma^{-1}(\overline{G}_i)$. Since $N \lhd G$ and $\overline{G}_{i+1} \lhd \overline{G}_i$, we have

$$G_{i+1} \lhd G_i$$

Moreover, by third isomorphism theorem we have

$$G_i/G_{i+1} \cong \overline{G}_i/\overline{G}_{i+1}$$

It follows that we have the tower

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq G_3 ..... \supseteq G_r = N = N_0 \supseteq N_1 \supseteq N_2 \supseteq N_3 ..... \supseteq N_m = \{1\}$$

with $G_{i+1} \lhd G_i$, $N_{i+1} \lhd N_i$ and G_i/G_{i+1}, N_i/N_{i+1} are all abelian. Thus, G is solvable.

■ **Example 6.2** S_4 contains subgroup isomorphic to S_3 and S_2. Since S_4 is solvable, by **Theorem 6.0.1** S_3 and S_2 are solvable. ■

Definition 6.0.2 — Simple Group.
A group G is **simple** if it is not trivial and has no normal subgroups except $\{1\}$ and G.

■ **Example 6.3** One can show that the alternating group A_5 is simple. Since $A_5 \supseteq \{1\}$ is the only tower and $A_5/\{1\}$ is not ableian. A_5 is not solvable. Thus by **Theorem 6.0.1**, S_5 is also not solvable. Moreover, since for all S_n with $n \geq 5$, it contains a subgroup isomorphic to S_5 which is not solvable. By **Theorem 6.0.1** S_n are not solvable for $n \geq 5$. ■

Corollary 6.0.3
Let G be a finite solvable group. Then there exists a tower

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq G_3..... \supseteq G_m = \{1\}$$

with $G_{i+1} \lhd G_i$ and G_i/G_{i+1} a cyclic group.

Proof: If G is solvable, there exists a tower

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq G_3..... \supseteq G_m = \{1\}$$

with $G_{i+1} \lhd G_i$ and G_i/G_{i+1} abelian for $0 \leq i \leq (n-1)$. Consider $A = G_i/G_{i+1}$ a finite abelian group. We have

$$A \cong C_{k_1} \times C_{k_2} \times .... \times C_{k_r}$$

where C_k is a cyclic group of order k. Since each G_i/G_{i+1} can be rewritten as a product of cyclic groups, the result follows.

■ **Remark 6.2** In the above proof, given a finite cyclic group C, by **Chinese Remainder Theorem**, we have

$$C \cong \mathbb{Z}/\langle p_1^{a_1}\rangle \times \mathbb{Z}/\langle p_2^{a_2}\rangle \times ..... \times \mathbb{Z}/\langle p_r^{a_r}\rangle$$

where p_i are distinct primes. Alsom for a cyclic group whose order is prime powerm say $\mathbb{Z}/\langle p^a\rangle$, we have a tower of subgroups

$$\mathbb{Z}/\langle p^a\rangle \supseteq \mathbb{Z}/\langle p^{a-1}\rangle \supseteq \mathbb{Z}/\langle p^{a-2}\rangle .....\mathbb{Z}/\langle p\rangle \supseteq \{1\}$$

so we can further require the quotient G_i/G_{i+1} in the above corollary to the cyclic group of prime order. ■

7. Automorphism Groups

7.1 General Automorphism Groups

Definition 7.1.1 — F-automorphism.
Let E/F be a field extension, if ψ is an automorphism of E, i.e. $\psi : E \to E$ is an isomorphism and $\psi\,|_F = 1_F$, we say ψ is an **F-automorphism** of E. By maps composition, the set

$$\{\psi : E \to E \mid \psi \text{ is an F-automorphism}\}$$

is a group. We call it **automorphism group** of E/F and denote by $Aut_F(E)$

Lemma 7.1.1
Let E/F be field extensions, $f(x) \in F[x]$ and $\psi \in Aut_F(E)$. If $\alpha \in E$ a root of $f(x)$, then $\psi(\alpha)$ is also a root of $f(x)$.

Proof: We write $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n \in F[x]$, we have

$$\begin{aligned} f(\psi(\alpha)) &= a_0 + a_1\psi(\alpha) + a_2\psi(\alpha)^2 + ... + a_n\psi(\alpha)^n \\ &= \psi(a_0) + \psi(a_1)\psi(\alpha) + \psi(a_2)\psi(\alpha)^2 + ... + \psi(a_n)\psi(\alpha)^n \\ &= \psi(a_0 + a_1\alpha + a_2\alpha^2 + ... + a_n\alpha^n) \\ &= \psi(0) = 0 \qquad \textbf{since } \alpha \textbf{ is a root} \end{aligned}$$

Thus $\psi(\alpha)$ is a root of $f(x)$

Lemma 7.1.2
Let $E = F(\alpha_1, \alpha_2, ..., \alpha_n)$ be a field extension of F. For $\psi_1, \psi_2 \in Aut_F(E)$, if $\psi_1(\alpha_i) = \psi(\alpha_i)$ for all α_i $(1 \leq i \leq n)$, then $\psi_1 = \psi_2$

Proof: Note that for $\alpha \in E$, α is of the form

$$\frac{f(\alpha_1, \alpha_2, ..., \alpha_n)}{g(\alpha_1, \alpha_2, ..., \alpha_n)}$$

where $f(\alpha_1, \alpha_2, ..., \alpha_n), g(\alpha_1, \alpha_2, ..., \alpha_n) \in F[x_1, ..., x_n]$, then the lemma follows

Corollary 7.1.3
If E/F is a finite extension, then $Aut_F(E)$ is a finite group

Proof: Since E/F is a finite extension, by **Theorem 2.2.4** we have $E = F(\alpha_1, \alpha_2, ..., \alpha_n)$ where α_i $(1 \leq i \leq n)$ are algebraic over F. For $\psi \in Aut_F(E)$, by **Lemma 7.1.1** $\psi(\alpha_i)$ for $(1 \leq i \leq n)$ is a root of the minimal polynomial of α_i. Thus it has only finitely many choices. By **Lemma 7.1.2** since $\psi \in Aut_F(E)$ is completely determined by $\psi(\alpha_i)$, there are only finitely many choices for ψ. Thus $Aut_F(E)$ is finite.

■ **Remark 7.1** The converse if the above Corollary is **FALSE**. For example, $\mathbb{R}/\mathbb{Q}$ is an finite extension, but $Aut_{\mathbb{Q}}(\mathbb{R}) = 1$. Indeed, we will show in **Assignment 7** that $Aut(\mathbb{R}) = \{1\}$ as $\psi \in Aut(\mathbb{R})$ with $\psi(1) = 1$ will imply that $\psi \mid_{\mathbb{Q}} = 1_{\mathbb{Q}}$ ■

7.2 Automorphism Groups of Splitting Fields

Definition 7.2.1
Let F be a field and $f(x) \in F[x]$. The **automorphism group** of $f(x)$ **over** F is defined to be group $Aut_F(E)$ where E is the splitting field of $f(x)$ over F

We recall **Theorem 3.2.1**: Let $\phi : F \to F_1$ be an isomorphism of fields and $f(x) \in F[x]$. Let $\Phi : F[x] \to F_1[x]$ be the unique ring isomorphism which extends ϕ and maps x to x. Let $f_1(x) = \Phi(f(x))$ and E/F and E_1/F_1 be splitting fields of $f(x)$ and $f_1(x)$ respectively. Then there exists an isomorphism $\psi : E \to E_1$ which extends ϕ.

In Assignment 3, we prove that the number of such ψ's is $\leq [E : F]$ and equality holds if and only if $f(x)$ is separable over F. As a direct consequence of this result, we have

Theorem 7.2.1
Let E/F be the splitting field of a non-zero polynomial $f(x) = F[x]$, we have $|Aut_F(E)| \leq [E : F]$ and equality holds if and only if $f(x)$ is separable.

Theorem 7.2.2
If $f(x) \in F[x]$ has n distinct roots in the splitting field E, then $Aut_F(E)$ is isomorphic to a subgroup of the symmetric group S_n. In particular, $|Aut_F(E)|$ divides $n!$

Proof: Let $X = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ be distinct roots of $f(x)$ in E. By **Lemma 7.1.1** if $\psi \in Aut_F(E)$, then $\psi(X) = X$. Let $\psi\mid_X$ be the restriction of ψ in X and S_X the permutation group of X. The map

$$Aut_F(E) \to S_X \cong S_n, \quad \psi \mapsto \psi\mid_X$$

is a group homomorphism. Moreover, by **Lemma 7.1.2** it is injective. Thusm $Aut_F(E)$ is isomorphic to a subgroup of S_n

■ **Example 7.1** Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ and $E/\mathbb{Q}$ the splitting field of $f(x)$. Thus $E = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ and $[E : F] = 6$. Since $ch(\mathbb{Q}) = 0$, $f(x)$ is separable. By **Theorem 7.2.1**

$$|Aut_{\mathbb{Q}}(E)| = |E : F| = 6$$

Also, since $f(x)$ has 3 distinct roots in E, by **Theorem 7.2.2**, $Aut_{\mathbb{Q}}(E)$ is a subgroup of S_3. Since the only subgroup of S_3 which is of order 6 is S_3, we have

$$Aut_{\mathbb{Q}}(E) \cong S_3$$

■

■ **Example 7.2** Let F be a field with $ch(F) = p$, $F^p \neq F$ and $f(x) = x^p - a$ with $a \in F \setminus F^p$. Let E/F be the splitting field of $f(x)$. We have seen in **Section 4.4** that $f(x) = (x - \beta)^p$ for some $\beta \in E \setminus F$. Then $E = F(\beta)$. Since β can only map to β, $Aut_F(E)$ is trivial. Note that

$$|Aut_F(E)| = 1 \quad \textbf{while} \quad |E : F| = p$$

We have $|Aut_F(E)| \neq |E : F|$. Notice that $f(x)$ is not separable ■

7.3 Fixed Fields

Definition 7.3.1 — Fixed Field.
Let E/F be a field extension and $\psi \in Aut_F(E)$. Define

$$E^{\psi} = \{a \in E : \psi(a) = a\}$$

which is a subfield of E containing F. We call E^{ψ} be the **fixed field** of ψ.
If $G \subseteq Aut_F(E)$, the **fixed field** of G is defined by

$$E^G = \bigcap_{\psi \in G} E^{\psi} = \{a \in E : \psi(a) = a \ \textbf{ for all } \psi \in G\}$$

Theorem 7.3.1
Let $f(x) \in F[x]$ be a **separable polynomial** and E/F its splitting field. If $G = Aut_F(E)$, then $E^G = F$

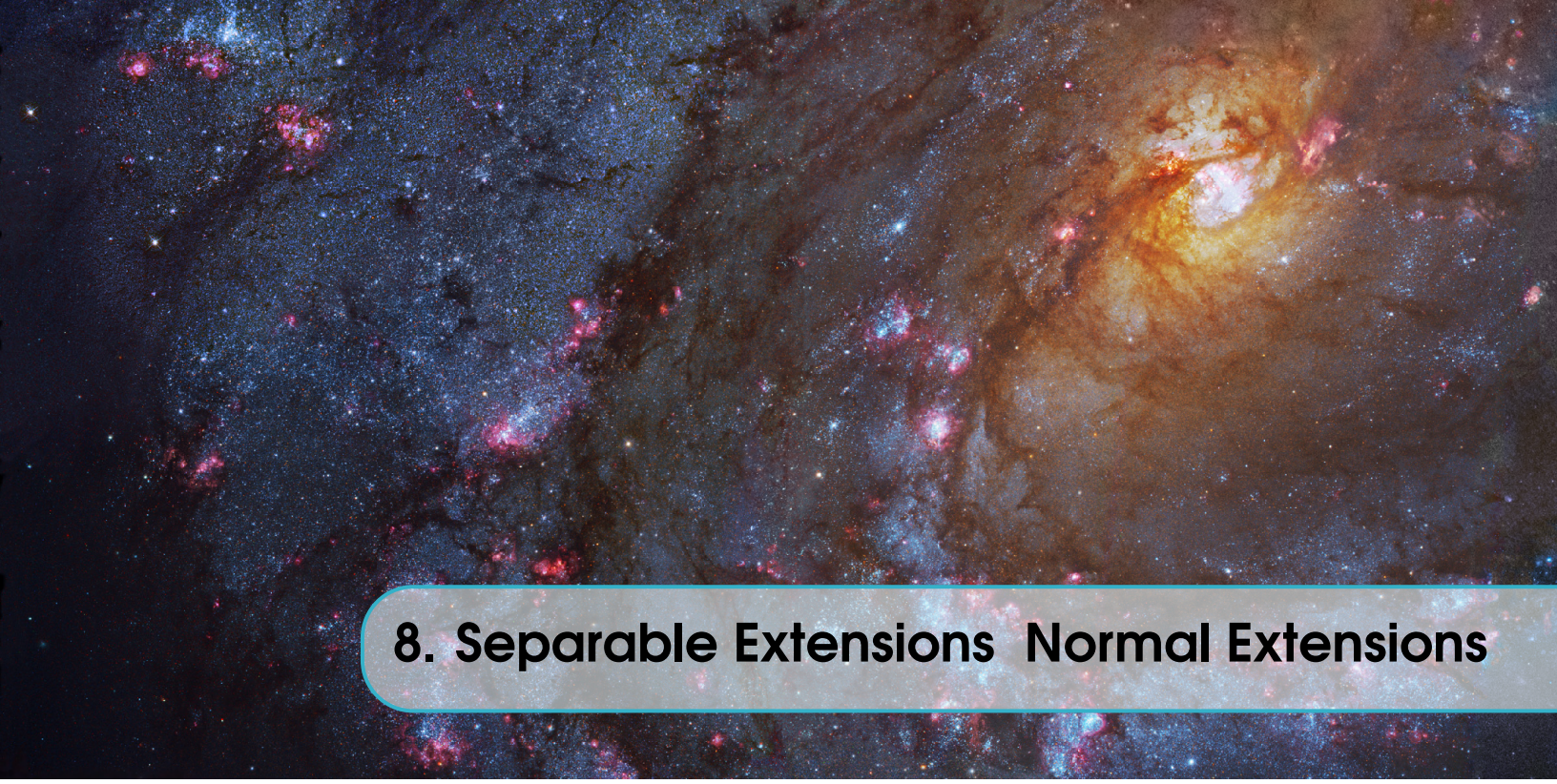
Proof: Set $S = E^G$. Since $F \subseteq L$, we have $Aut_L(E) \subseteq Aut_L(E)$. On the other hand, if $\psi \in Aut_F(E)$, by the definition of L, we have $\psi(a) = a$. This implies that $\psi \in Aut_L(E)$. Then

$$Aut_F(E) = Aut_L(E)$$

Note that since $f(x)$ is separable over F splits over E, $f(x)$ is also separable over L and has E as its splitting field over L. Then by **Theorem 7.2.1** we have

$$|Aut_F(E)| = |E : F| \quad \textbf{and} \quad |Aut_L(E)| = |E : L|$$

It follows that $[E : F] = [E : L]$, since $[E : F] = [E : L][L : F]$, we have $[L : F] = 1$. then $L = F$. i,e, $E^G = F$



8. Separable Extensions Normal Extensions

8.1 Separable Extensions

Definition 8.1.1 Let E/F be an algebraic field extension. For $\alpha \in E$, let $p(x) \in F[x]$ be the minimal polynomial of α. We say α is **separable** over F if $p(x)$ is separable. If for all $\alpha \in E$, α is separable, we say E/F is **separable**

■ **Example 8.1** If $ch(F) = 0$, by **Theorem 4.4.1**, F is perfect and every polynomial $f(x) \in F[x]$ is separable. Thus, if $ch(F) = 0$, any algebraic extension E/F is separable. ■

Theorem 8.1.1
Let E/F be the splitting field of $f(x) \in F[x]$. If $f(x)$ is separable, then E/F is separable.

Proof: Let $\alpha \in E$ and $p(x) \in F[x]$ be the minimal polynomial of α. Let $\{\alpha = \alpha_1, \alpha_2, ..., \alpha_n\}$ be all of the distinct roots of $p(x)$ in E. Define

$$\tilde{p}(x) = (x - \alpha_1)(x - \alpha_2).....(x - \alpha_n)$$

Claim: $\tilde{p}(x) \in F[x]$
Let $G = Aut_F(E)$ and $\psi \in G$. Since ψ is an automorphism, $\psi(\alpha_i) \neq \psi(\alpha_j)$ for $i \neq j$. By **Lemma 7.1.1**, ψ permutes $\alpha_1, \alpha_2, ..., \alpha_n$. Thus by extending $\psi : E \to E$ to $\psi : E[x] \to E[x]$, we have

$$\psi(\tilde{p}(x)) = (x - \psi(\alpha_1))(x - \psi(\alpha_2)).....(x - \psi(\alpha_n)) = (x - \alpha_1)(x - \alpha_2).....(x - \alpha_n)$$

It follows that $\tilde{p}(x) \in E^{\psi}[x]$. Since $\psi \in G$ is arbitrary, $\tilde{p}(x) \in E^G[x]$. Since E/F is the splitting field of the separable polynomial $f(x)$, by **Theorem 7.3.1** $\tilde{p}(x) \in E^G[x]$. Then the Claim holds. Then we have $\tilde{p}(x) \in F[x]$ with $\tilde{p}(\alpha) = 0$. Since $p(x)$ is the minimal polynomial of α over F, we

have $p(x) \mid \tilde{p}(x)$. Also, since $\alpha_1, \alpha_2, ..., \alpha_n$ are all distinct roots of $p(x)$, we have $p(x) \mid \tilde{p}(x)$. Since both $p(x)$ and $\tilde{p}(x)$ are monic, we have $\tilde{p}(x) = p(x)$. It follows that $p(x)$ is separable.

Corollary 8.1.2
Let E/F be a finite extension and $E = F(\alpha_1, \alpha_2, ..., \alpha_n)$. If each α_i is separable over F for $(1 \leq i \leq n)$, then E/F is separable

Proof: Let $p_i(x) \in F[x]$ be the minimal polynomial of α_i for $(1 \leq i \leq n)$. Let $f(x) = p_1(x)p_2(x)....p_n(x)$. Since each $p_i(x)$ is separable, so is $f(x)$. Let L be the splitting field of $f(x)$ over F. By **Theorem 8. 1.1**, L/F is separable, Since $E = F(\alpha_1, \alpha_2, ..., \alpha_n)$ is subfield of L, E is also separable.

Corollary 8.1.3
Let E/F be an algebraic extension and L the set of all $\alpha \in E$ which are separable over F. Then L is an intermediate field.

Proof: Let $\alpha, \beta \in F$, then $\alpha \pm \beta$, $\alpha\beta$ and α/β $(\beta \neq 0) \in F(\alpha, \beta)$. By **Corollary 8.1.2**, $F(\alpha, \beta)$ is separable and hence it is contained in L. Then $\alpha \pm \beta$, $\alpha\beta$ and α/β $(\beta \neq 0) \in L$

We have seen in **Theorem 2.2.4** that finite extension is a composition of simple extensions

Definition 8.1.2 — Primitive Element.
If $E = F(\gamma)$ is a simple extension, we say γ is a **primitive element** of E/F

Theorem 8.1.4 — Primitive Element Theorem.
If E/F is a finite separable extension, then $E = F(\gamma)$ for some $\gamma \in E$. In particular, if $ch(F) = 0$, then any finite extension E/F is a simple extension.

Proof: We have seen in **Corollary 4.3.3** that a finite extension of a finite field is always simple. Then **WLOG**, we assume that F is an infinite field. Since $E = F(\alpha_1, \alpha_2, ..., \alpha_n)$ for some $\alpha_1, \alpha_2, ..., \alpha_n \in E$, if suffices to consider the case when $E = F(\alpha, \beta)$ and the general case can be done by induction. Let $E = F(\alpha, \beta)$ with $\alpha, \beta \notin F$.
Claim: There exists $\lambda \in F$ such that $\gamma = \alpha + \gamma\beta$ and $\beta \in F(\gamma)$
If the claim holds, then $\alpha = \gamma - \lambda\beta \in F(\gamma)$ and we have $F(\alpha, \beta) \subseteq F(\gamma)$. Also, since $\gamma = \alpha + \lambda\beta$, $F(\gamma) \subseteq F(\alpha, \beta)$. Then $E = F(\alpha, \beta) = F(\gamma)$.
Proof of the Claim: Let $a(x)$ and $b(x)$ be the minimal polynomial of α and β over F respectively. Since $\beta \notin F$, $\deg(b) > 1$, then there exists a root $\tilde{\beta}$ of $b(x)$ such that $\tilde{\beta} \neq \beta$. Choose $\lambda \in F$ such that

$$\lambda \neq \frac{\tilde{\alpha} - \alpha}{\beta - \tilde{\beta}}$$

for all roots $\tilde{\alpha}$ of $a(x)$ and all roots $\tilde{\beta}$ of $b(x)$ with $\tilde{\beta} \neq \beta$ in some splitting field of $a(x)b(x)$ over F. The choice is possible since there are infinite many elements in F, by only finitely many choices of

$\tilde{\alpha}$ and $\tilde{\beta}$, Let $\gamma = \alpha + \lambda\beta$. Consider

$$h(x) = a(\gamma - \lambda x) \in F(\gamma)[x]$$

then

$$h(\beta) = a(\gamma - \lambda\beta) = a(\alpha) = 0$$

However, for any $\tilde{\beta} \neq \beta$, since

$$\gamma - \lambda\tilde{\beta} = a + \lambda(\beta - \tilde{\beta}) \neq \tilde{\alpha} \qquad \textbf{by the choices of } \lambda$$

We have

$$h(\tilde{\beta}) = a(\gamma - \lambda\tilde{\beta}) \neq 0$$

Then, $h(x)$ and $b(x)$ have β as a common root, but no other common root in any extension of $F(\gamma)$. Let $b_1(x)$ be the minimal polynomial of β over $F(\gamma)$, then $b_1(x)$ divides both $h(x)$ and $b(x)$. Since E/F is separable and $b(x) \in F[x]$ is irreducible, $b(x)$ has distinct roots, so does $b_1(x)$. The roots of $b_1(x)$ are also common to $h(x)$ and $b(x)$. Since $h(x)$ and $b(x)$ has only β as a common root, $b_1 = x - \beta$. Since $b_1(x) \in F(\gamma)[x]$, we obtain $\beta \in F(\gamma)$ as required.

8.2 Normal Extensions

Definition 8.2.1 Normal Extension
Let E/F be an algebraic extension. We say E/F is a **normal extension** if for any irreducible polynomial $p(x) \in F[x]$, either $p(x)$ has no root in E or $p(x)$ has all roots in E. In other words, if $p(x)$ has a root in E, $p(x)$ splits over E

■ **Example 8.2** Let $\alpha \in R$ satisfy $\alpha^4 = 5$. Since the roots of $x^4 - 5$ are $\pm\alpha, \pm\alpha i$ and $\mathbb{Q}(\alpha)$ is real, $\mathbb{Q}(\alpha)/\mathbb{Q}$ is normal, let $\beta = (1 + i)\alpha$
Claim: $\mathbb{Q}(\beta)/\mathbb{Q}$ is also not normal
Note that

$$\beta^2 = 2i\alpha^2 \qquad \beta^4 = -4\alpha^4 = -20$$

Since $\pm\beta, \pm i\beta$ all satisfy $x^4 = -20$, to show $\mathbb{Q}(\beta)$ is not normal, it suffices to show $i \notin \mathbb{Q}(\beta)$. Since the minimal polynomial of β over $\mathbb{Q}$ is $p(x) = x^4 + 20$, we have $[\mathbb{Q}(\beta) : \mathbb{Q}] = 4$. Also, the roots of $p(x)$ are $\pm\beta$ and $\pm i\beta$. Since the minimal polynomial of α is $x^4 - 5$, we have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Note that if $\alpha \in \mathbb{Q}(\beta)$, since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 = [\mathbb{Q}(\beta) : \mathbb{Q}]$, it implies that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$, which is impossible since $\beta = \alpha + i\alpha \notin \mathbb{Q}(\alpha)$. Then, $\alpha \notin \mathbb{Q}(\beta)$ and it implies that $i \notin \mathbb{Q}(\beta)$ (if $i \in \mathbb{Q}(\beta)$, then $a = \beta/(1 + i) \in \mathbb{Q}(\beta)$, a contradiction.) It follows that the factorization of $p(x)$ over $\mathbb{Q}(\beta)$ is

$$(x - \beta)(x + \beta)(x^2 + \beta^2)$$

Since $p(x)$ does not split over $\mathbb{Q}(\beta)$, $\mathbb{Q}(\beta)/\mathbb{Q}$ is not normal. ■

Theorem 8.2.1
A finite extension E/F is normal if and only if it is the splitting field of some $f(x) \in F[x]$

Proof: $\Longrightarrow$ Suppose that E/F is normal, write $E = F(\alpha_1, \alpha_2, ..., \alpha_n)$. Let $p_i(x) \in F[x]$ be the minimal polynomial of α_i for $1 \leq i \leq n$. We now define

$$f(x) = p_1(x)p_2(x)....p_n(x)$$

Since E/F is normal, each $p_i(x)$ splits over E. Let $\alpha_i = \alpha_{i,1}, \alpha_{i,2}, ..., \alpha_{i,r_i}$ for $1 \leq i \leq n$ be the roots of $p_i(x)$ in E. Then

$$\begin{aligned} E &= F(\alpha_1, \alpha_2, ..., \alpha_n) \\ &= F(\alpha_{1,1}\alpha_{1,2}, ..., \alpha_{1,r_1}, \alpha_{2,1}, \alpha_{2,2}, ..., \alpha_{n,1}, ..., \alpha_{n,r_n}) \end{aligned}$$

which is the splitting field of $f(x)$ over F

$\Longleftarrow$: Let E/F be the splitting field of $f(x) \in F[x]$. Let $p(x) \in F[x]$ be irreducible and has a root $\alpha \in E$. Let K/E be the splitting field of $p(x)$ over E. We write

$$p(x) = c(x - \alpha_1)(x - \alpha_2)...(x - \alpha_n)$$

where $0 \neq c \in F$. $\alpha = \alpha_1 \in E$, $\alpha_2, \alpha_3, ..., \alpha_n \in K = E(\alpha_1, \alpha_2, ..., \alpha_n)$. Since

$$F(\alpha) \cong F[x]/\langle p(x)\rangle \cong F(\alpha_2)$$

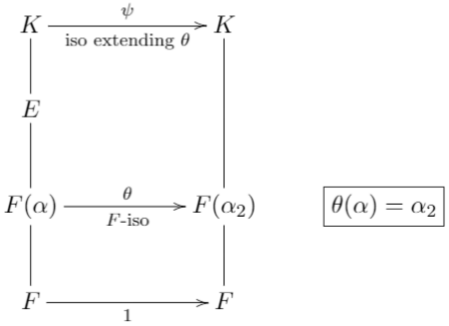
WE have the F-isomorphism

$$\theta : F(\alpha) \to F(\alpha_2) \quad \theta(a\langle) = \alpha_2$$

Note that $p(x) \in F[x] \subseteq F(\alpha)[x]$ and $p(x) \in F(\alpha_2)[x]$. Then we can view K as the splitting field of $p(x)$ over $F(\alpha)$ and $F(\alpha_2)$ respectively. Then, by **Theorem 3.2.1**, there exists an isomorphism

$$\psi : K \to K$$

which extends θ. In particular, $\psi \in Aut_F(K)$. **(see the picture below)**
Since $\psi \in Aut_F(K)$, ψ permutes the roots of $f(x)$. Since E is generated over F by the roots of $f(x)$. By **Lemma 7.1.1**, we have $\psi(E) = E$. It follows that for $\alpha \in E$, $\alpha_2 = \psi(\alpha) \in E$. Similarly, we can prove that $\alpha_i \in E$ for $3 \leq i \leq n$. Then $K = E$ and $p(x)$ splits over E. It follows that E/F is normal.



■ **Example 8.3** Claim: Every quadratic extension is normal.
Let E/F be a field extension with $[E:F]=2$. For $\alpha \in E/F$, we have $E=F(\alpha)$. Let $p(x)=x^2+ax+b$ be the minimal polynomial of α over F. If β is another root of $p(x)$, then

$$p(x)=(x-\alpha)(x-\beta)=x^2+(\alpha+\beta)x+\alpha\beta$$

Then $\beta=-a-\alpha$ ($\beta=b/a$) *too* is the other root of $p(x)$ and $\beta \in E$. Hence, E/F is normal. ■

■ **Example 8.4** The extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal since the irreducible polynomial $p(x)=x^4-2$ has a root in $\mathbb{Q}(\sqrt[4]{2})$ but $p(x)$ does not split over $\mathbb{Q}(\sqrt[4]{2})$. Note that the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is made up of two quadratic extensions. $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, which are normal. Then, if E/K and K/F are normal extensions, the extension E/F is not always normal. ■

Proposition 8.2.2
If E/F is a normal extension and K an intermediate field, then E/F is normal

Proof: Let $p(x) \in K[x]$ be irreducible and has a root $\alpha \in E$. Let $f(x) \in F[x] \subseteq K[x]$ be the minimal polynomial of α over F. Then $p(x) \mid f(x)$. Since E/F is normal, $f(x)$ splits over E, so does $p(x)$. Then E/K is normal extension.

■ **Remark 8.1** In **Proposition 8.2.2**, K/F is not always normal. For example, let $F=\mathbb{Q}$, $K=\mathbb{Q}(\sqrt[4]{2})$ and $E=\mathbb{Q}(\sqrt[4]{2},i)$. Then E/F is the splitting field of x^4-2 and hence normal. Also, E/K is normal but K/F is not normal. ■

Proposition 8.2.3
Let E/F be a finite normal extension and $\alpha, \beta \in E$. The following conditions are equivalent:

(1) There exists $\psi \in Aut_F(E)$ such that $\psi(\alpha)=\beta$.
(2) The minimal polynomials of α and β over F are the same.
In this case, we say that α and β are **conjugate over** F

Proof:
(1) $\Longrightarrow$ (2): Let $p(x)$ be the minimal polynomial of α over F and $\psi \in Aut_F(E)$ with $\psi(\alpha)=\beta$. By **Lemma 7.1.1** β is also a root of $p(x)$. Since $p(x)$ is monic and irreducible, it is the minimal polynomial of β over F. Hence, α and β have the same minimal polynomials
(2) $\Longrightarrow$ (1): Suppose that the minimal polynomials of α and β are the same, we say $p(x)$. Since

$$F(\alpha) \cong F[x]/\langle p(x)\rangle \cong F(\beta)$$

we have the F-isomorphism $\theta : F(\alpha) \to F(\beta)$ with $\theta(\alpha)=\beta$. Since E/F is a finite normal extension, by **Theorem 8.2.1**, E is the splitting field of some $f(x) \in F[x]$ over F. We can also view E as the splitting field of $f(x)$ over $F(\alpha)$ and $F(\beta)$ respectively. Then, by **Theorem 3.2.1**, there exists an isomorphism $\psi : E \to E$ which extends θ. It follows that $\psi \in Aut_F(E)$ and $\psi(\alpha)=\beta$.

■ **Example 8.5** The complex numbers $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta_3$ and $\sqrt[3]{2}\zeta_3^2$ are all conjugate over $\mathbb{Q}$ since they are roots of the irreducible polynomial $x^3 - 2 \in \mathbb{Q}[x]$. ■

We have seen some nice properties about normal extensions. Since not all finite extensions are normal. It's attempting to construct normal extensions related to them. Note taht we want to do it in the "minimal way" so that the associated group $Aut_F(E)$ is as small as possible.

Definition 8.2.2 — Normal Closure.
A **normal closure** of a finite extension E/F is a finite normal extension N/F satisfying the following properties:
(1) E is a subfield of N
(2) Let L be an intermediate field of N/E. If L is normal over F, then $L = N$

■ **Example 8.6** The normal closure of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$ ■

Theorem 8.2.4
Every finite extension E/F has a normal closure N/F which is unique up to E-isomorphism

Proof: We write $E = F(\alpha_1, \alpha_2, ..., \alpha_n)$

(Existence): Let $p_i(x)$ be the minimal polynomial of α_i over F for $1 \leq i \leq n$. We write $f(x) = p_1(x)p_2(x)...p_n(x)$ and let N/E be the splitting field of $f(x)$ over E. Since $\alpha_1, \alpha_2, ..., \alpha_n$ are roots of $f(x)$, N is also the splitting field of $f(x)$ over F. By **Theorem 8.2.1**, N is normal over F. Let $L \subseteq N$ be a subfield containing E. Then L contains all α_i. If L is normal over F, each $p_i(x)$ splits over L. Then, $N \subseteq L$, it follows that $L = N$

(Uniqueness): Let N/E be the splitting field of $f(x)$ over E defined as above. Let N_1/F be another normal closure of E/F. Since N_1 is normal over F and contains all α_i, N_1 must contains a splitting field $\tilde{N}$ of $f(x)$ over F, then over E. By **Corollary 3.2.2**, N and $\tilde{N}$ are E-isomorphic. Since $\tilde{N}$ is a splitting field of $f(x)$ over F, by **Theorem 8.2.1**, $\tilde{N}$ is normal over F. Therefore, by definition of a normal closure, $N_1 = \tilde{N}$. It follows that N and N_1 are E-isomorphic.

9. Galois Correspondence

9.1 Galois Extensions

Definition 9.1.1 — Galois Extension.
An algebraic extension E/F is Galois if it is normal and separable. If E/F is a Galois extension, the **Galois group** of E/F, $Gal_F(E)$ is defined to be the automorphism group $Aut_F(E)$.

Definition 9.1.2 A Galois extension E/F is called **abelian**, **cyclic** or **solvable** if $Gal_F(E)$ has the corresponding properties.

■ **Remark 9.1**
(1) By **Theorem 8.1.1** and **Theorem 8.2.1**, a finite Galois extension E/F is equivalent to the splitting field of a separable polynomial $f(x) \in F[x]$
(2) If E/F is a finite Galois extension, by **Theorem 7.2.1**

$$[Gal_F(E)] = [E : F]$$

(3) If E/F is the splitting field of a separable polynomial $f(x) \in F[x]$ with $\deg(f) = n$, then by **Theorem 7.2.2**, $Gal_F(E)$ is a subgroup of S_n ■

■ **Example 9.1** Let E be the splitting field of $(x^2-2)(x^2-3)(x^2-5) \in \mathbb{Q}[x]$. Then $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ and $[E : \mathbb{Q}] = 8$. For $\psi \in Gal_{\mathbb{Q}}(E)$ we have

$$\psi(\sqrt{2}) \in \left\{\pm\sqrt{2}\right\} \quad \psi(\sqrt{3}) \in \left\{\pm\sqrt{3}\right\} \quad \psi(\sqrt{5}) \in \left\{\pm\sqrt{5}\right\}$$

Since

$$[Gal_{\mathbb{Q}}(E)] = [E : \mathbb{Q}] = 8$$

we have

$$Gal_{\mathbb{Q}}(E) \cong \mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle$$

■

Definition 9.1.3

Let $t_1, t_2, ..., t_n$ be variables. We define the **elementary symmetric functions** in $t_1, t_2, ..., t_n$ as

$$s_1 \coloneqq t_1 + t_2 + ... + t_n \qquad s_2 \coloneqq \sum_{1\le i\le j\le n} t_i t_j \qquad .... \qquad s_n \coloneqq t_1 t_2 .... t_n$$

Then it follows that

$$f(x) = (x - t_1)(x - t_2)....(x - t_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - .... + (-1)^n s_n$$

Theorem 9.1.1 — E.Artin.

Let E be a field and G be a finite subgroup of $Aut(E)$, the automorphism group of E. Let $E^G = \{\alpha \in E : \ \psi(\alpha) = \alpha \ \ \forall \psi \in G\}$. Then E/E^G is a finite Galois extension and $Gal_{E^G}(E) = G$. In particular, we have

$$[E : E^G] = |G|$$

Proof: Let $n = |G|$ and $F = E^G$. For $\alpha \in E$, consider G-orbit of α. i.e.

$$\{\psi(\alpha) \mid \ \psi \in G\} = \{\alpha = \alpha_1, \alpha_2, ..., \alpha_m\} \quad \textbf{where } \alpha_i \textbf{ are distinct}$$

For any $\psi \in G$, ψ permutes the roots $\{\alpha_1, \alpha_2, ..., \alpha_m\}$. Since the coefficient of $f(x)$ are symmetric with respect to α_i $(1 \le i \le m)$, they are fixed by all $\psi \in G$. Then

$$f(x) \in E^G[x] = F[x]$$

To show $f(x)$ is actually the minimal polynomial of α, consider a factor $g(x) \in F[x]$ of $f(x)$. **WLOG** we can write

$$g(x) = (x - \alpha_1)(x - \alpha_2)....(x - \alpha_l)$$

If $l \ne m$. Since α_i $(1 \le i \le m)$ are in the G-orbit of α, there exists $\psi \in G$ such that

$$\{\alpha_1, \alpha_2, ..., \alpha_l\} \ne \{\psi(\alpha_1), \psi(\alpha_2), ..., \psi(\alpha_l)\}$$

It follows that

$$\psi(g(x)) = (x - \psi(\alpha_1))(x - \psi(\alpha_2)).....(x - \psi(\alpha_n))$$

Then, if $l \ne m$, $g(x) \notin F[x]$. It follows that $f(x)$ is the minimal polynomial of α over F. Since $f(x) \in F[x]$ is separable and splits over E, E/F is a Galois extension.

Claim: $[E : F] \le n$

If $[E : F] > n = |G|$, we can choose $\beta_1, \beta_2, ..., \beta_{n+1} \in E$ which are linearly independent over F. Consider the system

$$\psi(\beta_1)v_1 + ... + \psi(\beta_{n+1})v_{n+1} = 0 \qquad \textbf{for all } \psi \in G$$

of n linear equations in $(n+1)$ variables $v_1, v_2, ...v_{n+1}$. Then, it has a non-zero solution in E. Let $(\gamma_1, \gamma_2, ..., \gamma_{n+1})$ be such a solution which has the minimal number of non-zero coordinates, we say r. Clearly, $r > 1$. **WLOG** we assume

$$\gamma_1, ..., \gamma_r \neq 0 \quad \textbf{and} \quad \gamma_{r+1}, ..., \gamma_{n+1} = 0$$

Then we have

$$\psi(\beta_1)\gamma_1 + ... + \psi(\beta_r)\gamma_r = 0 \quad \textbf{for all } \psi \in G$$

By dividing the solution by γ_r, we can assume that $\gamma_r = 1$. Also, since $(\beta_1, \beta_2, ..., \beta_r)$ are independent over F and $\beta_1\gamma_1 + ... + \beta_r\gamma_r = 0$ (take $\psi = id$), there exists at least one $\gamma_i \notin F$ (if $\gamma_1, \gamma_2, ..., \gamma_r \in F$, then $\beta_1\gamma_1 + ... + \beta_r\gamma_r = 0$ implies that $\gamma_1 = \gamma_2 = ... = \gamma_r = 0$ a contradiction). Since $r \geq 2$, **WLOG** we can assume that $\gamma_1 \notin F$. Choose $\phi \in G$ such that $\phi(\gamma_1) \neq \gamma_1$. Applying ϕ into (1) we get

$$(\phi \circ \psi)(\beta_1)\phi(\gamma_1) + ... + (\phi \circ \psi)(\beta_r)\phi(\gamma_r) = 0 \quad \textbf{for all } \psi \in G$$

Since ψ runs through all elements of G, so does $\phi \circ \psi$. Then we can write above equation as

$$\psi(\beta_1)\phi(\gamma_1) + ... + \psi(\beta_r)\phi(\gamma_r) = 0 \quad \textbf{for all } \psi \in G$$

By subtracting (2) from (1) we get

$$\psi(\beta_1)(\gamma_1 - \phi(\gamma_1)) + ... + \psi(\beta_r)(\gamma_r - \phi(\gamma_r)) = 0 \quad \textbf{for all } \psi \in G$$

Since $\gamma_r = 1$, we have $\gamma_r - \phi(\gamma_r) = 0$. Also Since $\gamma_1 \notin F$, we have $\gamma_1 - \phi(\gamma_1) \neq 0$. Then $(\gamma_1 - \phi(\gamma_1), \gamma_2 - \phi(\gamma_2), , ...\gamma_r - \phi(\gamma_r) = 0, 0, ..., 0)$ is a non-zero solution of the system This contradicts the choices of $(\gamma_1, \gamma_2, ..., \gamma_{n+1})$ having the minimal number of non-zero coordinates, so $[E : F] \leq n$. We have proved that the E/F is a finite Galois-extension. Then E is the splitting field of some separable polynomial over F. Also, since

$$F = E^G = \{\alpha \in E : \ \psi(\alpha) = \alpha \ \textbf{ for all } \psi \in G\}$$

G is a subgroup of $Gal_F(E)$. By **Theorem 7.2.1**, we have

$$n = |G| \leq |Gal_F(E)| = [E : F] \leq n$$

It follows that

$$[E : F] = n \quad \textbf{and} \quad Gal_F(E) = G$$

This completes the proof.

■ **Remark 9.2** Let E be a field and G a finite subgroup of $Aut(E)$. For $\alpha \in E$, we let

$$\{\alpha_1 = \alpha, \alpha_2, ..., \alpha_m\}$$

be the G-orbit of α. i.e. the set of all conjugates of α.. Then we can see from the proof **Theorem 9.1.1** that the minimal polynomial of α over E^G is

$$(x - \alpha_1)(x - \alpha_2).....(x - \alpha_m) \in E^G[x]$$

■ ■

■ **Example 9.2** omit ■

9.2 The Fundamental Theorem

Theorem 9.2.1 — Fundamental Theorem of Galois Theory.
Let E/F be a finite Galois extension and $G = Gal_F(E)$. There is an order reversing bijection between the intermediate fields of E/F and the subgroup of G. More precisely, let $Int(E/F)$ denote the intermediate fields of E/F and $Sub(G)$ the set of subgroups of G. Then, the maps

$$Int(E/F) \to Sub(G), \quad L \mapsto L^* \coloneqq Gal_L(E)$$

and

$$Sub(G) \to Int(E/F), \quad H \mapsto H^* \coloneqq E^H$$

are inverse of each other and reverse inclusion relation. In particular, for $L_1, L_2 \in Int(E/F)$ with $L_2 \subseteq L_1$, $H_1, H_2 \in Sub(G)$ with $H_2 \subseteq H_1$, we have

$$[L_1 : L_2] = [L_1^* : L_2^*] \qquad \textbf{and} \qquad [H_1 : H_2] = [H_1^* : H_2^*]$$

Proof: Let $L \in Int(E/F)$ and $H \in Sub(G)$. We recall **Theorem 7.3.1** which states that if $G_1 = Gal_{F_1}(E_1)$, then $E_1^{G_1} = F_1$, so we have

$$(L^*)^* = (Gal_L(E))^* = E^{Gal_L(E)} = L$$

Also by **Theorem 9.1.1** states that if $G_1 \subseteq Aut(E_1)$ then $Gal_{E_1^{G_1}}(E_1) = G_1$. Then we have

$$(H^*)^* = (E^H)^* = Gal_{E^H} = H$$

Then we have

$$H \mapsto H^* \mapsto H^{**} = H \qquad \textbf{and} \qquad L \mapsto L^* \mapsto L :^{**}= L$$

In particular, the maps $L \mapsto L^*$ and $H \mapsto H^*$ are inverse of each other. Let $L_1, L_2 \in Int(E/F)$. Since E/F is the splitting field of some separable polynomial $f(x) \in F[x]$, E/L_1 and E/L_2 are also Galois extensions since E is the splitting field of $f(x)$ over L_1 and L_2 respectively. We have

$$L_2 \subseteq L_1 \implies Gal_{L_1}(E) \subseteq Gal_{L_2}(E) \;\; i.e. \;\; L_1^* \subseteq L_2^*$$

Also

$$[L_1 : L_2] = \frac{[E : L_2]}{[E : L_1]} = \frac{[Gal_{L_2}(E)]}{|Gal_{L_1}(E)|} = \frac{|L_2^*|}{|L_1^*|} = [L_2^* : L_1^*]$$

For $H_1, H_2 \in Sub(G)$ we have

$$H_2 \subseteq H_1 \implies E^{H_1} \subseteq E^{H_2} \;\; i.e. \;\; H_1^* \subseteq H_2^*$$

Also

$$[H_1 : H_2] = \frac{|H_1|}{|H_2|} = \frac{[Gal_{E^{H_1}}(E)]}{Gal_{E^{H_2}}(E)} = \frac{[E : E^{H_1}]}{[E : E^{H_2}]} = [E^{H_2} : E^{H_1}] = [H_2^* : H_1^*]$$

which completes the proof.

■ **Remark 9.3** omit ■

Proposition 9.2.2

Let E/F be a finite Galois extension with $G = Gal_F(E)$. Let L be an intermediate field. For $\psi \in G$ we have

$$Gal_{\psi(L)}(E) = \psi Gal_L(E)\psi^{-1}$$

Proof: For any $\alpha \in \psi(L)$, $\psi^{-1}(\alpha) \in L$. If $\psi \in Gal_L(E)$, we have

$$\phi\psi^{-1}(\alpha) = \psi^{-1}(\alpha), \quad thus \quad \psi\phi\psi^{-1}(\alpha) = \alpha$$

It follows that

$$\psi\phi\psi^{-1} \in Gal_{\psi(L)}(E) \quad \textbf{for all } \phi \in Gal_L(E)$$

so

$$\psi Gal_L(E)\psi^{-1} \subseteq Gal_{\psi(L)}(E)$$

Since

$$\left|\psi Gal_L(E)\psi^{-1}\right| = |Gal_L(E)| = |E : L| = |E : \psi(L)| = \left|Gal_{\psi(L)}(E)\right|$$

The third equality above can be seen by considering the basis of E over L. It follows that

$$Gal_{\psi(L)}(E) = \psi Gal_L(E)\psi^{-1}$$

which completes the proof.

The following theorem gives a criterion about when L/F is a Galois extension

Theorem 9.2.3

Let E/F, L, L^* be defined as **Theorem 9.2.1**. Then L/F is a Galois extension if and only if L^* is a normal subgroup of G. In this case

$$Gal_F(L) \cong G/L^*$$

Proof: Note that

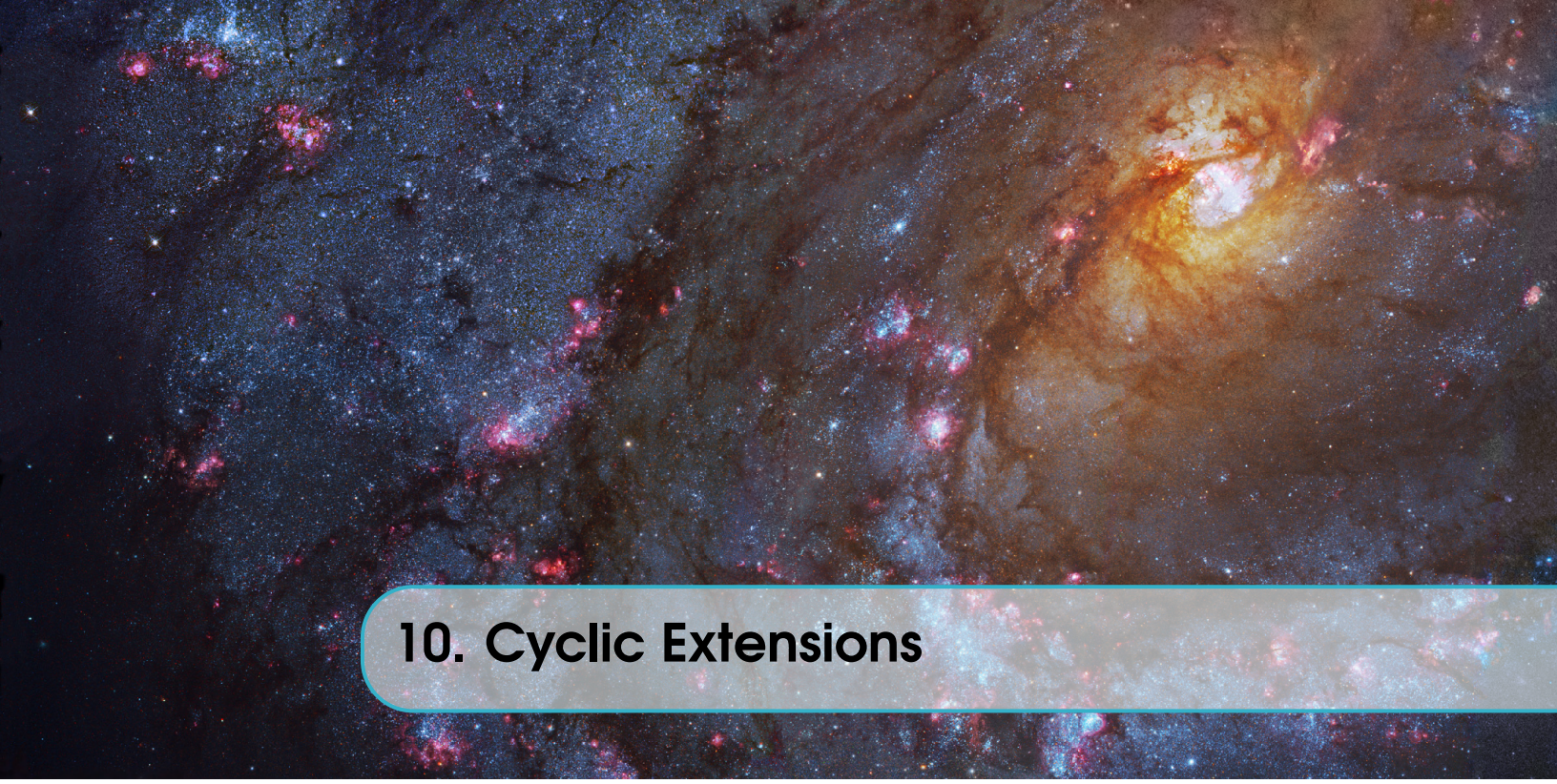
$$\begin{aligned}
L/F \textbf{ is normal} &\iff \psi(L) = L \quad \textbf{for all } \psi \in Gal_F(E) \\
&\iff Gal_{\psi(L)}(E) = Gal_L(E) \quad \textbf{for all } \psi \in Gal_F(E) \\
&\iff \psi Gal_L(E)\psi^{-1} = Gal_L(E) \quad \textbf{for all } \psi \in Gal_F(E) \quad \textbf{by Prop 9.2.2} \\
&\iff L^* = Gal_L(E) \quad \textbf{is a normal subgroup of } G
\end{aligned}$$

If L/F is a Galois extension, the restriction map

$$G = Gal_F(E) \longrightarrow Gal_F(L) \qquad \psi \mapsto \psi \mid_L$$

is well defined. Moreover, it is surjective and its kernel is $GalL(E) = L^*$, then

$$Gal_F(L) \cong G/L^*$$



10. Cyclic Extensions

We recall that if E/F is a Galois extension, we say E/F is cyclic if $Gal_F(E)$ is cyclic.

Lemma 10.0.1 — Dedekind's Lemma.
Let K and L be fields and let $\psi_i : L \to K$ be distinct non-zero homomorphisms $(1 \leq i \leq n)$. If $c_i \in K$ and

$$c_1\psi_1(\alpha) + c_2\psi_2(\alpha) + ...c_n\psi_n(\alpha) = 0 \quad \forall \alpha \in L$$

then $c_1 = c_2..... = c_n = 0$

Proof: Suppose the statement is false, i.e. there exists some $c_1, c_2, ..., c_n \in K$, not all 0, such that

$$c_1\psi_1(\alpha) + c_2\psi_2(\alpha) + ...c_n\psi_n(\alpha) = 0 \quad \forall \alpha \in L$$

Let $m \geq 2$ be minimal positive integer such that

$$c_1\psi_1(\alpha) + c_2\psi_2(\alpha) + ...c_m\psi_m(\alpha) = 0 \quad \forall \alpha \in L \qquad (*)$$

Since m is minimal, we have $c_i \neq 0$ $(1 \leq i \leq m)$. Since $\psi_1 \neq \psi_2$, we can choose $\beta \in L$ such that $\psi_1(\beta) \neq \psi_2(\beta)$. Moreover, since ψ_1 is surjective, we can assume $\psi_1(\beta) \neq 0$. By $(*)$, we have

$$c_1\psi_1(\alpha\beta) + c_2\psi_2(\alpha\beta) + ...c_m\psi_m(\alpha\beta) = 0 \quad \forall \alpha \in L$$

By dividing the above equation by $\psi(\beta)$. We have

In the previous chapter, we see the example of E being the splitting field of $x^5 - 7$ over $\mathbb{Q}$. Then $E = \mathbb{Q}(\alpha, \zeta_5)$ with $\alpha = \sqrt[5]{7}$ and $\zeta_5 = e^{\frac{2\pi i}{5}}$. We recall that E is a simple extension of $Q(\zeta_5)$. Moreover,

its Galois group $Gal_{\mathbb{Q}(\zeta_5)}(E) \cong \mathbb{Z}/\langle 5\rangle$, which is cyclic. This example is a special case of the following general theorem.

Theorem 10.0.2
Let F be a field and $n \in \mathbb{N}$. Suppose $ch(F) = 0$ or p with $p \nmid n$. Assume also that $x^n - 1$ splits over F

(1) If the Galois extension E/F is cyclic of degree n, then $E = F(\alpha)$ for some $\alpha \in E$ with $\alpha^n \in F$. In particular, $x^n - \alpha^n$ is the minimal polynomial of α over F

(2) If $E = F(\alpha)$ with $\alpha^n \in F$, then E/F is a cyclic extension of degree d with $d \mid n$ and $\alpha^d \in F$. In particular, $x^d - \alpha^d$ is the minimal polynomial of α over F

Proof: Let $\zeta_n \in F$ be **primitive n-th root of unity**. i.e. $\zeta_n^n = 1$ and $\zeta_n^d \neq 1$ for any $1 \leq d < n$. Note that since $ch(F) = 0$ or p with pn, $x^n - 1$ separable. Then $1, \zeta_n, \zeta_n^2, ...\zeta_n^{n-1}$ are all distinct.

(1) Let $G = Gal_F(E) = \langle \psi \rangle \cong C_n$, the cyclic group of order n. Apply Dedekind's Lemma ti $K = L = E$, ψ_i all elements of G, and $c_1 = 1$, $c_2 = \zeta_n^{-1}$,.....,$c_n = \zeta_n^{-(n-1)}$. Since $c_i \neq 0$ for $1 \leq i \leq n$, there exists $u \in E$ such that

$$\alpha = u + \zeta_n^{-1}\psi(u) + ... + \zeta_n^{-(n-1)}\psi^{n-1} \neq 0$$

we have

$$1(\alpha) = \alpha \quad \psi(\alpha) = \alpha\zeta_n \quad \psi^2(\alpha) = a\zeta_n^2 \quad ..... \quad \psi^{n-1}(\alpha) = \alpha\zeta_n^{n-1}$$

Then $\alpha, \alpha\zeta_n, ..., \alpha\zeta_n^{n-1}{}_n$ are conjugate to each other. i.e. they have the same minimal polynomial over F, say $p(x)$. Since $\alpha, \alpha\zeta_n, ..., \alpha\zeta_n^{n-1}$ are all distinct, it follows that $\deg(p) = n$. Also, since $p(x) \in F[x]$,

$$p(0) = \pm\alpha(\alpha\zeta_n).....(\alpha\zeta_n^{n-1}) = \pm\alpha^n\zeta_n^{\frac{n(n-1)}{2}} \in F$$

Since $\zeta_n \in F$, $\alpha^n \in F$, since α is a root of $x^n - \alpha^{\in}F[x]$ and $\deg(p) = n$, we have $p(x) = x^n - \alpha^n$. Moreover, since $F(\alpha) \subseteq E$ and $[F(\alpha) : F] = \deg(p) = n = [E : F]$, we have $E = F(\alpha)$.

(2) Suppose $\alpha^n \in F$, let $p(x) \in F[x]$ be the minimal polynomial of α over F. Since α is a root of $x^n - \alpha^n \in F[x]$, $p(x) \mid (x^n - \alpha^n)$. Then the roots of $p(x)$ are of the form $\alpha\zeta_n^i$ for some i and we have

$$p(0) = \pm\alpha^d\zeta_n^k \qquad \textbf{for some } k \in \mathbb{Z} \textbf{ and } d = \textbf{the number of roots of } p(x) = \deg(p)$$

Since $p(0) \in F$ and $\zeta_n \in F$, it follows that $\alpha^d \in F$. Since $x^d - \alpha^d \in F[x]$ has α as a root. $p(x) \mid (x^d - \alpha^d)$. Since $\deg(p) = d$ and $p(x)$ is monic, we have $p(x) = x^d - \alpha^d$.
Claim:$d \mid n$
Suppose not, we say $n = qd + r$ with $q \in \mathbb{Z}$ and $0 < r < d$. Since $\alpha^d, \alpha^n \in F$, we have

$$\alpha^r = \alpha^{n-qd} = (\alpha^n)(\alpha^{-d})^q \in F$$

Since $\alpha^r \in F$, α is a root of $x^r - \alpha^r \in F[x]$. It follows that $p(x) \mid (x^r - \alpha^r)$, a contradiction since $\deg(p) = d > r$. Thus $d \mid n$, write $n = md$, since $p(x) = x^d - \alpha^d$, the roots of $p(x)$ are

$$\alpha, \alpha\zeta_n^m, \alpha\zeta_n^{2m}, ..., \alpha\zeta_n^{(d-1)m}$$

Since $\zeta_n \in F$, $E = F(\alpha)$ is the splitting field of the separable polynomial $p(x)$ over F, then Galois. If $\psi \in G = Gal_F(E)$ satisfies $\psi(\alpha) = \alpha\zeta_n^m$, then $G = \langle\psi\rangle \cong C_d$. Then, E/F is a cyclic extension of degree d.

When the degree of the polynomial and the characteristic of the base field are both p, the criterion for cyclic extension is a bit more complicated.

Theorem 10.0.3
Let F be a field with $ch(F) = p$, where p is prime.

(1) If $x^p - x - a \in F[x]$ is irreducible, then its splitting field E/F is a cycylic extension of degree p

(2) If E/F is a cyclic extension of degree p, then E/F is the splitting field of some irreducible polynomial $x^p - x - a \in F[x]$

Proof:
(1) Let $f(x) = x^p - x - a$ and α a root of $f(x)$. Then since $ch(F) = p$

$$f(\alpha + 1) = (\alpha + 1)^p - (\alpha + 1) - a = \alpha^p + 1 - \alpha - 1 - a = f(\alpha) = 0$$

i.e. $\alpha + 1$ is also a root of $f(x)$. Similarly, $\alpha + 2, \alpha + 3, ..., \alpha + (p - 1)$ are roots of $f(x)$. Since $f(x)$ has at most p distinct roots,

$$\alpha, \alpha + 1, \alpha + 2, ..., \alpha + (p - 1)$$

are all roots of $f(x)$. It follows that $E = F(\alpha, \alpha + 1, , ..., \alpha + (p - 1)) = F(\alpha)$ and $[E : F] = \deg(f) = p$. Since C_p is the only group of order p, we have $Gal_F(E) \cong C_p$. Indeed, $Gal_F(E) = \langle\psi\rangle$, where

$$\psi : E \to E, \quad \psi_F = 1_F \qquad \alpha \mapsto \alpha + 1$$

(2) Let $G = Gal_F(E) = \langle\psi\rangle C_p$. Apply Dedekind's Lemma to $K = L = E$, ψ_i all elements of G and $c_1 = c_2 = ... = c_p = 1$. Since $c_i \neq 0$ for $1 \leq i \leq p$, there exists some $v \in E$ such that

$$\beta := v + \psi(v) + \psi^2(v) + ... + \psi^{p-1}(v) \neq 0$$

Since $\psi^i(\beta) = \beta$ for all $\psi^i \in G$ for $0 \leq i \leq p-1$, $\beta \in F$. Let $u = \frac{v}{\beta}$, since $\beta \in F$ we have

$$\begin{aligned} & u + \psi(u) + \psi^2(u) + ... + \psi^{p-1}(u) \\ &= \frac{v}{\beta} + \psi^2\left(\frac{v}{\beta}\right) + ... + \psi^{p-1}\left(\frac{v}{\beta}\right) \\ &= \frac{v + \psi(v) + \psi^2(v) + ... + \psi^{p-1}(v)}{\beta} \\ &= \frac{\beta}{\beta} \\ &= 1 \end{aligned}$$

Set

$$\alpha := 0 \cdot u - 1\psi(u) - 2\psi^2(u) - ..... - (p-1)\psi^{p-1}(u)$$

Then

$$\psi(\alpha) = -\psi^2(u) - 2\psi^3(u) - .... - (p-1)\psi^p(u)$$

Then

$$\psi(\alpha) - \alpha = \psi(u) + \psi^2(u) + ... + \psi^{p-1}(u) + \psi^p(u) = 1$$

i.e. $\psi(\alpha) = \alpha + 1$, since $ch(F) = p$, we have

$$\psi(\alpha^p) = \psi(\alpha)^p = (\alpha + 1)^p = \alpha^p + 1$$

It follows that

$$\psi(\alpha^p - \alpha) = \psi(\alpha 6p) - \psi(\alpha) = (\alpha^p + 1) - (\alpha + 1) = \alpha^p - \alpha$$

Then $\alpha^p - \alpha$ is fixed by ψ. Since $G = \langle\psi\rangle$, it follows that $a = \alpha^p - \alpha \in F$ and α is a root of $x^p - x - a \in F[x]$. Since $[E : F] = p$, $[F(\alpha) : F]$ is a factor of p. Since $\alpha \notin F$ (as $\psi(\alpha) = \alpha + 1$) and p is a prime, we have $[F(\alpha) : F] = p$ and $E = F(\alpha)$. Since $[F(\alpha) : F] = p$, $x^p - x - a \in F[x]$ is the minimal polynomial of α over F

11. Solvability by Radicals

11.1 Radical Extensions

Definition 11.1.1
A finite extension E/F is **radical** if there exists a tower of fields

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq .... \subseteq ....F_m = E$$

such that $F_i = F_{i-1}(\alpha_i)$ and $\alpha_i^{d_i} \in F_{i-1}$ for some $d_i \in N$ $(1 \leq i \leq m)$

Lemma 11.1.1
If E/F a finite separable radical extension, then its normal closure N/F is also radical.

Proof: Since E/F is a finite separable extension, by **Theorem 8.1.4** $E = F(\beta)$ for some $\beta \in E$. Since E/F is a radical extension, there is a tower

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq .... \subseteq ....F_m = E$$

such that $F_i = F_{i-1}(\alpha_i)$ and $\alpha_i^{d_i} \in F_{i-1}$ for some $d_i \in \mathbb{N}$. Let $p(x) \in F[x]$ be the minimal polynomial of β and let $\beta = \beta_1, \beta_2, ..., \beta_n$ be roots of $p(x)$. By the definition of normal closure and **Theorem 8.2.1**, $N = E(\beta_2, \beta_3, ..., \beta_n) = F(\beta_1, \beta_2, ..., \beta_n)$. Also, there is an $F-$isomorphism

$$\sigma_j : F(\beta) \to F(\beta_j), \quad \beta \mapsto \beta_j, \quad \forall j = 2, 3, ..., n$$

Since N can be viewed as the splitting field of $p(x)$ over $F(\beta)$ and $F(\beta_j)$ respective, by **Theorem 3.2.1**, there exists $\psi_j : N \to N$ which extends σ_j $(2 \leq j \leq n)$. Then, $\psi_j \in Gal_F(N)$ and

$\psi_j(\beta) = \beta_j$. We have the following tower of fields

$$\begin{aligned} F = F_0 \subseteq F_1 \subseteq F_2 \subseteq .... \subseteq F_m = E = F(\beta_1) = F(\beta_1)\psi_2(F_0) \\ = F(\beta_1)\psi_2(F_1) \subseteq F(\beta_1)\psi_2(F_2) \subseteq .... \subseteq F(\beta_1)\psi_2(F_m) = F(\beta_1, \beta_2) = F(\beta_1, \beta_2)\psi_3(F_0) \\ \subseteq F(\beta_1, \beta_2)\psi_3(F_1) \subseteq ..... \\ \subseteq .... \subseteq F(\beta_1, \beta_2, .., \beta_n) = N \end{aligned}$$

Note that since $F_i = F_{i-1}(\alpha_i)$ and $\alpha_i^{d_i} F_{i-1}$, we have

$$\begin{aligned} F(\beta_1, \beta_2, ..., \beta_{j-1})\psi_j(F_i) &= F(\beta_1, \beta_2, ..., \beta_{j-1})\psi_j(F_{i-1}(\alpha_i)) \\ &= (F(\beta_1, \beta_2, ..., \beta_{j-1})\psi_j(F_{i-1}))(\psi_j(\alpha_i)) \end{aligned}$$

and $(\psi_j(\alpha_i))^{d_i} = \psi_j(\alpha_j^{d_i}) \in \psi_j(F_{i-1})$, then N/F is also radical extension.

■ **Remark 11.1** By **Theorem 11.1.1**, to consider a finite separable radical extension, we could instead consider its normal closure, which is Galois. ■

Definition 11.1.2
Let F be a field and $f(x) \in F[x]$. We say $f(x)$ is **solvable by radicals** if there exists a radical extension E/F such that $f(x)$ splits over E

■ **Remark 11.2** It's possible that $f(x) \in F[x]$ is solvable by radicals, but splitting field is not a radical extension (see Assignment 11, Question 2) ■

■ **Remark 11.3** We recall that an expression involving only $+, -, *, \div, \sqrt[n]{}$. Let F be a field and $f(x) \in F[x]$ be separable. If $f(x)$ is solvable by radicals, by the definition of radical extensions, $f(x)$ has a radical root. Conversely, if $f(x)$ has a radical root, it's in some radical extension E/F. By **Lemma 11.1.1**, the normal closure N/F of E/F is radical. Since $f(x)$ splits over N, $f(x)$ is solvable by radicals. ■

11.2 Radical Solutions

Lemma 11.2.1
Let E/F be a field extension and let K, L be intermediate fields of E/F. Suppose that K/F is a finite Galois extension. Then KL is a finite Galois extension of L and $Gal_L(KL)$ is isomorphic to a subgroup of $Gal_F(K)$.

Proof: Since K/F is a finite Galois extension, K is the splitting field of some $f(x) \in F[x]$ over F. Since $F \subseteq L$, KL is the splitting field of $f(x)$ over L, then Galois. Consider the map

$$\Gamma : Gal_L(KL) \to Gal_F(K), \quad \psi \mapsto \psi \mid_K$$

Note that $\psi \in Gal_L(KL)$ fixes L, then F. Also, since K is a Galois extension. $\psi(K) = K$, then Γ is well-defined. Moreover, if $\psi \mid_K = 1_K$, then ψ is trivial on K and L. Then, ψ is trivial on KL. This shows that Γ is an injection. Then, $Gal_L(KL) \cong \operatorname{Im}\Gamma$, a subgroup of $Gal_F(K)$.

Definition 11.2.1
Let E/F be the splitting field of a separable polynomial $f() \in F[x]$. The **Galois group of** $f(x)$ is defined to be $Gal_F(E)$, denoted by $Gal(f)$.

Theorem 11.2.2
Let F be a field with $ch(F) = 0$ and $f(x) \in F[x] \setminus \{0\}$. Then $f(x)$ is solvable by radicals if and only if its Galois group $Gal(f)$ is solvable.

Proof: $\Longrightarrow$ Suppose that $f(x)$ is solvable by radicals, i.e. $f(x)$ splits over some extensions E/F satisfying

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq ..... \subseteq F_m = E$$

with $F_i = F_{i-1}(\alpha_i)$ and $\alpha_i^{d_i} \in F_{i-1}$ for some $d_i \in \mathbb{N}$. By **Lemma 11.1.1**, **WLOG** we can assume E/F is Galois. Then, E/F is the splitting field of some $\tilde{f}(x) \in F[x]$. Let

$$n = \prod_{i=1}^{m} d_i$$

Let L/E be the splitting field of $x^n - 1$ over E and $\zeta_n \in L$ a primitive n-th root of unity. Set $K = F(\zeta_n)$ and we have $L = E(\zeta_n) = KE$. Define

$$K_i = KF_i = F_i(\zeta_n)$$

Then we have

$$F \subseteq F(\zeta_n) = K = K_0 \subseteq K_1 \subseteq .... \subseteq K_{m-1} \subseteq K_m = F_m(\zeta_n) = L$$

Since $F_i = F_{i-1}(\alpha_i)$, we have $K_i = K_{i-1}(\alpha_i)$. Since $\alpha_i^{d_i} \in F_{i-1} \subseteq K_{i-1}$ and $\zeta_n \in K_{i-1}$. (thus $\zeta_{d_i} = \zeta_n^{\frac{n}{d_i}}$). By **Theorem 10.0.2**, K_i/K_{i-1} is a cyclic Galois extension. Note that L is the splitting field of $\tilde{f}(x)(x^n - 1)$ over F (also over K_i). Hence, L/F (also L/K_i) is Galois. We have

$$G = Gal_F(L) \supseteq Gal_{K_0}(L) \supseteq Gal_{K_1}(L) \supseteq .... \supseteq Gal_{K_{m-1}}(L) \supseteq Gal_{K_m}(L) = \{1\}$$

Since K_i/K_{i-1} is Galois extension, by **Theorem 9.2.3**, $Gal_{K_i}(L) \lhd Gal_{K_{i-1}}(L)$ and we have

$$Gal_{K_{i-1}}(L)/Gal_{K_i}(L) \cong Gal_{K_{i-1}}(K_i)$$

which is a cyclic group, then abelian. Also we have

$$Gal_F(L)/Gal_{K_0}(L) = Gal_F(L)/Gal_K(L) \cong Gal_F(K) = \langle \mathbb{Z}/\langle n \rangle \rangle^*$$

is abelian. Then, $Gal_F(L)$ is solvable. Let $\tilde{E}$ be the splitting field of $f(x)$, which is a subfield of L. Since $\tilde{E}/F$ is a Galois extension, by **Theorem 9.2.3** we have

$$Gal(f) = Gal_F(\tilde{E}) \cong Gal_F(L)/Gal_{\tilde{E}}(L)$$

Since $Gal(f)$ is a quotient group of the solvable group $Gal_F(L)$, by **Theorem 6.1**, $Gal(f)$ is solvable.

$\Longleftarrow$ Suppose $G = Gal(f)$ is solvable. Let E/F be the splitting field of $f(x)$ and $|G| = n$. Let L/E be the splitting field of $x^n - 1$ over E and $\zeta_n \in L$ a primitive n-th root of unity. Set $K = F(\zeta_n)$ and we have $L = E(\zeta_n) = KE$. Since $L = KE$ and E/F is a finite Galois extension, by **Lemma 11.2.1** L/K is a finite Galois extension and $H = Gal_K(L)$ is isomorphic to a subgroup of G. By **Theorem 6.0.1**, H is solvable, we write

$$H = H_0 \supseteq H_1 \supseteq H_2 \supseteq ..... \supseteq H_m = \{1\}$$

where $H_i \lhd H_{i-1}$ and $H_{i-1}/H_i \cong C_{d_i}$, a cyclic group of order d_i $(1 \leq i \leq m)$. Since H is a subgroup of G, we have $d_i \mid n$. Let $K_i = H_i^* = L^{H_i}$ $(0 \leq i \leq m)$, then $Gal_{K_i}(L) = H_i$. We have a tower of fields

$$F \subseteq F(\zeta_n) = K = K_0 \subseteq K_1 \subseteq K_2 \subseteq .... \subseteq K_{m-1} \subseteq K_m = L = E(\zeta_n)$$

Since $H_i \lhd H_{i-1}$, by **Theorem 9.2.3**, K_i/K_{i-1} is Galois and $Gal_{K_{i-1}}(K_i) \cong H_{i-1}/H_i \cong C_d$. Since ζ_n, then $\zeta_{d_i} = \zeta_n^{\frac{n}{d_i}}$, is K_{i-1}. By **Theorem 10.0.2**, there exists $\alpha_i \in K_i$ s.t.

$$K_i = K_{i-1}(\alpha_i) \quad \textbf{and} \quad a_i^{d_i} \in K_{i-1}$$

Moreover, we have

$$K_0 = K = F(\zeta_n) \quad \textbf{and} \quad \zeta_n^n = 1 \in F$$

It follows that L/F is a radical extension. Since all roots of $f(x)$ are in E, then in L, we conclude that $f(x)$ is solvable by radicals

Proposition 11.2.3
Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of prime degree p. If $f(x)$ contains precisely two non-real roots in $\mathbb{C}$, then $Gal(f) \cong S_p$

Proof: We recall that the symmetric group S_n can be generated by cycles (12) and (123....n). Then, to show $Gal(f) \cong S_p$, it suffices to find a p-cycle and 2-cycle in $Gal(f)$. Since $\deg(f) = p$, by **Theorem 7.2.2**, $Gal(f)$ is a subgroup of S_p. Let α be a root of $f(x)$. Since $f(x)$ is irreducible of degree p, we have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = p$. Then we have $p \mid |Gal(f)|$. By **Cauchy's Theorem**, there exists an element of $Gal(f)$ which is of order p. i.e. a p-cycle. Also, the complex conjugate map $\sigma(a + bi) = a - bi$ will interchange two non-real roots of $f(x)$ and fixes all real roots. Then, it is an element of $Gal(f)$ which is of order 2. i.e. a 2-cycle. By changing notetion, if necessary, we have $(12), (12.....p) \in Gal(f)$. It follows that $Gal(f) \cong S_p$

■ **Example 11.1** Consider $f(x) = x^5 + 2x^3 - 24x - 2 \in \mathbb{Q}[x]$ which is irreducible by **Eisenstein's Criterion** with $p = 2$. Since

$$f(-1) = 19 \qquad f(1) = -23 \qquad \lim_{x\to\infty} f(x) = \infty \qquad \lim_{x\to-\infty} f(x) = -\infty$$

there are at least 3 real roots of $f(x)$. Let $\alpha_1, \alpha_2, ..., \alpha_5$ be roots of $f(x)$. i.e. $f(x) = (x-\alpha_1).....(x-\alpha_5)$. By considering the coefficients of x^4 and x^3 terms of $f(x)$ we have

$$\sum_{i=1}^{5} \alpha_i = 0 \qquad \sum_{i<j} \alpha_i\alpha_j = 2$$

From the first sum, we have

$$\left(\sum_{i=1}^{5} \alpha_i\right)^2 = \sum_{i=1}^{5} \alpha_i^2 + 2\sum_{i<j} \alpha_i\alpha_j = 0$$

It follows that

$$\sum_{i=1}^{5} \alpha_i^2 = -4$$

Then, not all roots of $f(x)$ are real. It follows that $f(x)$ has 3 real roots and 2 complex root. By **Prop 11.2.3**, $Gal(f) \cong S_5$. Since S_5 is not solvable, by **Theorem 11.2.2** the polynomial $x^5+2x^3-24x-2$ over $\mathbb{Q}$ is not solvable by radicals. ■

From the above example, we see a polynomial of degree 5 is not always solvable by radicals. Since $S_5 \subseteq S_n$ for all $n \geq 5$, we have

Theorem 11.2.4 — The Abel-Ruffini Theorem.
A general polynomial $f(x)$ with $\deg(f) \geq 5$ is not solvable by radicals.