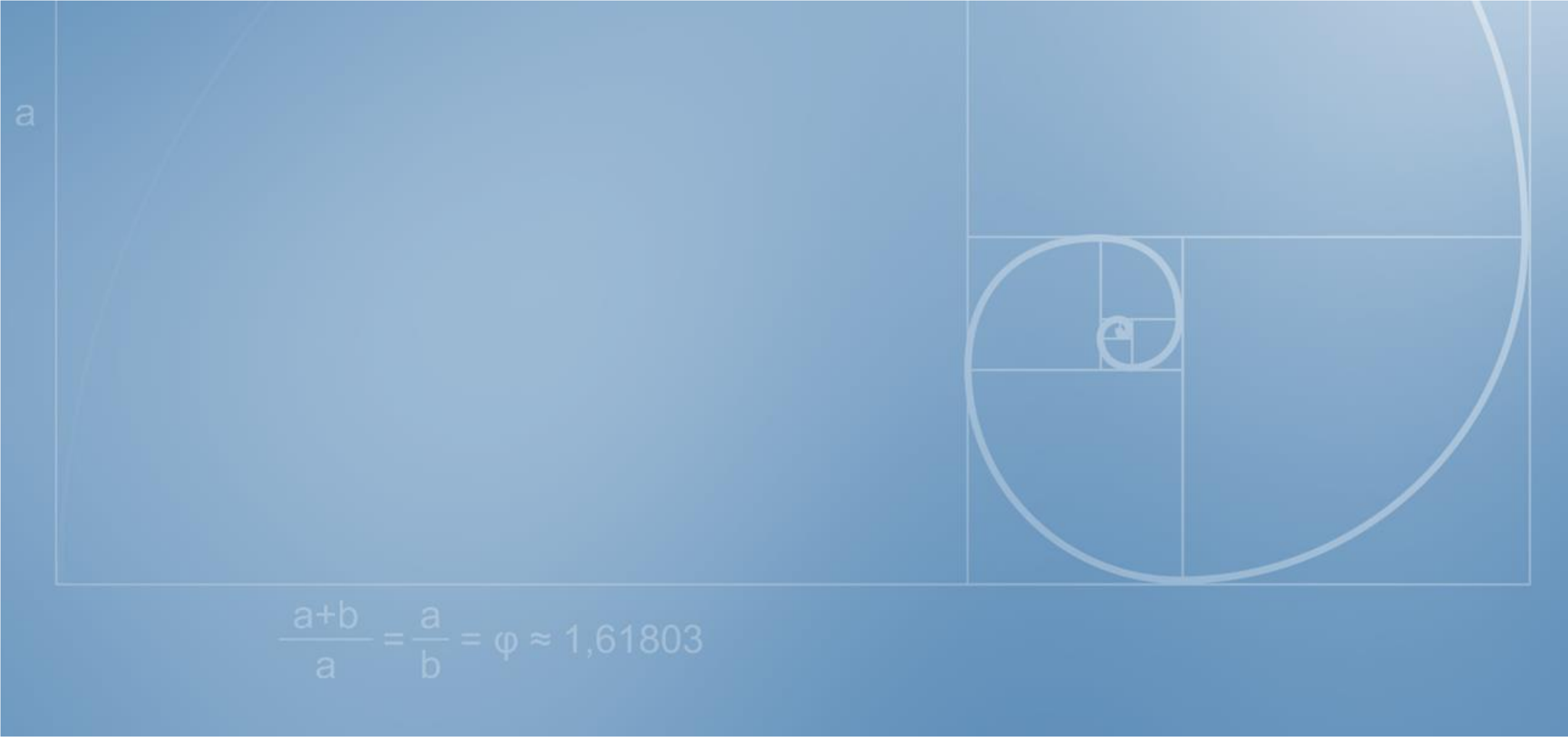
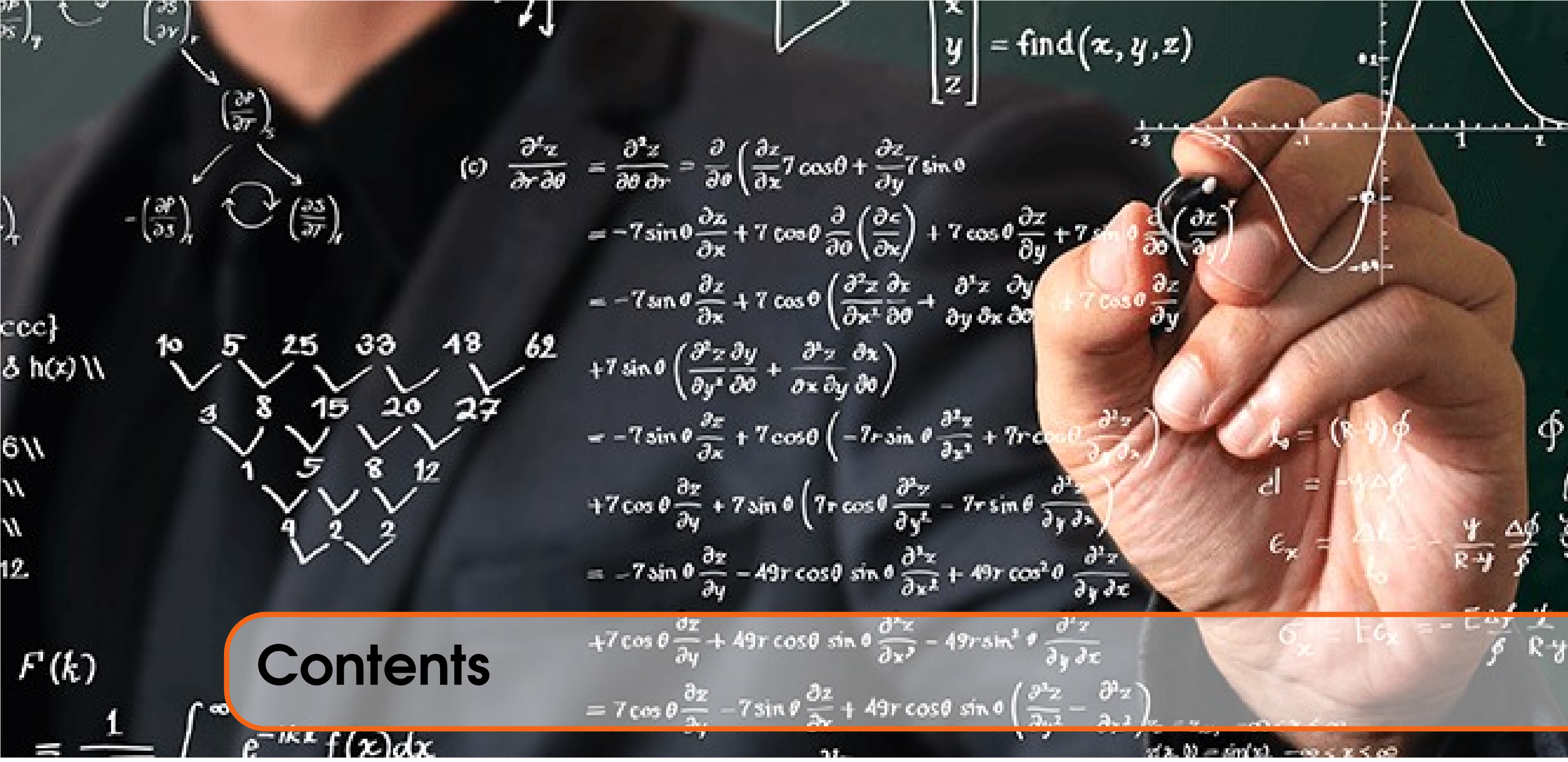


PMATH 348 Course Notes

University of Waterloo

The One And Only
Waterloo 76er
Bill Zhuo

[section]Lemma



Contents

I	**Field Theory**	
1	**Introduction**	**7**
1.1	**Introduction**	**7**
1.1.1	Polynomial Equations	7
1.1.2	Two Main Steps of Galois Theory	8
1.2	**Review of Ring Theory**	**8**
2	**Field Extensions**	**11**
2.1	**Degree of Extensions**	**11**
2.2	**Algebraic and Transcendental Extensions**	**13**
2.3	**Eisenstein's Criterion**	**16**
3	**Splitting Fields**	**19**
3.1	**Splitting Fields**	**19**
3.1.1	Existence of Splitting Fields	19
3.2	**Uniqueness of Splitting Field (up to isomorphism)**	**20**
3.3	**Degrees of Splitting Fields**	**21**
4	**More Field Theory**	**23**
4.1	**Prime Fields**	**23**
4.2	**Formal Derivatives and Repeated Roots**	**24**
4.3	**Finite Fields**	**25**

4.4 Separable Polynomial 26

5 The Sylow Theorems 29
5.1 Back in the Group Days 29
5.2 The Sylow Theorems 31

6 Solvable Groups 35
6.1 Introduction 35
6.1.1 Simple Group 36

7 Automorphism Groups 39
7.1 Automorphism Groups 39
7.2 Fixed Fields 40

8 Separable Extensions and Normal Extensions 43
8.1 Separable Extensions 43
8.1.1 Simple Extension 44
8.2 Normal Extensions 45

9 Galois Correspondence 49
9.1 Galois Extension 49
9.2 The Fundamental Theorem 52

Field Theory

1 Introduction 7
1.1 Introduction
1.2 Review of Ring Theory

2 Field Extensions 11
2.1 Degree of Extensions
2.2 Algebraic and Transcendental Extensions
2.3 Eisenstein's Criterion

3 Splitting Fields 19
3.1 Splitting Fields
3.2 Uniqueness of Splitting Field (up to isomorphism)
3.3 Degrees of Splitting Fields

4 More Field Theory 23
4.1 Prime Fields
4.2 Formal Derivatives and Repeated Roots
4.3 Finite Fields
4.4 Separable Polynomial

5 The Sylow Theorems 29
5.1 Back in the Group Days
5.2 The Sylow Theorems

6 Solvable Groups 35
6.1 Introduction

7 Automorphism Groups 39
7.1 Automorphism Groups
7.2 Fixed Fields

8 Separable Extensions and Normal Extensions 43
8.1 Separable Extensions
8.2 Normal Extensions

9 Galois Correspondence 49
9.1 Galois Extension
9.2 The Fundamental Theorem

1. Introduction

General Outline

1. 5 Assignments due at 6pm on Tuesdays (25%)
2. In-class midterm on Wednesday Feb 12 (25%)
3. Final (50%)

1.1 Introduction

1.1.1 Polynomial Equations

Definition 1.1.1 — Linear Equation. Let $ax+b=0$ with $a,b \in \mathbb{R}$ and $a \neq 0$ then $x = -\frac{b}{a}$

Definition 1.1.2 — Quadratic Equation. Let $ax^2+bx+c=0$ with $a,b,c \in \mathbb{R}$ and $a \neq 0$ then its solutions are

$$x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$$

Definition 1.1.3 — Radical. A expression involving only $+,-,*,/,\sqrt[n]{\cdot}$ is a called a radical

Cubic Equations (Tartagilia, def Ferro, Fontana (1535))

All cubic equations can be reduced to the following equation

$$x^3 + px = q$$

a radical solution of the above equation is of the folowing form

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$$

or also known as **Cardano's Formula**

Quartic Equations (Ferrari)

A radical solution for quartic eqautions can be found.

Quintic Equations?

1. Attempted by Euler, Bezout, Lagrange without success
2. In 1799, Ruffini gave a 516-page proof about the insolvability of quintic equations. His proof was “almost correct"
3. In 1824, Abel filled the gap in Ruffini’s proof and it was later simplified by Kronecker in 1879

Question Given a quintic equation, is it solvable by radicals? (Not a good question)

Revered Question Suppose that a radical solution exists, how does its associated quintic equation look like? (Galois Theory way)

1.1.2 Two Main Steps of Galois Theory

1. Link a root of a quintic equation say α to $\mathscr{Q}(\alpha)$, **the smallest field containing $\mathscr{Q}$ and α**
   (a) $\mathscr{Q}(\alpha)$ is a field to be played with than α alone
   (b) However, out knowledge of $\mathscr{Q}(\alpha)$ is still too little to answer the question

   ■ **Example 1.1** We do not know how many intermediate fields E between $\mathscr{Q}$ and $\mathscr{Q}(\alpha)$, i.e $\mathscr{Q} \leq E \leq \mathscr{Q}(\alpha)$ ■

   Note that

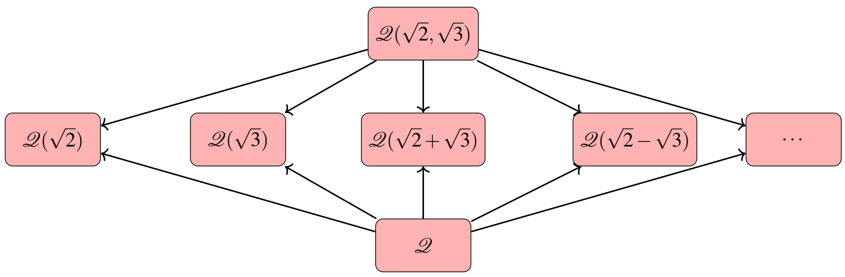


Figure 1.1.1: *There are infinitely many of intermediate fields*

2. Link the field $\mathscr{Q}(\alpha)$ to a group. More precisely, we associate the field extension $\mathscr{Q}(\alpha)\big/\mathscr{Q}$ to the group

$$\textbf{Aut}_{\mathscr{Q}}(\mathscr{Q}(\alpha)) = \{\phi : \mathscr{Q}(\alpha) \to \mathscr{Q}(\alpha) \text{ is an isomorphism and } \phi\big|_{\mathscr{Q}} = 1_{\mathscr{Q}}\}$$

   (a) It can be shown that if α is ‘good’, say algebraic $\textbf{Aut}_{\mathscr{Q}}(\mathscr{Q}(\alpha))$ is finite
   (b) If α is ‘very good’, say constructible, the order of $\textbf{Aut}_{\mathscr{Q}}(\mathscr{Q}(\alpha))$ is in certain forms
   (c) Moreover, there is a $1-1$ correspondence between the intermediate fields of $\mathscr{Q}(\alpha)\big/\mathscr{Q}$ and the subgroups of $\textbf{Aut}_{\mathscr{Q}}(\mathscr{Q}(\alpha))$

Definition 1.1.4 — Galois Theory. The interplay between fields and groups

1.2 Review of Ring Theory

Definition 1.2.1 — Commutative Ring with 1. A commutative ring with 1 is a set R equipped with addition $+$ and multiplication $\cdot$ such that

1. R is an abelian additive group with the additive identity to be 0
2. The multiplication is a commutative and associative. Also, there exists $1 \in R$ such that $1 \cdot r = r, \forall r \in R$
3. For all $r,s,t \in R$, $r(s+t) = rs + rt$

Definition 1.2.2 — Field. A field is a ring R in which every $a \in R \backslash \{0\}$ is a unit, i.e. $ab = 1$ for some $b \in R$.

Definition 1.2.3 — Integral Domain. A ring R is an integral domain if for $a, b \in R$, then

$$ab = 0 \rightarrow a = 0 \text{ or } b = 0$$

■ **Example 1.2** We know that $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ with p as a prime are all fields.
And the set of integer $\mathbb{Z}$ is an integral domain. ■

Proposition 1.2.1 Every subring of a field is an integral domain.

Definition 1.2.4 — Ideal. An ideal of 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 1.3** The only ideals of a field F are 0 and F. ■

Definition 1.2.5 — Principle Ideal Domain (PID). An integral doamin R is a principle ideal domain (PID) if every ideal is generated by one element.

■ **Example 1.4** The set of $\mathbb{Z}$ is an ID. The units of $\mathbb{Z}$ are $\{\pm 1\}$.

Lemma 1.2.2 — Division Algorithm. For $a, b \in \mathbb{Z}$ with $b > 0$, we can write $a = qb + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < b$.

using this, 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 is unique. ■

Consider all fields containing $\mathbb{Z}$. Their intersection (the smallest field containing $\mathbb{Z}$) is the set of rational numbers

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

Definition 1.2.6 — Polynomial Ring Over Field F. Let F be a field. Define

$$F[x] = \{ f(x) = a_0 + a_1 x + \cdots + a_m x^m, m \geq 0, a_i \in F \}$$

1. If $a_n = 1$, we say $f(x)$ is monic
2. If $a_n \neq 0$, we define the degree of f to be $\deg(f) = m$; Also, $\deg(0) = -\infty$ (why? to make the following contents work).
3. For $f(x), g(x) \in F[x]$,
$$\deg(fg) = \deg(f) + \deg(g)$$
4. The set $F[x]$ is an ID and the units of $F[x]$ are $F^* = F \backslash \{0\}$

   Lemma 1.2.3 — Division Algoritheorem for Polynomial Over F . For $f(x), g(x) \in F[x]$, $f(x) \neq 0$, we can write

   $$g(x) = q(x) f(x) + r(x)$$

   where $q(x), r(x) \in F[x]$ and $\deg(r) < \deg(f)$

   using this, we can prove that an ideal I of $F[x]$ is of the form $I = \langle f(x) \rangle = f(x)F[x]$

R Thus, $F[x]$ is a PID. Note that if $f(x)$ is monic modolo the units F^*, then the generator $f(x)$ is unique.

Definition 1.2.7 — Function Field. Consider all fields containing $F[x]$. Their intersection is the set of rational functions

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

Definition 1.2.8 — Quotient Ring. the quotient ring of R modulo I, denoted by ${}^{R}\big/_{I}$ contains elements of the form $r+I, r \in R$. The additiona and multiplication on ${}^{R}\big/_{I}$ are defined by

$$\begin{aligned}(r_1+I)+(r_2+I) &= (r_1+r_2)+I \\ (r_1+I)\cdot(r_2+I) &= (r_1\cdot r_2)+I\end{aligned}$$

■ **Example 1.5** For $n \in \mathbb{Z}$

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

For $f(x) \in F[x]$

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

■

Proposition 1.2.4 — First Isomorphism Theorem. Let $\phi : R \to S$ be a ring isomorphism. Then the kernel of ϕ is an ideal I. Moveover, there is an isomorphism

$$\psi : {}^{R}\big/_{I} \to \mathrm{Im}(\phi)$$

■ **Example 1.6** Let F be a field and S be a ring. Let $\phi : F \to S$ be a ring homomorphism. Since the only ideals of F are F and $\{0\}$, either $\phi = 0$ or ϕ is injective. ■

Definition 1.2.9 — Maximal Ideal. An ideal I is a ring R is maximal if $I \neq R$ and there is no ideal j with $I \subsetneq J \subsetneq R$.

Definition 1.2.10 — Prime Ideal. An ideal I in a ring R is prime if $I \neq R$ and

$$ab \in I \to a \in I \text{ or } b \in I$$

Proposition 1.2.5 Every maximal ideal is prime. Moverover, in **PID**, every prime ideal is maximal.

■ **Example 1.7** In $\mathbb{Z}$, $\langle n\rangle$ is maximal (prime) if and only if $\pm n$ is a prime
In $F[x]$, $\langle f(x)\rangle$ is maximal (prime) if and only if $f(x)$ is irreducible ■

Proposition 1.2.6 Let I be an ideal of a ring R and $I \neq R$, then

1. I is maximal if and only if ${}^{R}\big/_{I}$ is a field
2. I is prime if and only if ${}^{R}\big/_{I}$ is an PID

2. Field Extensions

2.1 Degree of Extensions

Definition 2.1.1 — Field Extension. If E is a field containing another field F, we will say E is a field extension of F, denoted by E/F.
Note: E/F does not mean quotient rings as fields have no 'honest' ideals

Definition 2.1.2 — $^E/_F$ is a vector space. If $^E/_F$ be the field extension, we can view E as a vector space over F.

1. Addition: $e_1, e_2 \in E$,
$$e_1 + e_2 := e_1 + e_2$$
regular addition of E
2. Scalar Multiplication: for $c \in F$, $e \in E$,
$$ce := ce$$
multiplication of E

Definition 2.1.3 — Degree of $^E/_F$. The dimension of E over F (viewed as a vector space) is called the degree of $^E/_F$, denoted by $[E : F]$

1. If $[E : F]$ is finite, we say $^E/_F$ is a finite extension
2. Otherwise, $^E/_F$ is an infinite extension

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

■ **Example 2.2** Let F be a field, we know $F[x]$ is not necessary a field, typically an Euclidean domain. But
$$F(x) = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in F[x], g(x) \neq 0 \right\}$$

is a field (proof is similar to fields of fraction). Then, $[F(x):F]$ is infinite, since

$$\{1, x, x^2, \ldots, x^n, \ldots\}$$

is a infinite linearly independent set. ∎

Theorem 1 If E/K and K/F are finite field extensions, then E/F is a finite extension. Moreover,

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

In particular, if K is an intermediate field of a finite extension E/F, then $[K:F] \big| [E:F]$.
Note: the same result also holds for infinite extensions

Proof. Suppose that $[E:K] = m$ and $[K:F]$=n. Let $\{a_1, \ldots, a_m\}$ be a basis of E/K. Let $\{b_1, \ldots, b_n\}$ be a basis of K/F. It suffices to prove

$$\{a_i b_j : 1 \leq i \leq m, 1 \leq j \leq n\}$$

is a basis of E/F.

1. Claim: every element of E is a linear combination of $\{a_1 b_j\}$ over F

   Proof. For $e \in E$, we have unique representation

   $$e = \sum_{i=1}^{m} k_i a_i, k_i \in K$$

   And for any $k_i \in K$, we have unique representation

   $$k_i = \sum_{j=1}^{n} c_{i,j} b_j, c_{i,j} \in F$$

   then,

   $$e = \sum_{i,j} c_{i,j} a_i b_j$$

   ∎

2. Claim: $\{a_i b_j : 1 \leq i \leq m, 1 \leq j \leq n\}$ is linearly independent over F.

   Proof. Suppose that

   $$\sum_{i=1}^{m} \sum_{j=1}^{n} c_{i,j} b_j a_i = 0, c_{i,j} \in F$$

   since $\sum_{j=1}^{n} c_{i,j} b_j \in K$ and $\{a_1, \ldots, a_m\}$ is linearly independent over K due to basis' property. Thus,

   $$\sum_{j=1}^{n} c_{i,j} b_j = 0, \forall 1 \leq i \leq m$$

   Then, since $c_{i,j} \in F$ and $\{b_1, \ldots, b_n\}$ is linearly independent over F due to basis' property. Thus,

   $$c_{i,j} = 0, \forall 1 \leq i \leq m, 1 \leq j \leq n$$

   Thus, $\{a_i b_j : 1 \leq i \leq m, 1 \leq j \leq n\}$ is linearly independent. ∎

   Thus, $\{a_i b_j : 1 \leq i \leq m, 1 \leq j \leq n\}$ is a basis for E/F and

   $$mn = [E:F] = [E:K][K:F] = m \times n$$

∎

2.2 Algebraic and Transcendental Extensions

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

■ **Example 2.3 — Algebraic Numbers.** $\frac{c}{d} \in \mathbb{Q}, \sqrt{2}, \sqrt[3]{7} + 2i$ are algebraic over $\mathbb{Q}$. ■

■ **Example 2.4 — Transcendental Numbers.** $e = 2.718...$ is transcendental proved by (Hermite 1873) and $\pi = 3.14...$ is transcendental by (Lindemann 1882) over $\mathbb{Q}$. ■

Definition 2.2.2 — $F[\alpha], F(\alpha)$. Let E/F be a field extension and $\alpha \in E$. Let $F[\alpha]$ to denote the smallest subring of E containing F and α. Let $F(\alpha)$ to denote the smallest subfield of E containing F and α. We can define $F[\alpha, \beta]$ and $F(\alpha, \beta)$ similarly, $\alpha, \beta \in E$.

Definition 2.2.3 — Simple Extension. If $E = F(\alpha)$ for some $\alpha \in E$, we say E is a simple extension.

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

Definition 2.2.4 Let R and R_1 be two rings which contain a field F. A ring homomorphism $\varphi : R \to R_1$ is said to be an "F-homomorphism" if

$$\varphi\big|_F = 1_F$$

Theorem 2 — (MIDTERM). Let E/F be a field extension and $\alpha \in E$.

1. If α is transcendental over F, then

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

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

Proof. Let $\phi : F(x) \to F(\alpha)$ be the unique F-homomorphism defined by $\phi(x) = \alpha$

(a) Well-definedness: for $f(x), g(x) \in F[x]$ with $g(x) \neq 0$, then

$$\phi\left(\frac{f}{g}\right) = \frac{f(\alpha)}{g(\alpha)} \in F(\alpha)$$

note that $g(\alpha) \neq 0$ since α is transcendental. Thus, the map is well-defined.

(b) Injective: Since $F(x)$ is a field and note that $\ker(\phi)$ is an ideal of $F(x)$, we have $\ker(\phi) = 0$ or $F(x)$. Thus, $\phi = 0$ or ϕ is injective. Since $\phi(x) = \alpha \neq 0$, we have the injectivity.

(c) Surjective: Also, since $F(x)$ is a field, $\mathrm{im}(\phi)$ contains a field generated by F and α, thus,

$$F(\alpha) \subseteq \mathrm{im}(\phi)$$

Thus, $\mathrm{im}(\phi) = F(\alpha)$ and ϕ is surjective.

Thus, ϕ is an isomorphism.

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

■

Theorem 3 — (MIDTERM). Let E/F be a field extension and $\alpha \in E$. If α is algebraic over F, there exits a unique monic irreducible polyonomial $p(x) \in F[x]$ such that there exists a F-isomorphism

$$\phi : F[x] \Big/ \langle p(x) \rangle \to F[\alpha] \text{ with } \phi(x) = \alpha$$

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

Proof. Consider the unique F-homorphism$\phi : F[x] \to F[\alpha]$ defined by $\phi(x) = \alpha$.

1. Well-defined: Thus, for $f(x) \in F[x]$, we have $\phi(f) = f(\alpha) \in F[\alpha]$.
2. Surjective: Since $F[x]$ is a ring, imϕ contains a ring generated by F and α, i.e, $F[\alpha] \subseteq$ imϕ. Thus, im$\phi = F[\alpha]$.
3. Injective: let
$$I = \ker\phi = \{f(x) \in F[x], f(\alpha) = 0\}$$
since α is algebraic, we know that $I \neq \{0\}$, we have
$$F[x]/I \cong \text{im}\phi$$
a subring of a field $F(\alpha)$. Thus, $F[x]/I$ is an integral domain and I is a prime ideal. It follows that $I = \langle p(x) \rangle$ where $p(x)$ is irreducible. If we assume $p(x)$ is monic, then it is unique. It follows that
$$F[x] \Big/ \langle p(x) \rangle \cong F[\alpha]$$
since $p(x)$ is irreducible, prime, maximal in a PID, so $F[x] \Big/ \langle p(x) \rangle$ is a field. Thus, $F[\alpha]$ is a field and hence $F[\alpha] \cong F(\alpha)$.

■

Definition 2.2.5 — Minimal Polynomial. If α is algebraic over a field F, the unique monic polynomial $p(x)$ in Theorem 3 is called the minimal polynomial of α over F. From the proof of Theorem 3, we see that if $f(x) \in F[x]$ with $f(\alpha) = 0$, then $p(x)|f(x)$.

Theorem 4 Let E/F be a field extension and $\alpha \in E$

1. α is transcendental over F if and only if $[F(\alpha) : F] = \infty$
2. α is algebraic over F if and only if $[F(\alpha) : F] < \infty$

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 $F(\alpha)/F$.

Proof. It suffices to prove one direction for (1) and (2).

1. From Theorem 2, if α is transcendental over F, then $F(\alpha) \cong F(x)$. In $F(x)$, the elements $\{1, x, x^2, \ldots\}$ are linearly independent over F. Thus, $[F(\alpha) : F] = \infty$.

2. From Theorem 3, if α is algebraic over F, then $F[\alpha] = F(\alpha) \cong F[x] \big/ \langle p(x) \rangle$ with $x \mapsto \alpha$. Note that
$$F[x] \big/ \langle p(x) \rangle = \{r(x) \in F[x], \deg(r) < \deg(p)\}$$
Thus, $\{1, \alpha, \alpha^2, \dots, \alpha^{\deg(p)-1}\}$ is a basis of $F[x] \big/ \langle p(x) \rangle$. It follows that
$$[F(\alpha) : F] = \deg(p)$$
and $\{1, \alpha, \alpha^2, \dots, \alpha^{\deg(p)-1}\}$ is a basis of $F(\alpha)$ over F.

■

Proposition 5 Let $E \big/ F$ be a field extension with $[E : F] < \infty$, then there exists $\alpha_1, \alpha_2, \dots, \alpha_n \in E$ such that
$$F \subsetneq F(\alpha_1) \subsetneq F(\alpha_1, \alpha_2) \subsetneq \cdots \subsetneq F(\alpha_1, \dots, \alpha_n) = E$$

Proof. We will prove this theorem by induction on $[E : F]$. If $[E : F] = 1$, $E = F$ and we have done. Now, suppose $[E : F] > 1$ and the statement holds for all field extensions $\tilde{E} \big/ \tilde{F}$ with $[\tilde{E} : \tilde{F}] < [E : F]$, let $\alpha_1 \in E \backslash F$. Then, by Theorem 1,
$$[E : F] = [E : F(\alpha_1)][F(\alpha_1) : F]$$
since $[F(\alpha_1) : F] > 1$, we have $[E : F(\alpha_1)] < [E : F]$.
By induction hypothesis, there exists $\alpha_1, \dots, \alpha_n$ such that
$$F(\alpha_1) \subsetneq F(\alpha_1, \alpha_2) \subsetneq \cdots \subsetneq F(\alpha_1, \dots, \alpha_n) = E$$
, thus, we have
$$F \subsetneq F(\alpha_1) \subsetneq F(\alpha_1, \alpha_2) \subsetneq \cdots \subsetneq F(\alpha_1, \dots, \alpha_n) = E$$

■

Definition 2.2.6 — Algebraic/Transcendental Field Extension. A field extension $E \big/ F$ is algebraic if every $\alpha \in E$ is algebraic over F. Otherwise, it is transcendental.

Theorem 6 Let $E \big/ F$ be a field extension. If $[E : F] < \infty$, then $E \big/ F$ is algebraic.

Proof. Suppose $[E : F] = n$ for $\alpha \in E$, the elements
$$\{1, \alpha, \dots, \alpha^n\}$$
are not linearly independent over F. Thus, there exists $c_i \in F$ such that
$$\sum_{i=0}^{n} c_i \alpha^i = 0$$
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. ■

R It might be tempting to think the converse is true, but not correct.

Theorem 7 — (MIDTERM). Let E/F be a field extension. 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 $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta} \in L$ for $\beta \neq 0$. Then, by definition of L, we know that $[F(\alpha) : F] < \infty$ and $[F(\beta) : F] < \infty$. Consider $F(\alpha, \beta)$. 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 $p(x) \in F[x]$, 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 1, we have

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

Since $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta} \in F(\alpha, \beta)$, they are in L. ∎

Definition 2.2.7 — Algebraic Closure. Let E/F be a field extension. The set

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

is called the algebraic closure of F in E.

Definition 2.2.8 — Algebraically Closed. A field F is algebraically closed if for any algebraic extension E/F, we have $E = F$.

■ **Example 2.5** By the 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 $[\mathbb{C} : \mathbb{R}] = 2$. ■

2.3 Eisenstein's Criterion

See SNew's Chapter 11 notes on LEARN!

Definition 2.3.1 — Primitive Polynomial. Let

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

we say $f(x)$ is primitive if $a_n > 0$ and the coefficients $a_0, \ldots, a_n$ have no common integer factor except for ± 1

Lemma 2.3.1 Every non-zero polynomial $f(x) \in \mathbb{Q}[x]$ can be written uniquely as a product $f(x) = c f_0(x)$ where $c \in \mathbb{Q}$ and $f_0 \in \mathbb{Z}[x]$ is a primitive polynomial. Moreover, $f(x) \in \mathbb{Z}[x]$ if and only $c \in \mathbb{Z}$.

Proposition 2.3.2 — Gauss' Lemma for $\mathbb{Z}[x]$. Let $f(x) \in \mathbb{Z}[x]$ be non-constant. If $f(x)$ is irreducible in $\mathbb{Z}[x]$, then it is irreducible in $\mathbb{Q}[x]$.

■ **Example 2.6** The converse of the above result is not true. For example, the polynomial $2x + 8$ is irreducible in $\mathbb{Q}[x]$, but $2x + 8 = 2(x + 4)$ is reducible in $\mathbb{Z}[x]$ ■

■ **Example 2.7** The polynomial $2x^7 + 3x^4 + 6x^2 + 12$ is irreducible in $\mathbb{Q}[x]$. By Eisenstein's criterion with $p = 3$ ■

■ **Example 2.8** Let p be a prime and let

$$U_p = e^{\frac{2\pi i}{p}} = \cos\left(\frac{2\pi}{p}\right) + i \sin\left(\frac{2\pi}{p}\right)$$

be the p-th root of unity. It is a root of the p-th cyclotomic polynomial

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

Eisenstein's Criterion does not apply here. However, we can consider

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

Since p is a prime, then $p \nmid 1, p \,\big|\, \binom{p}{1}, p \,\big|\, \binom{p}{2}, \ldots, p \,\big|\, \binom{p}{p-1}$ and $p^2 \,\big|\, \binom{p}{p-1}$. By Eisenstein's criterion, $\Phi_p(x+1)$ 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, $\Phi_p(x)$ is also irreducible in $\mathbb{Z}[x]$. ■

R The constant 2 in the example above is the only obstruction between irreducibility between $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$. More precisely, $f(x) \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$ if and only if either

1. $f(x)$ is a prime integer, **or**
2. $f(x)$ is primitive which is irreducible in $\mathbb{Q}[x]$

Theorem 8 — Eisenstein's Criterion in $\mathbb{Z}[x]$. Let $f(x) = a_n x^n + \ldots a_1 x + a_0 \in \mathbb{Z}[x]$ and let p be a prime. Suppose that $p \nmid a_n$, $p | a_i, 0 \leq i \leq n-1$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$. In particular, if $f(x)$ is primitive, then it is irreducible in $\mathbb{Z}[x]$.

Proof. Let's consider the map $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$ defined by

$$f(x) \mapsto \bar{f}(x) = \bar{a}_n x^n + \cdots + \bar{a}_1 x + \bar{a}_0 \mod p$$

since $p \nmid a_n$ and $p | a_i, 0 \leq i \leq n-1$. We have $\bar{f}(x) = \bar{a}_n x^n$ with $\bar{a}_n \neq 0$. If $f(x)$ is irreducible in $\mathbb{Q}[x]$, then it can be factored in $\mathbb{Z}[x]$ into polynomials of positive degrees. Say $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{Z}[x]$ with $\deg(g) \geq 1, \deg(h) \geq 1$ (By Gauss' Lemma). It follows that $\bar{a}_n x^n = \bar{g}(x)\bar{h}(x)$. Since $\mathbb{Z}_p[x]$ is a UFD, from which we see that $\bar{g}(x) = bx^m$ and $\bar{h} = cx^k$ for some $b, c \in \mathbb{Z}_p$. In other words, $\bar{g}(x)$ and $\bar{h}(x)$ have 0 constants in $\mathbb{Z}_p$. Since the constants of both $g(x), h(x)$ are divisible by p, this implies that the constant of $f(x)$ is divisible by p^2, which yields a contradiction. We're done. $f(x)$ is irreducible in $\mathbb{Q}[x]$. ■

We recall that $\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1$, which has $U_p = e^{\frac{2\pi i}{p}}$ as a root. By apply Eisenstein's Criterion to $\Phi_p(x+1)$, we see it is irreducible, then so is $\Phi_p(x)$.

■ **Example 2.9** Let p be a prime and $U_p = e^{\frac{2\pi i}{p}}$. Since U_p is a root of the p-th cyclotomic polynomial $\Phi_p(x)$, which is irreducible and monic. Then, by Theorem, $\Phi_p(x)$ is the minimal polynomial of U_p and $[\mathbb{Q}(U_p) : \mathbb{Q}] = p - 1$. The field $\mathbb{Q}(U_p)$ is called the **p-th cyclotomic extension of** $\mathbb{Q}$. ■

■ **Example 2.10 — Algebraic extension can be of infinite degree.** Let $\bar{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. i.e,

$$\bar{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}$$

suppose $U_p \in \bar{\mathbb{Q}}$, we ahve $[\bar{\mathbb{Q}} : \mathbb{Q}] \geq [\mathbb{Q}(U_p) : \mathbb{Q}] = p - 1$. Since $p \to \infty$, we have $[\bar{\mathbb{Q}} : \mathbb{Q}] = \infty$. We have seen in a theorem before that if E/F is finite, then E/F is algebraic. However, this example shows that the converse of the previous theorem is false. ■

Now, let R be any UFD with the fields of fractions F. Let $f(x) \in R[x]$ be non-constant. Therefore, $R[x]$ is a subring of $F[x]$ and the above results hold with $\mathbb{Z}$ replaced by R and $\mathbb{Q}$ by F.
In particular, we have

Theorem 9 — Eisenstein's Criterion. Let R be a UFD with the field of fraction F. Let l be an irreducible in R. If

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x], n \geq 1$$

and $l \nmid a_n, l | a_i, 0 \leq i \leq n-1$ and $l^2 \nmid a_0$, then $f(x)$ is irreducible in $F[x]$. Moreover, if $f(x)$ is primitive in $F[x]$, then $f(x)$ is also irreducible in $R[x]$.

3. Splitting Fields

3.1 Splitting Fields

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

Definition 3.1.2 — Splitting Field. Let $\tilde{E}\big/F$ be a field extension and $f(x) \in F[x]$ and $F \subseteq E \subseteq \tilde{E}$. 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** $f(x) \in F[x]$ in $\tilde{E}$.

3.1.1 Existence of Splitting Fields

Theorem 10 Let $p(x) \in F[x]$ be irreducible. The quotient ring $F[x]\big/\langle p(x)\rangle$ is a field containing F and a root of $p(x)$.

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

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

since F is a field and ψ is non-zero, we have ψ is injective. Thus, by identifying F with $\psi(F)$. F is a subfield of E.
We claim the let $\alpha = x + I \in E$, then α is a root of $p(x)$. Write

$$p(x) = a_0 + a_1x + \cdots + a_nx^n = (a_0 + I) + (a_1 + I)x + \cdots + (a_n + I)x^n \in E[x]$$

we have

$$p(\alpha) = (a_0 + I) + (a_1 + I)\alpha + \cdots + (a_n + I)\alpha^n$$
$$p(\alpha) = (a_0 + I) + (a_1 + I)(x + I) + \cdots + (a_n + I)(x + I)^n$$

$$= (a_0 + a_1x + \cdots + a_nx^n) + I = p(x) + I = 0 + I = I$$

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

Theorem 11 — Kronecker. Let $f(x) \in F[x]$. There exists a field E containing F such that $f(x)$ splits over E.

Proof. We prove this theorem by induction on the degree of f. If $\deg(f) = 1$, we can take $E = F$, 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

$$f(x) = p(x)h(x), p(x), h(x) \in F[x]$$

and $p(x)$ is irreducible. By theorem 10, there exists a field K such that $F \subseteq K$ and K containing a root of $p(x)$, say α. Thus,

$$p(x) = (x-\alpha)q(x) \to f(x) = (x-\alpha)q(x)h(x)$$

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

Theorem 12 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 11, there exists a field extension ${}^{E}/_{F}$ over which $f(x)$ splits, and say

$$\alpha_1, \alpha_2, \ldots, \alpha_n$$

are roots of $f(x)$ in E. Consider $F(\alpha_1, \ldots, \alpha_n)$. This fields contains all roots of $f(x)$ and $f(x)$ does not split over any proper subfield of it. Thus, $F(\alpha_1, \ldots, \alpha_n)$ is the splitting field of $f(x)$ in E. In addition, since α_i are all algebraic, ${}^{F(\alpha_1, \ldots, \alpha_n)}/_{F}$ is finite. ■

3.2 Uniqueness of Splitting Field (up to isomorphism)

Question: If we change ${}^{E}/_{F}$ to a different field extension, say ${}^{E_1}/_{F}$, what is the relation between the splitting field of $f(x)$ in E and the one in E_1?

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

Theorem 13 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. Then, let $f_1(x) = \Phi(f(x))$ and ${}^{E}/_{F}$ and ${}^{E_1}/_{F_1}$ be the splitting fields of $f(x)$ and $f_1(x)$ respectively. Then, there exists an isomorphism $\psi : E \to E_1$ whcih extends ϕ.

Proof. Induction on $[E : F]$. If $[E : F] = 1$, then $f(x)$ is a product of linear factors in $F[x]$ and so is $f_1(x)$ in $F_1[x]$. Thus, $E = F$ and $E_1 = F_1$. Take $\psi = \phi$. We are done.
Suppose that $[E : F] > 1$ and the statement is true for all field extension ${}^{\tilde{E}}/_{\tilde{F}}$ with $[\tilde{E} : \tilde{F}] < [E : F]$. Let $p(x) \in F[x]$ be an irreducible factor of $f(x)$ with degree $\deg(p) \geq 2$ and let $p_1(x) = \Phi(p(x))$

(such $p(x)$ exists as if all irreducible factors of $f(x)$ are of 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. By Theorem 3, we have an F-isomorphism,

$$F(\alpha) \to F[x] \big/ \langle p(x) \rangle$$

$$\alpha \mapsto x + \langle p(x) \rangle$$

similarly, there is an F_1-isomorphism,

$$F_1(\alpha_1) \to F_1[x] \big/ \langle p_1(x) \rangle$$

$$\alpha_1 \mapsto x + \langle p_1(x) \rangle$$

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

$$\tilde{\Phi} : F[x] \big/ \langle p(x) \rangle \to F_1[x] \big/ \langle p_1(x) \rangle$$

$$x + \langle p(x) \rangle \mapsto x + \langle p_1(x) \rangle$$

which extends ϕ isomorphism. It follows that

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

$$\alpha \mapsto \alpha_1$$

which extends ϕ. Note that since $\deg(p) \geq 2$,

$$[E : F(\alpha)] < [E : F]$$

since E (respectively E_1) is the splitting field of $f(x) \in F(\alpha)[x]$ repsectively, $f_1(x) \in F_1(\alpha)[x]$. By induction, there exists $\psi : E \to E_1$, which extends $\tilde{\phi}$, so ψ extends ϕ. ■

Corollary 14 Any two splitting fields of $f(x) \in F[x]$ over F are F-isomorphic. Thus, we can now say **the** splitting field of $f(x)$ over F,

Proof. Let $\phi : F \to F_1$ be the identity map and apply theorem 13. ■

3.3 Degrees of Splitting Fields

Theorem 15 — (MIDTERM). Let F be a fields and $f(x) \in F[x]$ with degree $\deg(f) = n \geq 1$. If $E \big/ F$ is the splitting field of $f(x)$, then $[E:F] \big| n!$.

Proof. We prove this theorem by induction on $\deg(f)$. If $\deg(f) = 1$, choose $E = F$, and $[E:F] \big| 1!$. Suppose that $\deg(f) > 1$, and the statement holds for all polynomials $g(x)$ with $\deg(g) < \deg(f)$ ($g(x)$ is not necessarily in $F[x]$).

1. If $f(x) \in F[x]$ is irreducible and $\alpha \in E$ a root of $f(x)$, by Theorem 3, we have

$$F(\alpha) \cong F[x] \big/ \langle f(x) \rangle$$

and $[F(\alpha):F] = \deg(f) = n$. Write

$$f(x) = (x-\alpha)g(x), g(x) \in F(\alpha)[x]$$

since E is the splitting field of $g(x)$ over $F(\alpha)$ and $\deg(g) = n-1$, by induction hypothesis, $[E:F(\alpha)] \big| (n-1)!$. Since

$$[E:F] = [E:F(\alpha)][F(\alpha):F] \big| n!$$

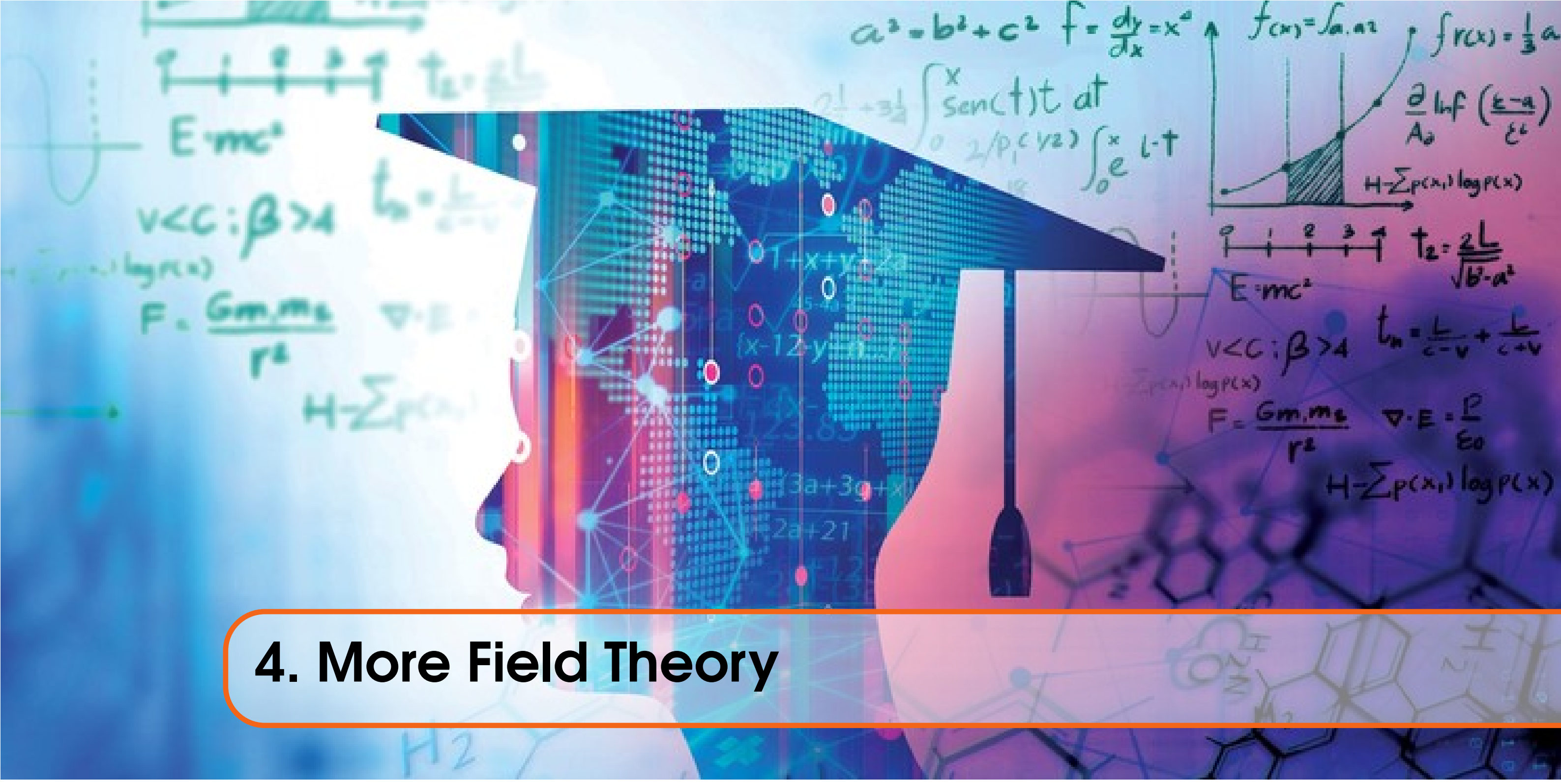
2. If $f(x)$ is not irreducible, $f(x) = g(x)h(x)$ for $g(x), h(x) \in F[x]$ with $\deg(g) = m < n, \deg(h) = k < n$ and $n = m + k$. Let K be the splitting field of $g(x)$ over F. Since $\deg(g) = m < n$, by induction $[K : F] \big| m!$. Similarly, since E is the splitting field of $h(x)$ over K and $\deg(h) = k < n$, by induction hypothesis, $[E : K] \big| k!$. Thus,

$$[E : F] \big| m!k!$$

But $m!k! | n!$ since

$$\frac{n!}{m!k!} = \binom{n}{k} \in \mathbb{Z}$$

■



4. More Field Theory

4.1 Prime Fields

Definition 4.1.1 — Prime Field. If F is a field, then the prime field of F is the intersection of all subfields of F. (???)

Theorem 16 If F is a field, then its prime filed is isomorphic to $\mathbb{Q}$ or $\mathbb{Z}_p$ for some prime number p.

Proof. Consider the $\chi : \mathbb{Z} \to F$ such that

$$n \mapsto n \cdot 1 = 1 + \cdots + 1, 1 \in F$$

Let $I = \ker \chi$. Then, $\mathbb{Z}/_I \cong \text{im}(\chi)$ by the First Isomorphism theorem, which is a subring of F, so it is an integral domain. So, I is a prime ideal. Two cases

1. If $I = \langle 0 \rangle$, then $\mathbb{Z} \subseteq F$ since F is a field

$$\mathbb{Q} = \text{Frac}(\mathbb{Z}) \subseteq F$$

2. If $I = \langle p \rangle$, then $\mathbb{Z}_p = \mathbb{Z} \big/ \langle p \rangle \cong \text{im}(\chi) \subseteq F$.

■

Definition 4.1.2 Given a field F, it its prime field is isomorphic to $\mathbb{Q}$, respectively $\mathbb{Z}_p$, we say F has characteristics 0, respectively characteristic p, denoted by

$$\text{ch}(F) = 0 \qquad\qquad (\text{ch}(F) = p)$$

R Note that if $\text{ch}(F) = p$ for $a, b \in F$, wee have have

$$(a+b)^p = a^p + b^P$$

using this property, we can show that

Proposition 17 — Exercise. Let F be a field with positive characteristics $\mathrm{ch}(F) = p$ and let $n \in \mathbb{N}$. Then, the map

$$\varphi : F \to F$$

given by $u \mapsto u^p$ is an injective $\mathbb{Z}_p$ homomorphism of fields. If F is finite, then φ is a $\mathbb{Z}_p$-isomorphism of F.

4.2 Formal Derivatives and Repeated Roots

Definition 4.2.1 — Formal Derivatives. If F is a field, the the monomials $\{1, x, x^2, \dots\}$ for an F-basis of $F[x]$. Define the linear operator $D : F[x] \to F[x]$ by $D(1) = 0$ and $D(x^i) = ix^{i-1}$ for all in $i \in \mathbb{N}$. Thus, for $f(x) = a_0 + a_1x + \cdots + a_nx^n, a_i \in F$, we have

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

Note that
1. $D(f+g) = D(f) + D(g)$
2. Leibniz Rule: $D(fg) = D(f)g + fD(g)$

We call $D(f) = f'$ the formal derivative of f.

Theorem 18 — (MIDTERM). Let F be a field and $f(x) \in F[x]$
1. If $\mathrm{ch}(F) = 0$, then $f'(x) = 0 \iff f(x) = c, c \in F$
2. If $\mathrm{ch}(F) = p$, then $f'(x) = 0 \iff f(x) = g(x^p), g(x) \in F[x]$

Proof. 1. ($\Longleftarrow$) is clear. We check ($\Longrightarrow$): if $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and

$$f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1} = 0 \to ia_i = 0, 1 \le i \le n$$

since $\mathrm{ch}(F) = 0$, we have $a_i = 0, \forall 1 \le i \le n$, so $f(x) = a_0 \in F$

2. ($\Longleftarrow$) Write $g(x) = b_0 + b_1x + \cdots + b_mx^m \in F[x]$, then

$$f(x) = g(x^p) = b_0 + b_1x^p + b_2x^{2p} + \cdots + b_mx^{mp}$$

thus,

$$f'(x) = pb_1x^{p-1} + 2pb_2x^{2p-1} + \cdots + mpb_mx^{pm-1}$$

since $\mathrm{ch}(F) = p$, we have $f'(x) = 0$

($\Longrightarrow$) For $f(x) = a_0 + a_1x + \cdots + a_nx^n$, $f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$ implies $ia_i = 0, 1 \le i \le n$. Since $\mathrm{ch}(F) = p$, $ia_i = 0$, this implies $a_i = 0$ unless $p|i$, thus,

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

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

■

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

Theorem 19 — (MIDTERM). 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 $(x-a)|f$ and $(x-a)|f'$, i.e., $(x-a)|\gcd(f, f')$.

Proof. 1. ($\Longrightarrow$) suppose that $f(x) = (x-\alpha)^2 g(x)$, then

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

Thus, $(x-\alpha)$ divides both of f and f'

2. ($\Longleftarrow$) suppose that $(x-\alpha)$ divides both f and f'. Say $f(x) = (x-\alpha)h(x), h(x) \in E[x]$. Then, $f'(x) = h(x) + (x-\alpha)h'(x)$. Since $f'(\alpha) = 0$, we have $h(\alpha) = 0$. Thus, $(x-\alpha)$ is a factor of $h(x)$ and $f(x) = (x-\alpha)^2 g(x)$ for some $g \in E[x]$.

■

Theorem 20 Let F be a field, $f(x) \in F[x]$. Then, $f(x)$ has no repeated root in any extension of F if and only if $\gcd(f, f') = 1$. (We remark that the condition of repeated roots depends on the extension of F, while the gcd condition involves only F)

Proof. Note that $\gcd(f, f') \neq 1 \iff (x-\alpha) | \gcd(f, f')$ for α in some extension of F. By Theorem 19, the result follows. ■

4.3 Finite Fields

Theorem 21 If F is a finite field, then $\mathrm{ch}(F) = p \neq 0$ for some prime number and $|F| = p^n$ for some $n \in \mathbb{N}$.

Proof. Since F is a finite field, by Theorem 16, its prime field is $\mathbb{Z}_p$. Since F is a finite dimensional vector space over $\mathbb{Z}_p$, we have $F \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ for some n times. Thus, $|F| = p^n$. ■

Theorem 22 Let F be a field and $F^\times = F \backslash \{0\}$ the multiplicative group of nonzero elements of F. Let G be a finite subgroup of $F^\times$. Then, G is a cyclic group. In particular, if F is a finite field, then $F^\times$ is a cyclic group.

Proof. WLOG, we can assume that G is non-trivial. Since G is a finite abelian group, we have $G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$ where $n_1 > 1$ and $n_1 | n_2 | n_3 | \ldots | n_r$. (This follows from Fundamental Theorem of Finitely Generated Abelian Groups, this is Theorem 3 Page 158 in DF). Since $n_r\left(\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/\mathbb{Z}_{n_r\mathbb{Z}}\right) = 0$, it follows that every $u \in G$ is a root of $x^{n_r} - 1 = 0$. (This is due to the isomorphism between the multiplicative group and the additive group). Since the polynomial $x^{n_r} - 1$ has at most n_r distinct roots in F. We have, $r = 1$ and $G \cong \mathbb{Z}/n_r\mathbb{Z}$ by dimensions of the isomorphism. ■

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

Corollary 23 If F is a finite field, then F is a simple extension of $\mathbb{Z}_p$. i.e. $F = \mathbb{Z}_p(u)$

Proposition 24 — (MIDTERM).

1. Let p be a prime number and $n \in \mathbb{N}$, then F is a finite field with $|F| = p^n$ if and only if F is the splitting field of

$$x^{p^n} - x$$

over $\mathbb{Z}_p$.

2. Let F be a finite field with $|F| = p^n$ for some $n \in \mathbb{N}$. Let $m \in \mathbb{N}$ with $m | n$. Then, F contains a unique subfield K with $|K| = p^m$.

Proof. 1. (a) ($\Longrightarrow$) If $|F| = p^n$, then $|F^\times| = p^n - 1$. Thus, every $u \in F^\times$ satisfies

$$u^{p^n-1} = 1$$

and thus it is a root of $x\left(x^{p^n-1} - 1\right) = x^{p^n} - x \in \mathbb{Z}_p[x]$. Since $0 \in F$ is a root of $x^{p^n} - x$, the polynomial $x^{p^n} - x$ has p^n distinct roots in F, i.e, F is the splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$.

(b) ($\Longleftarrow$) suppose that F is the splitting field of $f(x) = x^{p^n} - x$. Since $\operatorname{ch}(F) = p$, we have $f'(x) = -1$. Since $\gcd(f, f') = 1$, by Corollary 20, $f(x)$ has p^n distinct roots in F. Let E be the set of all roots of $f(x)$ in F. Let $\varphi : F \to F$ given by $u \mapsto u^{p^n}$.
For $u \in F$, u is a root of $f(x)$ if and only if $\varphi(u) = u$ since the condition is closed under addition, subtraction, multiplication, and 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 $u^p = u$ (FLT) and thus $u^{p^n} = u$). Since F is the splitting field of $f(x)$, it is generated over $\mathbb{Z}_p$ by the roots of $f(x)$, i.e, the elements in E. Thus, $F = \mathbb{Z}_p(E) = E$. Since $\mathbb{Z}_p$ is contained in E.

2. Observe that $x^{ab} - 1 = (x^a - 1)(x^{ab-a} + x^{ab-2a} + \cdots + x^a + 1)$. Then, if $n = mk$, then

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

for some $g(x) \in \mathbb{Z}_p[x]$. Since $x^{p^n} - x$ splits over F, so does $(x^p - x)$. Let $K = \{u \in F, u^{p^m} - u = 0\}$. Then, $|K| = p^m$ since the roots of $x^{p^m} - x$ are distinct. Also, by (1), K is a field. Note that if $\tilde{K} \subseteq F$ is any subfield of F with $|\tilde{K}| = p^m$ then $\tilde{K} \subseteq K$. Since $\tilde{K}$ is the splitting field of $x^{p^m} - x$, thus, K and $\tilde{K}$ have the same elements of roots. Thus, $K = \tilde{K}$.

■

Corollary 25 — L.H.Moore. Let p be a prime and $n \in \mathbb{N}$. Then, any two finite fields of order p^n are isomorphic. We denote such a field F by $\mathbb{F}_{p^n}$.

Proof. Follows from Proposition 24 and Corollary 14. ■

4.4 Separable Polynomial

Definition 4.4.1 — Separable Polynomial. Let F be a field and $f(x) \in F[x]$, $f(x) \neq 0$. If $f(x)$ is irreducible, we say $f(x)$ is separable over F if f 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 $\mathbb{Q}[x]$. ■

Exercise 4.1 Consider the polynomial $f(x) = x^n - a \in F[x]$ with $n \geq 2$.
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 $\operatorname{ch}(F) = 0$, then $\gcd(f, f') = 1$, thus, $f(x)$ is separable.
2. If $\operatorname{ch}(F) = p$ and $\gcd(n, p) = 1$, since $x \nmid f(x)$, then $\gcd(f, f') = 1$. Hence, $f(x)$ is separable.
3. If $\operatorname{ch}(F) = p$, consider $f(x) = x^p - a$. Since $f'(x) = px^{p-1} = 0$. We have $\gcd(f, f') \neq 1$. It is still possible that all irreducible factors $l(x)$ of $f(x)$ has the property that $\gcd(l, l') = 1$.

To decide if $f(x)$ is separable, we need to find its irreducible factors first. First, define

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

which is a subfield of F (like a subgroup with all the operations)

(a) 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 separable.

(b) If $a \notin F^p$,

Lemma 4.4.1 $f(x) = x^p - a$ is irreducible in $F[x]$.

Proof. Write $x^p - a = g(x)h(x)$ where $g(x), h(x)$ are monic polynomials. Let E/F be an extension where $x^p - a$ has a root, say $\beta \in E$. i.e. $\beta^p - a = 0$. Note that $\beta \notin F$ since $a = \beta^p \notin F^p$. 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 $r + s = p$. If we write

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

then, $r\beta \in F$ but $\beta \notin F$. Thus, this forces $r = 0$. As an integer, we have $r = 0$ or $r = p$. It follows that either $g(x) = 1$ or $h(x) = 1$ in $F[x]$. Thus, $f(x)$ is irreducible. ∎

By this lemma, since $f(x)$ is irreducible and $f(x) = (x-\beta)^p \in E[x]$, it is 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 Field. A field F is perfect if every (irreducible) polynomial $r(x) \in F[x]$ is separable over F.

Theorem 26 — (MIDTERM). Let F be a field

1. If $\mathrm{ch}(F) = 0$, then F is perfect
2. If $\mathrm{ch}(F) = p$ and $F^p = F$, then F is perfect

Proof. Let $r(x) \in F[x]$ be irreducible. Then,

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

suppose that $r(x)$ is not separable. Then, by Theorem 20, $\gcd(r, r') \neq 1$. Thus, $r'(x) = 0$.

1. If $\mathrm{ch}(F) = 0$, from Theorem 18, $r'(x) = 0 \iff r(x) = c \in F$. A contradiction since $\deg(r) \geq 1$. Thus, $r(x)$ is separable and F is perfect.
2. If $\mathrm{ch}(F) = p$, from Theorem 18, $r'(x) = 0 \iff f(x) = g(x^p)$, say

$$r(x) = a_0 + a_1 x^p + \dots + a_m x^{mp}, a_i \in F$$

since $F = F^p$, we can write $a_i = b_i^p$, $b_i \in F$. Thus,

$$r(x) = b_0^p + b_1^p x^p + \dots + b_m^p x^m = (b_0 + b_1 x + \dots + b_m x^m)^p$$

A contradiction since $r(x)$ is irreducible. Thus, $r(x)$ is separable and F is perfect.

■

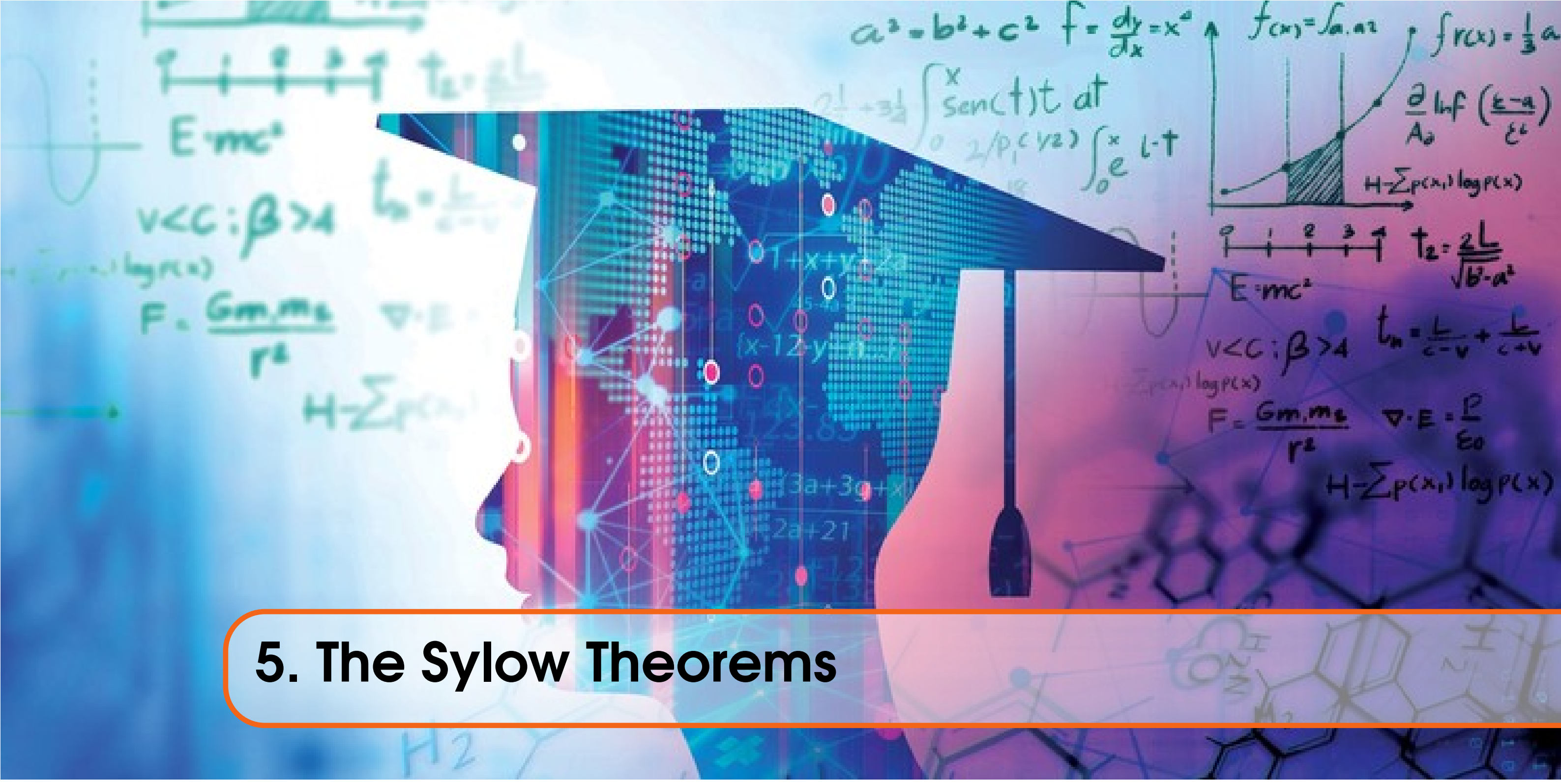
R Let $\mathrm{ch}(F) = p$ and $F^p \neq F$ (e.g. $F = \mathbb{F}_p(x)$). If we take $a \in F \backslash F^p$, then $x^p - a$ is purely inseparable. Thus, if $\mathrm{ch}(F) = p$, F is perfect if and only if $F^p = F$.

Corollary 27 — (MIDTERM). Every finite field is perfect.

Proof. Every finite field $F = \mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_{p^n}$ for some prime p and $n \in \mathbb{N}$. Thus, for every $a \in F$,

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

since $a^{p^{n-1}} \in F$ and $F = F^p$. By Theorem 26, F is perfect. ■



5. The Sylow Theorems

5.1 Back in the Group Days

Recall: Lagrange Theorem
If H is a subgroup of a group G, then

$$|G| = [G : H]|H|$$

In particular, if G is finite and $g \in G$, then $|\langle g \rangle| \big| |G|$

> **R** **Rever Question:**
> If $m \in \mathbb{N}$ with $m \big| |G|$, does G have a subgroup or an element of order m?

Definition 5.1.1 — Action, Orbit, Stablizer. An **action** of a group $GonasetS$ is a function $G \times S \to S$ (usually denoted by $(g,x) \mapsto gx$) such that for all $x \in S$ and $g_1, g_2 \in G$, we have

$$ex = x$$

and $(g_1 g_2)x = g_1(g_2 x)$ where e is the identity of G. If G acts on S, for $x \in S$, we denote $\bar{x}$ as the **orbit** of x.

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

Also, we denote G_x as the **stablizer** of x.

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

which is a subgroup of G and we have

$$|\bar{x}| = [G : G_x]$$

■ **Example 5.1** Let G be a group on itself by conjugation, i.e

$$(g,x) \mapsto gxg^{-1}$$

then for $x \in G$,

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

which is the **centralizer** of $x \in G$ (the elements in G that can commute with x). Let $Z(G)$ be the **centre** of G.

$$Z(G) = \left\{g \in G : gxg^{-1}, \forall x \in G\right\}$$

Note that for $x \in G$, we have $|\bar{x}| = 1 \iff x \in Z(G)$. Thus, we have the following **class equation of G**

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

where $x_i \in G \backslash Z(G)$, the orbits $\bar{x}_i = \left\{gx_ig^{-1} : g \in G\right\}$ are distinct conjugacy class of G and $|\bar{x}_i| = [G : C_G(x)] > 1$ for each i. ▪

Lemma 28 Let H be a group of order p^n where p is prime, acts on a finite set S. Let

$$S_0 = \{x \in S : hx = x, \forall h \in H\}$$

then, we have $|S| \equiv |S_0| \mod p$

Proof. For $x \in S$, $|\bar{x}| = 1 \iff x \in S_0$. Thus, S can be written as a disjoint union

$$S = S_0 \cup \bar{x}_1 \cup \bar{x}_2 \cup \cdots \cup \bar{x}_m$$

where $|\bar{x}_i| > 1$ for each i. Thus,

$$|S| = |S_0| + |\bar{x}_1| + \cdots + |\bar{x}_m|$$

since $|\bar{x}_i| > 1$ and $|\bar{x}_i| = [H : H_{x_i}]$ divides $|H| = p^n$. We have $p \big| |\bar{x}_i|$ for each i. It follows that $|S| \equiv |S_0| \mod p$. ■

Theorem 29 — Cauchy. Let p be a prime and G is a finite group. If $p \big| |G|$, then G contains an element of order p.

Proof. (J.Mckay) Define

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

Since a_p is unquely determind by $a_1, \ldots, a_{p-1}$, if $|G| = n$, we have $|S| = n^{p-1}$. Since $p \big| n$, we have

$$|S| \equiv 0 \mod p$$

Let the group $\mathbb{Z}_p = \mathbb{Z} \big/ \langle p \rangle$ acts on S by cyclic permutation, i.e, for $k \in \mathbb{Z}_p$

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

one can verify this action is well-defined. Also, $(a_1, \ldots, a_p) \in S_0$ if and only if $a_1 = a_2 = \cdots = a_p$. Clearly, $(e, e, \ldots, e) \in S_0$ and hence $|S_0| \geq 1$. By previous lemma 28, we have proved. We have

$$|S_0| \equiv |S| \equiv 0 \mod p$$

Since $|S_0| \geq 1$ and $|S_0| \equiv 0 \mod p$ (**THIS IS NICE!**), we have $|S_0| \geq 0$. Thus, there exists $a \neq e$ such that

$$(a, a, \ldots, a) \in S_0$$

which implies that $a^p = e$. Since p is a prime, the order of a is p. ■

R We see that we don't need G to be abelian since

$$a_1a_2 \ldots a_p = e = a_p^{-1}a_p \implies a_pa_1a_2 \ldots a_{p-1} = e = a_pa_p^{-1}$$

5.2 The Sylow Theorems

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

R As a direct consequence of Theorem 29, we have

Corollary 30 A finite group G is a p-group if and only if $|G|$ is a power of p.

Lemma 31 The centre $Z(G)$ of a non-trivial finite p-group G contains more than 1 element.

Proof. Since G is a p-group, by corollary 30, $|G|$ is a power of p. We recall the class equation of G

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

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

Definition 5.2.2 — Normalizer of H. We recall that if H is a subgroup of a group G, then

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

is the normalizer of H. In particular, $H \trianglelefteq N_G(H)$.

Lemma 32 If H is a p-subgroup of a finite subgroup G, then

$$[N_G(H) : H] \equiv [G : H] \mod p$$

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

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

Thus, $|S_0|$ is the number of cosets xH with $x \in N_G(H)$. Hence, $|S_0| = [N_G(H) : H]$. By Lemma 28, we have

$$[N_G(H) : H] = |S_0| \equiv |S| = [G : H] \mod p$$

■

Corollary 33 If H is a p-subgroup of a finite group G with $p \big| [G : H]$, then $N_G(H) \neq H$.

Proof. Since $p \big| [G : H]$, by Lemma 32, we have

$$[N_G(H) : H] \equiv [G : H] \equiv 0 \mod p$$

Since $p \big| [N_G(H) : H]$ and $[N_G(H) : H] \geq 1$, we have $[N_G(H) : H] \geq p$. Thus, $N_G(H) \neq H$. ■

Theorem 34 — 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 $1 \leq i \leq n$ and 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 $p \big| |G|$, by Theorem 29, G contains an element a of order p, i.e, $|\langle a \rangle| = p$. Suppose that the statement holds for some $1 \leq i < n$. Say H is a subgroup of G of order p^i. Then, we have $p \big| [G : H]$. We have seen in the proof of the corollary 33 that $p \big| [N_G(H) : H]$ and $[N_G(H) : H] \geq p$. Then, by Theorem 29, $N_G(H) \big/ H$ contains a subgroup of over p. Such a group if of the form $H_1 \big/ H$ where H_1 is a subgroup of $N_G(H)$ containing H since $H \trianglelefteq N_G(H)$, we have $H \trianglelefteq H_1$. Finally, $|H_1| = |H| \left| H_1 \big/ H \right| = p^i p = p^{i+1}$. ■

Definition 5.2.3 — Sylow P-Subgroup. A subgroup P of a group G is called a Sylow p-subgroup if P is maximal p-group. i.e, $P \subseteq H \subsetneq$ with H a p-group, then $P = H$.

As a direct consequence of Theorem 34, we have the following

Corollary 35 Let G be a group of order $p^n m$, where p is a prime and $n \geq 1$ and $\gcd(p,m) = 1$. Let H be p-subgroup of G. Then,

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. (gHg^{-1})
3. If there is only one Sylow p-subgroup P, then $P \trianglelefteq G$.

Theorem 36 — 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 particular, any two Sylow p-subgroups 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 28, we have $|S_0| \equiv |S| \equiv [G : P] \mod p$. Since $p \nmid [G : P]$, we have $S_0 \neq \{0\}$. Thus, there exists $xP \in S_0$ for some $x \in G$ and note that

$$xP \in S_0 \iff hxP = xP, \forall h \in H \iff x^{-1}hxP = P, \forall h \in H \iff x^{-1}Hx \subseteq P \iff H \subseteq xPx^{-1}$$

In particular, when H is also a Sylow p-subgroup, then $|H| = |P| = |xPx^{-1}|$. Thus,

$$H = xPx^{-1}$$

■

Theorem 37 — Third Sylow Theorem. If G is a finite group and p is a prime, 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 36, 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 acts of S by conjugation. Then, $Q \in S_0 \iff xQx^{-1} = Q$ for all $x \in P$. The later condition holds if and only if $P \subseteq N_G(Q)$. Both P, Q are Sylow p-subgroups of G and hence of $N_G(Q)$. Thus, by Corollary 35, they are conjugate in $N_G(Q)$. Since $Q \trianglelefteq N_G(Q)$, this can only occur if $Q = P$. Thus, $S_0 = \{P\}$. Then, by Lemma 28, $|S| \equiv |S_0| \equiv 1 \mod p$. Thus, the number of Sylow p-subgroups is of the form $kp + 1$ for some $k \in \mathbb{N} \cup \{0\}$. ■

R Suppose that G is a group with $|G| = p^n m$ and $\gcd(p,m) = 1$. The n_p be the number of Sylow p-subgroups of G. By the Third Sylow Theorem, we have $n_p \big| p^n m$ and $n_p \equiv 1 \mod p$. Since $p \nmid n_p$. We must have $n_p \big| m$.

■ **Example 5.2** **Claim:** every group of order 15 is cyclic.
Let G be a group of order $15 = 3 \times 5$. Let n_p be the number of Sylow p-subgroup of G. By the Third Sylow Theorem, we have $n_3 \big| 5$ and $n_3 \equiv 1 \mod 3$. Thus, $n_3 = 1$. Similarly, we have $n_5 \big| 3$ and $n_5 \equiv 1 \mod 5$. Thus, $n_5 = 1$. It follows taht there is only one Sylow 3-group and Sylow 5-group of G, say P_3 and P_5 respectively. Thus, $P_3 \trianglelefteq G$ and $P_5 \trianglelefteq G$. Now, consider $|P_3 \cap P_5|$ which divides 3 and 5. Thus, $|P_3 \cap P_5| = 1$. Also, $|P_3 P_5| = |G| = 15$. It follows that

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

■

R **Correction of A3 Q3 replace** 225 **by** 175

■ **Example 5.3** **Claim:** there are two isomorphism classes of group of order 21.
Let G be a group of order $21 = 3 \times 7$. Let n_p be the number of Sylow p-subgroup of G. By the Third Sylow Theorem, wee have $n_3 \big| 7$ and $n_3 \equiv 1 \mod 3$. Thus, $n_3 = 1$ or 7. Also, $n_7 \big| 3$ and $n_7 \equiv 1 \mod 7$. Thus, $n_7 = 1$. It follows that G has a unique Sylow p-subgroup, say P_7. Note that $P_7 \trianglelefteq G$ and P_7 is cyclic, say $P_7 = \langle x\rangle$ with $x^7 = 1$. Let H be a Sylow 3-subgroup and $|H| = 3$. Thus, H is cyclic and $H = \langle y\rangle$ with $y^3 = 1$. Since $P_7 \trianglelefteq G$, we have $yxy^{-1} = x^i$ for some $0 \le i \le 6$. It follows that (since $y^3 = 1$)

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

Since $x^7 = 1$, we have $1 \mod i^3 \mod 7$. Since $0 \le i \le 6$, we jave $i = 1, 2, 4$.

1. If $i = 1$, then $yxy^{-1} = x$, i.e, $xy = yx$. Thus, G is abelian and $G \cong \mathbb{Z}\big/\langle 21\rangle$.
2. If $i = 2$, then $yxy^{-1} = x^2$. Thus, $G = \left\{x^i y^j : 0 \le i \le 6, 0 \le j \le 2, yxy^{-1} = x^2\right\}$.
3. If $i = 4$, then $yxy^{-1} = x^4$. Thus, $G = \left\{x^i y^j : 0 \le i \le 6, 0 \le j \le 2, yxy^{-1} = x^4\right\}$. Note that $y^2 x y^{-2} = y x^4 y^{-1} = x^{16} = x^2$. Note that y^2 is also a generator of H. Thus, by replacing y be y^2, we get back to case 2.

Thus, it follows that there are two isomorphism classes of groups of order 21. ■

6. Solvable Groups

6.1 Introduction

Definition 6.1.1 — Solvable Group. A group G is solvable if there exists a tower

$$G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_m = \{1\}$$

with $G_{i+1} \trianglelefteq G_i$ and ${G_i}/{G_{i+1}}$ is abelian for $0 \leq i \leq m-1$.

R G_{i+1} is not necessarily a normal subgroup.

■ **Example 6.1** Consider of the 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 subgroups 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. ■

Recall: Second & Third Isomorphism Theorem

Theorem 6.1.1 — Second Isomorphism Theorem. If H and N are subgroups of G with $N \trianglelefteq G$, then

$$H/H\cap N \cong NH/N$$

Theorem 6.1.2 — Third Isomorphism Theorem. If H and N are normal subgroups of G such that $N \subsetneq H$, then have $H/N \trianglelefteq G/N$ and

$$\left. {G/N} \middle/ {H/N} \right. \cong G/H$$

Theorem 38 1. If G is a solvable group, every subgroup and every quotient group of G is solvable.
2. Conversely, if N is a normal subgroup of a group G and with N and G/N are solvable, then G is solvable. In particular, a direct product of finitely many solvable groups if solvable.

Proof. 1. Suppose that G is a solvable group with a tower

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_m = \{1\}$$

where $G_{i+1} \trianglelefteq G_i$ and G_i/G_{i+1} is abelian.

(a) **Claim:** let H be subgroup of G, then H is solvable.

Proof. Define $H_i = H \cap G_i$. Since $G_{i+1} \trianglelefteq G_i$, we have a tower

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

and $H_{i+1} \trianglelefteq H_i$. Note that both H_i and G_{i+1} are both subgroups 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

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

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

(b) **Claim:** let N be a normal subgroup of G, then G/N is solvable.

Proof. Consider the tower,

$$G = G_0N \supseteq G_1N \supseteq G_2N \supseteq \cdots \supseteq G_mN = N$$

and

$$G/N = G_0N/N \supseteq G_1N/N \supseteq \cdots \supseteq G_mN/N = \{1\}$$

since $G_{i+1} \trianglelefteq G_i$ and $N \trianglelefteq G$, we have $G_{i+1}N \trianglelefteq G_iN$, which implies that $G_{i+1}N/N \trianglelefteq G_iN/N$. By the Third Isomorphism Theorem, we have

$$G_iN/N \Big/ G_{i+1}N/N \cong G_iN/G_{i+1}N$$

by the Second Isomorphsim Theorem, we have

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

since $G_{i+1} \subsetneq G_i \cap G_{i+1}N$, there is a natural injection

$$G_i/G_i \cap G_{i+1}N \to G_i/G_{i+1}, g + (G_i \cap G_{i+1}N) \mapsto g + G_{i+1}$$

Since G_i/G_{i+1} is abelian, so it $G_i/G_i \cap G_{i+1}N$. Thus,

$$G_iN/N \Big/ G_{i+1}N/N$$

is abelian. It follows that G/N is solvable. ■

■

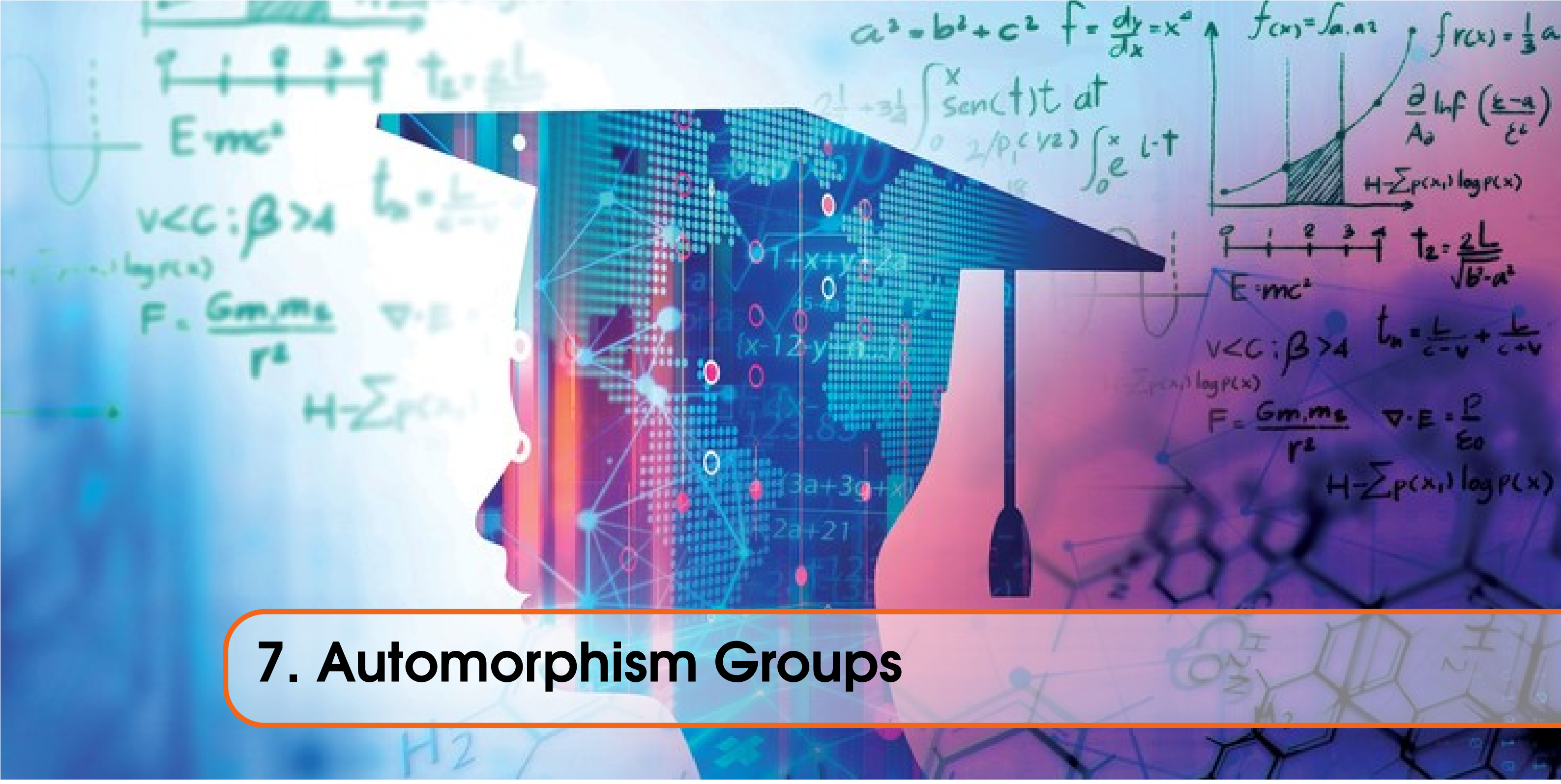
■ **Example 6.2** We have S_4 contains subgroups isomorphic to S_3 and S_2. Since S_4 is solvable, we have S_3 and S_2 are also solvable. ■

6.1.1 Simple Group

Definition 6.1.2 — Simple Group. A group G is simple if it is not trivial and has no normal subgroup except G and $\{1\}$.

■ **Example 6.3** One can show that A_5 is simple. Since $A_5 \geq 1$ is the only tower and $A_5 / \{1\}$ is not abelian, thus, A_5 is not solvable. Thus, by Theorem 38, S_5 is also not solvable. Moreover, since for $n \geq 5$, all S_n contains S_5, we have S_n is not solvable for $n \geq 5$. ■

Corollary 39 G is a finite solvable group if and only if there exists a tower $G = G_0 \leq G_1 \leq \cdots \leq G_m = \{1\}$ with $G_{i+1} \trianglelefteq G_i$ and G_i / G_{i+1} is a cyclic group of prime order for each i.



7. Automorphism Groups

7.1 Automorphism Groups

Definition 7.1.1 — Automorphism of E. Let ${}^{E}/_{F}$ be a field extension. If ψ is an automorphism of E and $\psi|_F = 1_F$, we say ψ is an F-automorphism of E.

> **R** We see F-automorphism of E forms a subgroup of automorphism group of E.

Definition 7.1.2 — Automophism Group of ${}^{E}/_{F}$. We call the group

$$\mathbf{Aut}_F(E) := \{\text{F-Automorphism of } E\}$$

to be the automorphism group of ${}^{E}/_{F}$.

Lemma 40 Let ${}^{E}/_{F}$ be a field extension, $f(x) \in F[x]$ and $\psi \in \mathbf{Aut}_F(E)$. If $\alpha \in E$ is a root of $f(x)$, then $\psi(\alpha)$ is a root of $f(x)$.

Proof. Say $f(x) = \sum_{i=0}^{n} a_i x^i$. We have

$$f(\psi(\alpha)) = \sum_{i=0}^{n} a_i \psi(\alpha)^i = \psi\left(\sum_{i=0}^{n} a_i \alpha^i\right) = \psi(0) = 0$$

∎

Lemma 41 Let $E = F(\alpha_1, \ldots, \alpha_n)$, for $\phi_1, \phi_2 \in \mathbf{Aut}_F(E)$, if $\phi_1(\alpha_i) = \phi_2(\alpha_i)$ for all i, then $\phi_1 = \phi_2$.

Proof. Note that for $\alpha \in E$, we have

$$\alpha = \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)}$$

where $f, g \in F[x_1, \ldots, x_n]$. Thus, the lemma follows. ∎

Corollary 42 If ${}^{E}/_{F}$ is a finite extension, then $\textbf{Aut}_F(E)$ is finite.

Proof. Since ${}^{E}/_{F}$ is a finite extension, by Theorem 5, we have $E = F(\alpha_1, \dots, \alpha_n)$ where α_i are algebraic over F. For $\phi \in \textbf{Aut}_F(E)$, by Lemma 40, we must have $\phi(\alpha_i)$ is a root of the minimal polynomial of α_i.
Thus, it has only finitely many choices. By Lemma 41, since $\phi \in \textbf{Aut}_F(E)$ is completely determined by $\phi(\alpha_i)$, there are only finitely many choices of ϕ and $|\textbf{Aut}_F(E)| < \infty$. ■

R The converse of the above corollary is false. For example ${}^{\mathbb{R}}/_{\mathbb{Q}}$ is an infinite extension but one can show $\textbf{Aut}_{\mathbb{Q}}(\mathbb{R}) = \{1\}$ as $\mathbb{Q}$ is dense in $\mathbb{R}$.

Definition 7.1.3 — Automorphism group of $f(x)$ over F. Let F be a field and $f \in F[x]$. The automorphism of $f(x)$ over F is $\textbf{Aut}_F(E)$ where E is the splitting field of F.

Theorem 43 Let $0 \neq f \in F[x]$ and E be the splitting field of f. We have $|\textbf{Aut}_F(E)| \leq [E:F]$ and equality holds if and only if $f(x)$ is separable.

Proof. This is an immediate results from Assignment 2 Q3. ■

■ **Example 7.1** Let F be field with $\text{ch}(F) = p$ and $F^p \neq F$ and $f(x) = x^p - a$ with $a \in F \backslash F^p$. Let ${}^{E}/_{F}$ be the splitting field of $f(x)$. We have seen before that $f(x) = (x - \beta)^p$ with $\beta \in {}^{E}/_{F}$. Thus, $E = F(\beta)$. Since β can only map to β, $\textbf{Aut}_F(E)$ is trivial. Note that

$$|\textbf{Aut}_F(E)| = 1 \text{ while } [E:F] = p$$

We have $|\textbf{Aut}_F(E)| \neq [E:F]$ since $f(x)$ is not separable. ■

Theorem 44 If $f(x) \in F[x]$ has n distinct roots in the splitting field E. Then, $\textbf{Aut}_F(E)$ is isomorphism to a subgroup of the symmetric group S_n. In particular, $|\textbf{Aut}_F(E)|\big| n!$.

Proof. Let $X = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ be distinct roots of $f(x)$ in E. By Lemma 40, if $\psi \in \textbf{Aut}_F(E)$, then $\psi(X) = X$. Let $\psi\big|_X$ be the restriction of ψ in X and S_X, the permutation group of X. The map

$$\textbf{Aut}_F(E) \longrightarrow S_X \cong S_n, \psi \mapsto \psi\big|_X$$

is a group homorphism. Moreover, by Lemma 41, it is injective. Thus, $\textbf{Aut}_F(E)$ is a subgroup of S_n. ■

■ **Example 7.2** Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ and ${}^{E}/_{\mathbb{Q}}$ be the splitting field of $f(x)$. Thus, $E = \mathbb{Q}(\sqrt[3]{2}, U_3)$ where U_3 is the 3rd root of unity and $[E:F] = 6$. $\text{ch}(\mathbb{Q}) = 0$, $f(x)$ is separable. By Theorem 43,

$$|\textbf{Aut}_{\mathbb{Q}}(E)| = [E:F] = 6$$

Also, since $f(x)$ has 3 distinct roots in E, by Theorem 44, $\textbf{Aut}_{\mathbb{Q}}(E)$ is a subgroup of S_3. It follows that $\textbf{Aut}_{\mathbb{Q}}(E) \cong S_3$. ■

7.2 Fixed Fields

Definition 7.2.1 — Fixed Field. Let E/F be the field extension and $\psi \in \mathbf{Aut}_F(E)$. Define

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

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

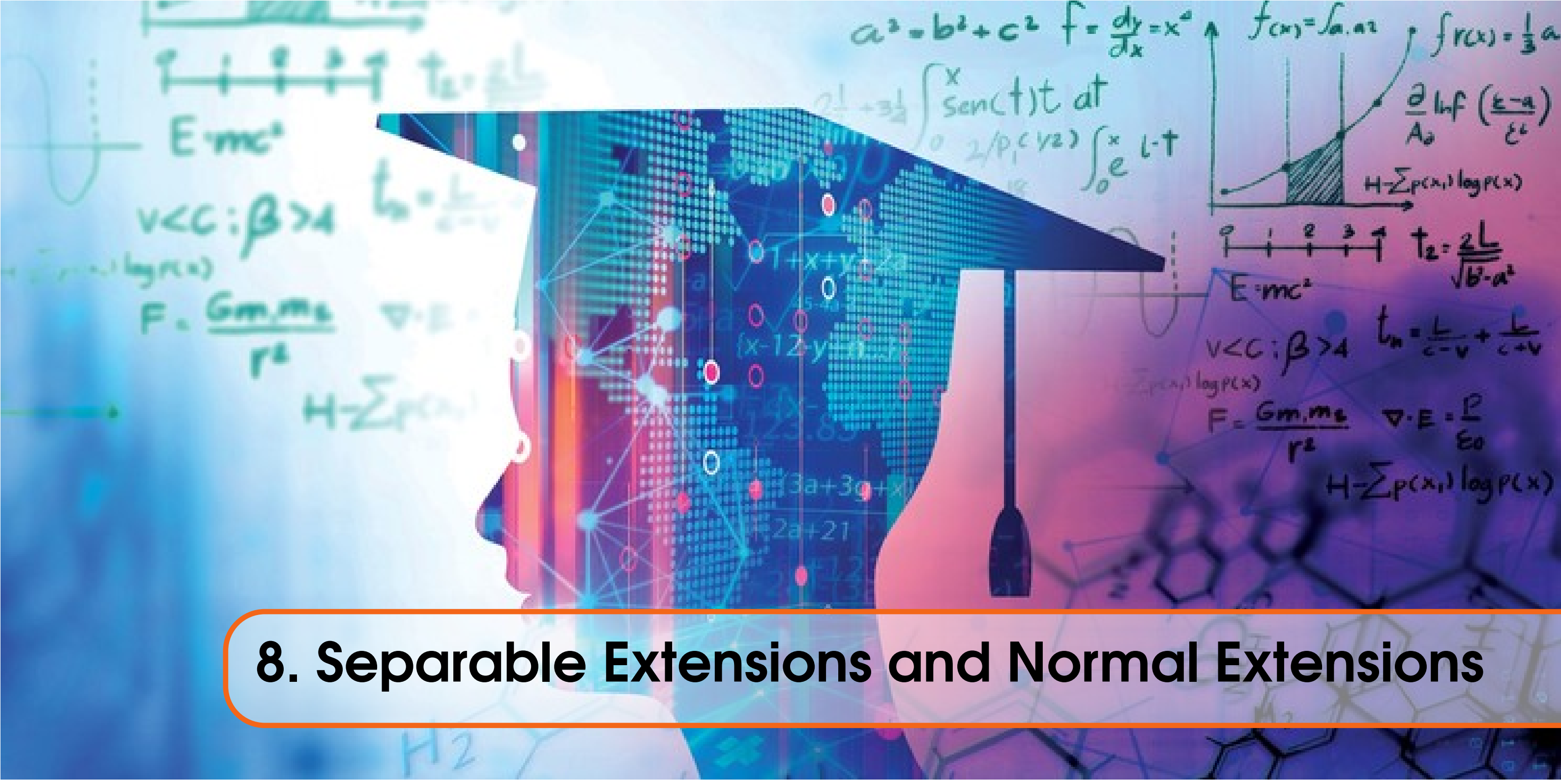
$$E^G := \bigcap_{\psi \in G} E^{\psi} = \{a \in E : \psi(a) = a, \forall \psi \in G\}$$

Theorem 45 Let $f(x) \in F[x]$ be a separable polynomial and E/F is its splitting field. If $G = \mathbf{Aut}_F(E)$, then $E^G = F$.

Proof. Set $L = E^G$. Since $F \subseteq L$, we have $\mathbf{Aut}_L(E) \subseteq \mathbf{Aut}_F(E)$. On the other hand, if $\psi \in \mathbf{Aut}_F(E)$, by the definition of L, for all $a \in L$, we have $\psi(a) = a$. This implies that $\psi \in \mathbf{Aut}_L(E)$. Thus, $\mathbf{Aut}_F(E) = \mathbf{Aut}_L(E)$. Note that since $f(x)$ is separable over F and splits over E. $f(x)$ is also separable over L and has E as its splitting field over L. Thus, by Theorem 43, $|\mathbf{Aut}_F(E)| = [E : F]$ and $|\mathbf{Aut}_L(E)| = [E : L]$. It follows that $[E : F] = [E : L]$. Since $[E : F] = [E : L][L : F]$, we have $[L : F] = 1$. Thus,

$$E^G = L = F$$

■



8. Separable Extensions and Normal Extensions

8.1 Separable Extensions

Definition 8.1.1 — Separable Extension. Let ${}^{E}/_{F}$ be an **algebraic** extension of F. 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 $\mathrm{ch}(F) = 0$, by Theorem 26, F is perfect, which means every polynomial $f(x) \in F[x]$ is separable. Thus, if $\mathrm{ch}(F) = 0$, any algebraic extension ${}^{E}/_{F}$ is separable. ■

Theorem 46 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 $p(x) \in F[x]$ is the minimal polynomial of α. And let $\{\alpha = \alpha_1, \alpha_2, \dots, \alpha_n\}$ be the distinct roots of $p(x)$ in E. **Claim:** $\tilde{p}(x) = (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n) \in F[x]$

Proof. Let $G = \mathbf{Aut}_F(E)$ and $\phi \in G$. Since ϕ is an automorphism. We have $\phi(\alpha_i) \neq \phi(\alpha_j)$ if $i \neq j$. Thus, by Lemma 40, ϕ permutes $\alpha_1, \alpha_2, \dots, \alpha_n$. Thus, we have

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

It follows that $\tilde{p}(x) \in E^{\phi}[x]$.
Since $\phi \in G$ is arbitrary $\tilde{p}(x) \in E^{G}[x]$. Since ${}^{E}/_{F}$ is the splitting field of the separable polynomial $f(x)$. By Theorem 45, $\tilde{p}(x) \in F[x]$. Thus, the claim holds. ■

Therefore, we have $\tilde{p}(x) \in F[x]$ with $\tilde{p}(\alpha) = 0$. Since $p(x)$ is the minimal polynomial over F, we have $p(x) \big| \tilde{p}(x)$. Also, since $\alpha_1, \dots, \alpha_n$ are all distinct roots of $p(x)$, we have $\tilde{p}(x) \big| p(x)$. Since both $p(x), \tilde{p}(x)$ are monic, we have $p(x) = \tilde{p}(x)$. It follows that $p(x)$ is separable. ■

Corollary 47 Let E/F be a finite extension and $E = F(\alpha_1, \dots, \alpha_n)$. If each α_i is separable over F $(1 \le i \le n)$, then E/F is separable.

Proof. Let $p_i(x) \in F[x]$ be the minimal polynomial of α_i $(1 \le i \le n)$. Let

$$f(x) = p_1(x) \dots p_n(x)$$

Since each $p_i(x)$ is separable, so is $f(x)$. Let L be the splitting field of $f(x)$ over F. By Theorem 46, L/F is separable. Since $E = F(\alpha_1, \dots, \alpha_n)$ is a subfield of L, E/F is also separable. ■

Corollary 48 Let E/F be an algebraic extension and L be the set of all $\alpha \in E$ which are separable. Then, L is an intermediate field.

Proof. Let $\alpha, \beta \in L$, then $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta}, (\beta \neq 0) \in F(\alpha, \beta)$. By Corollary 47, $F(\alpha, \beta)$ is separable and hence it is contained in L. Thus, $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta}, (\beta \neq 0) \in L$. ■

8.1.1 Simple Extension

Definition 8.1.2 — Simple Extension. If $E = F(\alpha)$ is a simple extension, we say α is a primitive element of E/F

Theorem 49 — Primitive Element Theorem. If E/F is a finite separable extension, then $E = F(\gamma)$ for some $\gamma \in E$. In particular, $\text{ch}(F) = 0$, then any finite extension E/F is a simple extension.

Proof. We have seen in Corollary 23 that a finite extension a finite field is always simple. Thus, WLOG, we assume F is an infinite field.
Since $E = F(\alpha_1, \dots, \alpha_n)$ for some $\alpha_1, \dots, \alpha_n \in E$. It suffices to consider the case when $E = F(\alpha, \beta)$. The general case is done by induction.
Let $E = F(\alpha, \beta)$ and $\alpha, \beta \notin F$. **Claim:** there exists $\lambda \in F$ such that $\gamma = \alpha + \lambda\beta$ and $\beta \in F(\gamma)$.

Proof. Let $a(x), b(x)$ be the minimal polynomial of α, β over F. Since $\beta \notin F$, $\deg(b) > 1$. Thus, there exists a root $\tilde{\beta}$ of $b(x)$ such that $\tilde{b} \neq \beta$. Choose any $\lambda \in F$ such that $\lambda \neq \frac{\tilde{\alpha} - \alpha}{\beta - \tilde{\beta}}$ for all roots $\tilde{\alpha}$ of $a(x)$ and for all rootf of $\tilde{\beta}$ of $b(x)$ with $\tilde{\beta} \neq \beta$ (This is possible since F is an infinite field, but finitely many choices for $\tilde{\alpha}, \tilde{\beta}$) in some splitting field of $a(x), b(x)$ over F. Let

$$\gamma = \alpha + \lambda\beta$$

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

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

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

$$\gamma - \lambda\tilde{\beta} = \alpha + \lambda(\beta - \tilde{\beta}) \neq \tilde{\alpha}$$

by the choice of λ. We have $h(\tilde{\beta}) = a(\gamma - \lambda\tilde{\beta}) \neq 0, \forall \tilde{\beta} \neq \beta$. Thus, $h(x), b(x)$ 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, $b_1 | b, b_1 | h$. 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 $h(x), b(x)$ have only β as a common root, $b_1(x) = x - \beta$. Since $b_1(x) \in F(\gamma)[x]$, we have $\beta \in F(\gamma)$ as required. ■

Given the above lemma, we have $\alpha = \gamma - \lambda\beta \in F(\gamma)$ and we have $F(\alpha,\beta) \subseteq F(\gamma)$. Also, since $\gamma = \alpha + \lambda\beta$, $F(\gamma) \subseteq E(\alpha,\beta)$. Thus,

$$E = F(\alpha,\beta) = F(\gamma)$$

■

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, then $p(x)$ splits over E.

■ **Example 8.2** Let $\alpha \in \mathbb{R}$ with $\alpha^4 = 5$. Since the roots of $x^4 - 5$ are $\pm\alpha$ and $\pm i\alpha$, and $\mathbb{Q}(\alpha)$ is real, then ${}^{\mathbb{Q}(\alpha)}/_{\mathbb{Q}}$ is not normal. (Can use Eisenstein to show irreducibility) Let $\beta = (1+i)\alpha$.
Claim: ${}^{\mathbb{Q}(\beta)}/_{\mathbb{Q}}$ is not normal.

Proof. Note that $\beta^2 = 2i\alpha^2$ and $\beta^4 = -4\alpha^4 = -20$. 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 $\pm\beta, \pm i\beta$. 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 $[\mathbb{Q}(\beta) : \mathbb{Q}] = 4$. This implies that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$, which is not possible since $\beta = \alpha + i\alpha \notin \mathbb{Q}(\alpha)$. Thus, $\alpha \notin \mathbb{Q}(\beta)$ and it implies that $i \notin \mathbb{Q}(\beta)$ since $\alpha = \frac{\beta}{1+i}$. It follows that the factorization of $p(x)$ over $\mathbb{Q}(\beta)$ is

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

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

■

Theorem 50 A **finite** extension ${}^{E}/_{F}$ is normal if and only if it is the splitting field of some $f(x) \in F[x]$.

Proof.
1. $\Longrightarrow$: suppose that ${}^{E}/_{F}$ is normal. Write $E = F(\alpha_1, \ldots, \alpha_n)$. Let $p_i(x) \in F[x]$ be the minimal polynomial of $\alpha_i (1 \le i \le n)$. Define

$$f(x) = p_1(x) \ldots p_n(x)$$

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

$$\begin{aligned} E &= F(\alpha_1, \ldots, \alpha_n) \\ &= F(\alpha_{1,1}, \ldots, \alpha_{1,r_1}, \alpha_{2,2}, \ldots, \alpha_{2,r_2}, \ldots, \alpha_{n,n}, \ldots, \alpha_{n,r_n}) \end{aligned}$$

which is the splitting field of $f(x)$ over F.
2. $\Longleftarrow$: 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. Write

$$p(x) = c(x-\alpha_1)\ldots(x-\alpha_n)$$

$$\begin{tikzcd}
K \arrow[r, "\psi", "extend\theta"'] \arrow[d, dash] & B \arrow[dd, dash] \\
E \arrow[d, dash] & \\
F(\alpha) \arrow[r, "\theta", "F-IM"'] \arrow[d, dash] & F(\alpha_2) \arrow[d, dash] \\
F \arrow[r, "1"] & F
\end{tikzcd}$$

Figure 8.2.1: *Proof Outline*

where $0 \neq c \in F$, $\alpha = \alpha_1 \in E$, $\alpha_2, \dots \alpha_n \in K = E(\alpha_1, \dots, \alpha_n)$. Since $F(\alpha) \cong F[x] \big/ \langle p(x) \rangle$, we have F-isomorphism

$$\theta : F(\alpha_1) \to F[\alpha_2], \theta(\alpha) = \alpha_2$$

Note taht $p(x)f(x) \in F[x] \subseteq F(\alpha)[x]$ and $p(x)f(x) \in F(\alpha_2)[x]$. Thus, we can view K as the splitting field of $p(x)f(x)$ over $F(\alpha)$ and $F(\alpha_2)$ respectively. Thus, by Theorem 13, there exists an isomorphism $\psi : K \to K$ which extends θ. In particular, $\psi \in \mathbf{Aut}_F(K)$ Since $\psi \in \mathbf{Aut}_F(K)$, ψ will permute the roots of $f(x)$. Since E is generated over F by the roots of $f(x)$. By lemma 40, 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 all $2 \leq i \leq n$. Thus, $K = E$ and $p(x)$ splits over E. It follows that $E \big/ F$ is normal.

■

■ **Example 8.3** **Claim:** every quadratic extension is normal.

Proof. Let $E \big/ F$ be a field extension with $[E : F] = 2$. For $\alpha \in E \big/ F$, we must have $E = F(\alpha)$. Let $p(x) = x^2 + ax + b$ be the minimal polynomial of α over F. If β is another roots of $p(x)$, then

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

Thus, $\beta = \frac{b}{\alpha}$ (or $\beta = -a - \alpha$) is the other root of $p(x)$ and the splitting field of $p(x)$ is $F\left(\alpha, \frac{a}{\alpha}\right) = F(\alpha) = E$. Since $E \big/ F$ is the splitting field of $p(x)$ over F, by Theorem 50, it is normal. ■

■

■ **Example 8.4** The extension $\mathbb{Q}\left(\sqrt[4]{2}\right) \big/ \mathbb{Q}$ is not normal since the irreducible polynomial $x^4 - 2$ 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 $\mathbb{Q}\left(\sqrt[4]{2}\right) \big/ \mathbb{Q}$ is made up of two quadratic extensions $\mathbb{Q}\left(\sqrt[4]{2}\right) \big/ \mathbb{Q}(\sqrt{2})$, and $\mathbb{Q}\left(\sqrt{2}\right) \big/ \mathbb{Q}$, which are normal. Thus, if $E \big/ K$ and $K \big/ F$ are normal extension, then $E \big/ F$ is not necessarily normal. ■

Proposition 51 If $E \big/ F$ is a normal extension and K is an intermediate field, then $E \big/ K$ 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. Thus, $p(x) \big| f(x)$. Since $E \big/ F$ is normal, $f(x)$ splits over E, so does $p(x)$. Thus, $E \big/ K$ is a normal extension. ■

R Take $F=\mathbb{Q}$ and $K=\mathbb{Q}\left(\sqrt[4]{2}\right)$ and $E=\mathbb{Q}\left(\sqrt[4]{2},i\right)$, then ${}^{E}\!/_{F}$ is normal and so is ${}^{E}\!/_{K}$. However, ${}^{K}\!/_{F}$ is not normal.

Proposition 52 Let ${}^{E}\!/_{F}$ be a finite normal extension and $\alpha,\beta\in E$, TFAE:
1. There exists $\psi\in\mathbf{Aut}_F(E)$ such that $\psi(\alpha)=\beta$
2. Th minimal polynomial of α and β over F are the same. In this case, we say α and β are **conjugate over** F

Proof.
1. $\Longrightarrow$: let $p(x)$ be the minimal polynomial of α over F and $\psi\in\mathbf{Aut}_F(E)$ with $\psi(\alpha)=\beta$. By Lemma 40, β is also a root of $p(x)$, but $p(x)$ is monic and irreducible, it is the minimal polynomial of β over F. Thus, α and β have the same minimal polynomial.
2. $\Longleftarrow$: Suppose that the minimal polynomial of α,β are the same and it is $p(x)$. Since $F(\alpha)\cong {}^{F[x]}\!\big/_{\langle p(x)\rangle}\cong F(\beta)$, 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 50, 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. Thus, by Theorem 13, there exists an isomorphism $\psi:E\to E$ which extends θ. It follows that $\psi\in\mathbf{Aut}_F(E)$ and $\psi(\alpha)=\beta$.

■

■ **Example 8.5** The complex numbers $\sqrt[3]{2},\sqrt[3]{2}U_3,\sqrt[3]{2}U_3^2$, where $U_3=e^{\frac{2\pi i}{3}}$ are all conjugates over $\mathbb{Q}$ since they are roots of the irreducible polynomial $x^3-2\in\mathbb{Q}[x]$. ■

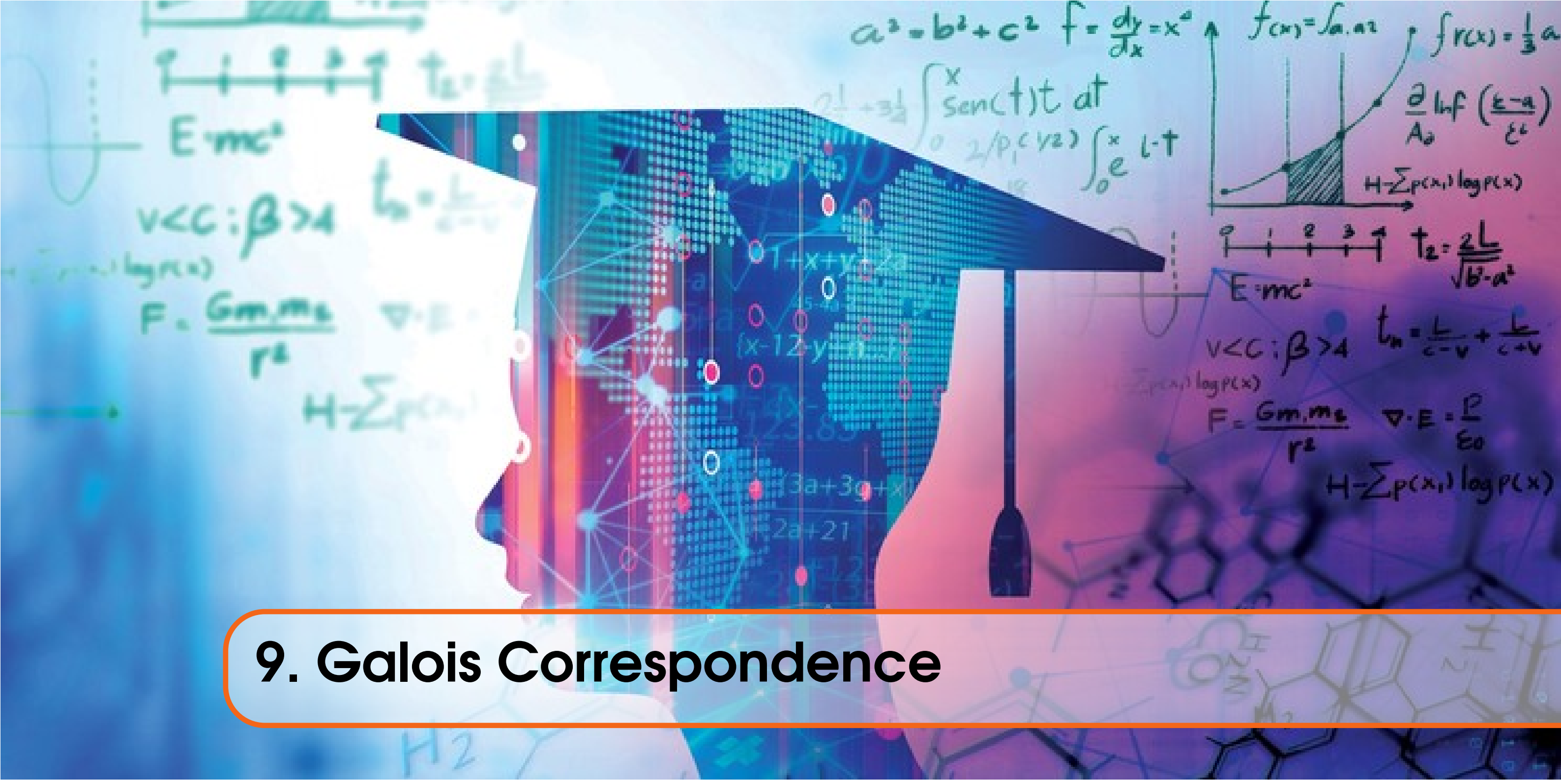
Definition 8.2.2 — Normal Closure. A normal closure of a finite extension ${}^{E}\!/_{F}$ is a finite normal extension ${}^{N}\!/_{F}$ satisfying the following properties:
1. E is a subfield of N
2. Let L be an intermediate field of ${}^{N}\!/_{E}$. If L is normal over L, then $L=N$.

■ **Example 8.6** The normal closure of ${}^{\mathbb{Q}\left(\sqrt[3]{2}\right)}\!/_{\mathbb{Q}}$ is ${}^{\mathbb{Q}\left(\sqrt[3]{2},U_3\right)}\!/_{\mathbb{Q}}$. ■

Theorem 53 Every finite extension ${}^{E}\!/_{F}$ has a normal closure ${}^{N}\!/_{F}$, which is unique up to E-isomorphism.

Proof. Write $E=F(\alpha_1,\dots,\alpha_n)$
1. **Existence:** let $p_i(x)$ be the minimal polynomial of α_i over F $(1\le i\le n)$. Write
$$f(x)=p_1(x)\dots p_n(x)$$
and let ${}^{N}\!/_{E}$ be the splitting field of $f(x)$ over E. Since $\alpha_1,\dots,\alpha_n$ are the roots of $f(x)$, N is also the splitting field of $f(x)$ over F. By Theorem 50, N is normal over F. Let $L\subsetneq N$ be a subfield containing E. Then, L contains all α_i. If L is normal over F. Each $p_i(x)$ splits over L, thus, $N\subseteq L$. It follows that $L=N$.
2. **Uniqueness:** Let ${}^{N}\!/_{E}$ be the splitting field of $f(x)$ over E defined as above. Let ${}^{N_1}\!/_{E}$ be another normal closure of ${}^{E}\!/_{F}$. Then, N_1 is normal over F and contains all α_i. Therefore, N_1 must contains a splitting field $\tilde{N}$ of $f(x)$ over F, thus, over E. By Corollary 14, N and $\tilde{N}$ are E-isomorphic. Since $\tilde{N}$ is a splitting field of $f(x)$ over F, by Theorem 50, $\tilde{N}$ is normal over F. Thus, by definition of normal closure, $N_1=\tilde{N}$. It follows that N and N_1 are E-isomorphic.

■



9. Galois Correspondence

9.1 Galois Extension

We already have the notions of normal extension (Theorem 50) and separability of splitting fields (Theorem 46).

R The converse of Theorem 46 is true.

Definition 9.1.1 — Galois Extension. An algebraic extension over ${}^{E}\!/_{F}$ is normal and separable if and only if it is Galois. If ${}^{E}\!/_{F}$ is a Galois extension, we say the automorphism group $\mathbf{Aut}_F(E)$ is the Galois group and ${}^{E}\!/_{F}$ is denoted by $\mathbf{Gal}_F(E)$.

Definition 9.1.2 A Galois extension ${}^{E}\!/_{F}$ is called **abelian**, **cyclic**, or **solvable**, if $\mathbf{Gal}_F(E)$ has the corresponding properties.

R

1. By Theorem 46 and 50, 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 43,
$$|\mathbf{Gal}_F(E)| = [E : F]$$
3. If ${}^{E}\!/_{F}$ is a splitting field of a separable polynomial $f(x) \in F[x]$, with $\deg(f) = n$. By Theorem 44, $\mathbf{Gal}_F(E)$ is a subgroup of S_n (considering n is the number of roots to be permuted).

■ **Example 9.1** Let E be the splitting field of

$$f(x) = (x^2 - 2)(x^2 - 3)(x^2 - 5) \in \mathbb{Q}[x]$$

then, $E = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}, \sqrt{5}\right)$ and $[E : \mathbb{Q}] = 8$. For $\psi \in \mathbf{Gal}_{\mathbb{Q}}(E)$, we have

$$\begin{cases} \psi\left(\sqrt{2}\right) \in \left\{\pm\sqrt{2}\right\} \\ \psi(\sqrt{3}) \in \{\pm\sqrt{3}\} \\ \psi\left(\sqrt{5}\right) \in \left\{\pm\sqrt{5}\right\} \end{cases}$$

Since $[E : \mathbb{Q}] = 8 = |\mathbf{Gal}_{\mathbb{Q}}(E)|$. We have

$$\mathbf{Gal}_{\mathbb{Q}}(E) \cong {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$$

■

Theorem 54 — E. Artin. Let E be a field and G is a finite subgroup of $\mathbf{Aut}(E)$ (the automorphism group of E)

$$E^G = \{\alpha \in E : \psi(\alpha) = \alpha, \forall \psi \in G\}$$

(is a subfield of E). Then, ${}^{E}\!/_{E^G}$ is a **finite Galois** extension and

$$\mathbf{Gal}_{E^G}(E) = G$$

In particular, we have

$$\left[E : E^G\right] = |G|$$

Proof. Let $n = |G|$ and $F = E^G$. We can check easily that $F = E^G$ is a subfield of E. For $\alpha \in E$, consider the G-orbit of α, i.e,

$$\{\psi(\alpha) : \psi \in G\} = \{\alpha_1, \ldots, \alpha_m\}$$

where α_i are distinct. Note that $m \leq n$. Let

$$f(x) = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_m)$$

For any $\psi \in G$, ψ permutes the roots $\{\alpha_1, \ldots, \alpha_m\}$. Since the coefficients of $f(x)$ are symmetric with respect to α_i $(1 \leq i \leq m)$, they are fixed by all $\psi \in G$. Thus, $f(x) \in E^G[x] = F[x]$. Now, we want to show $f(x)$ is the minimal polynomial of α over F. Let $g(x) \in F[x]$ be a factor of $f(x)$. WLOG, we can write

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

If $l \neq m$, since α_i $(1 \leq i \leq m)$ are in the G-orbit, there exists $\psi \in G$ such that $\{\alpha_1, \ldots, \alpha_l\} \neq \{\psi(\alpha_1), \ldots, \psi(\alpha_l)\}$. It follows that

$$\psi(g(x)) = (x - \psi(\alpha_1))\ldots(x - \psi(\alpha_l)) \neq g(x)$$

the coefficients change...
Thus, if $l \neq m$, $g(x) \notin F[x]$. Contradiction!
Thus, $f(x)$ is the minimal polynomial of α over F. Since $f(x) \in F[x]$ is separable and splits over E. ${}^{E}\!/_{F}$ is Galois.
Claim: $[E : F] \leq n$

Proof. For the sake of contradiction, we suppose $[E : F] > n = |G|$. Then, we can choose $\beta_1, \ldots, \beta_{n+1} \in E$ which are linearly independent over F.

Consider the system

$$\psi(\beta_1)v_1 + \cdots + \psi(\beta_{n+1})v_{n+1} = 0, \forall \psi \in G \qquad (*)$$

for all $\psi \in G$ of n linear equations in the $n+1$ variables $v_1, \ldots, v_2$. Thus, it has a non-zero solution in E. Let $(\gamma_1, \ldots, \gamma_{n+1})$ be such a solution which has the minimal number of non-zero coordinates, say r. Clearly, $r > 1$, WLOG, we can assume $\gamma_1, \ldots, \gamma_r \neq 0$ and $\gamma_{r+1}, \ldots, \gamma_{n+1} = 0$. Thus,

$$\psi(\beta_1)\gamma_1 + \cdots + \psi(\beta_r)\gamma_r = 0$$

for all $\psi \in G$. By dividing γ_r, we can assume $\gamma_r = 1$. Since $(\beta_1, \ldots, \beta_r)$ are linearly independent over F and

$$\beta_1\gamma_1 + \cdots + \beta_r\gamma_r = 0$$

Thus, there exists at least one $\gamma_i \notin F$. Since, WLOG, we can assume $\gamma_1 \notin F$. Choose $\phi \in G$ such that $\phi(\gamma_1) \neq \gamma_1$. Applying ϕ into system $(*)$, we have

$$\phi \circ \psi(\beta_1)\phi(\gamma_1) + \cdots + \phi \circ \psi(\beta_r)\phi(\gamma_r) = 0, \forall \psi \in G(1)$$

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

$$\psi(\beta_1)\phi(\gamma_1) + \cdots + \psi(\beta_r)\phi(\gamma_r) = 0, \forall \psi \in G(2)$$

By subtracting (2) from (1), we get

$$\psi(\beta_1)(\gamma_1 - \phi(\gamma_1)) + \cdots + \psi(\beta_r)(\gamma_r - \phi(\gamma_r)) = 0, \forall \psi \in G$$

Since $\gamma_r = 1$, we have $\gamma_r - \phi(\gamma_r) = 0$. Also, $\gamma_1 \notin F$, we have $\gamma_1 - \phi(\gamma_1) \neq 0$. Thus,

$$(\gamma_1 - \phi(\gamma_1), \ldots, \gamma_r - \phi(\gamma_r))$$

is also a non-zero solution of the system

$$\psi(\beta_1)v_1 + \cdots + \psi(\beta_{n+1})v_{n+1} = 0, \forall \psi \in G$$

This contradicts the choices of $(\gamma_1, \ldots, \gamma_n, \gamma_{n+1})$. Thus, $[E : F] \leq n$. ■

We have proved that E/F is a finite Galois extension. Thus, E is the splitting field of some separable polynomial over F. Also, since $F = E^G = \{\alpha \in E : \psi(\alpha) = \alpha, \forall \psi \in G\}$. Thus, G is a subgroup of $\mathbf{Aut}_F(E)$. By Theorem 46, we have $n = |G| \leq |\mathbf{Gal}_F(E)| = [E : F] \leq n$. Thus,

$$[E : F] = n \text{ and } \mathbf{Gal}_F(E) = G$$

■

R Let E/F be a Galois extension with the Galois group G. For $\alpha \in E$, let $\{\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_m\}$ be the G-orbit of α. Then, we see from the proof of Theorem 54 that the minimal polynomial of α over E^G is

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

■ **Example 9.2** Let $E = F(t_1, \ldots, t_n)$ be a function field in n variables, $t_1, \ldots, t_n$ over a field F. Consider the symmetric group S_n as the subgroup of $\mathbf{Aut}(E)$ which permutes the variables. We want to find $E^{S_n} = E^G$ with $G = S_n$. The G-orbit of t_1 is $\{t_1, \ldots, t_n\}$. By the remark, we see that

$$f(x) = (x - t_1)(x - t_2) \ldots (x - t_n)$$

is the minimal polynomial of t_1 over E^G. Define the elementary symmetric functions in $t_1, \ldots, t_n$ as

$$\begin{aligned} S_1 &= t_1 + t_2 + \cdots + t_n \\ S_2 &= \sum_{1 \le i < j \le n} t_i t_j \\ \vdots & \qquad \vdots \\ S_n &= t_1 t_2 \ldots t_n \end{aligned}$$

Thus,

$$f(x) = x^n - S_1 x^{n-1} + S_2 x^{n-2} - \cdots + (-1)^n S_n \in L[x]$$

where $L = F(S_1, \ldots, S_n) \subseteq E^G$.

Claim: $L = E^G$

Proof. Note that E is the splitting field of $f(x)$ over L. Since $\deg(f) = n$, by Theorem 15, we have

$$[E : L] \le n!$$

On the other hand, by Theorem 54,

$$[E : E^G] = |G| = |S_n| = n!$$

Since $L \subseteq E^G$, we have that

$$n! = [E : E^G] \le [E : L] \le n! \Longrightarrow E^G = L$$

■

■

9.2 The Fundamental Theorem

Theorem 55 — Fundamental Theorem of Galois Theory. Let E/F be a finite Galois extension and $G = \mathbf{Gal}_F(E)$, then there is an order reverising bijection between the intermediate fields of E/F and the subgroups of G. More precisely, let $\mathbf{Int}(E/F)$ denote the set of intermediate fields of E/F and $\mathbf{Sub}(G)$ the set of subgroups of G. Then, the maps

$$\mathbf{Int}(E/F) \to \mathbf{Sub}(G) \qquad L \mapsto L^* := \mathbf{Gal}_L(E)$$

and

$$\mathbf{Sub}(G) \mapsto \mathbf{Int}(E/F) \qquad H \mapsto H^* := E^H$$

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

$$[L_1 : L_2] = [L_2^* : L_1^*]$$

$$
\begin{array}{ccc}
E & \longleftrightarrow & \{1\} = \mathbf{Gal}_E(E) \\
\uparrow & & \downarrow \\
L_1 & \longleftrightarrow & L_1^* = \mathbf{Gal}_{L_1}(E) \\
\uparrow & & \downarrow \\
L_2 & \longleftrightarrow & L_2^* = \mathbf{Gal}_{L_2}(E) \\
\uparrow & & \downarrow \\
F & \longleftrightarrow & G = \mathbf{Gal}_F(E)
\end{array}
$$

Figure 9.2.1: *Fundamental Theorem of Galois Theory*

and

$$[H_1 : H_2] = [H_2^* : H_1^*]$$

Proof. Let $I \in \mathbf{Int}(E/F)$ and $H \in \mathbf{Sub}(G)$. We recall Theorem 45, which states that if $G_1 = \mathbf{Gal}_{F_1}(E_1)$, then $E^{G_1} = F_1$. Thus, we have

$$(L^*)^* = (\mathbf{Gal}_L(E))^* = E^{\mathbf{Gal}_L(E)} = L$$

Also, Theorem 54 states that if $G_1 \in \mathbf{Aut}(E_1)$, then $\mathbf{Gal}_{E_1^{G_1}}(E_1) = G_1$. Thus, we have

$$(H^*)^* = \left(E^H\right)^* = \mathbf{Gal}_{E^H}(E) = H$$

Thus, we have $H \mapsto H^* \mapsto H^{**} = H$ and $L \mapsto L^* \mapsto L^{**} = L$. In particular, the map $L \mapsto L^*$ and $H \mapsto H^*$ are inverses of each other.
For $L_1, L_2 \in \mathbf{Int}(E/F)$, Proposition 51, E/L_1 and E/L_2 are also Galois extension, we have

$$L_2 \subseteq L_1 \Longrightarrow \mathbf{Gal}_{L_1}(E) \subseteq \mathbf{Gal}_{L_2}(E) \Longrightarrow L_1^* \subseteq L_2^*$$

Also,

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

For $H_1, H_2 \in \mathbf{Sub}(G)$ and $H_2 \subseteq H_1$. We have $E^{H_1} \subseteq E^{H_2} \Longrightarrow H_1^* \subseteq H_2^*$. Also,

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

■

R From Theorem 55, we see that the

$$\mathbf{Int}(E/F)$$

are in one-to-one correspondence with $\mathbf{Sub}(G)$ since $|\mathbf{Sub}(G)| < \infty$, there are only finitely many $L \in \mathbf{Int}(E/F)$.

We have seen an example before that if E/F : Galois extension and $L \in \mathbf{Int}(E/F)$, then L/F is not always Galois.

$$
\begin{array}{ccc}
E & \longleftrightarrow & \{1\} = \mathbf{Gal}_E(E) \\
\uparrow & & \downarrow \\
L & \longleftrightarrow & L^* = \mathbf{Gal}_{L_1}(E) \\
\uparrow & & \downarrow \\
F & \longleftrightarrow & G = \mathbf{Gal}_F(E)
\end{array}
$$

Proposition 56 Let ${}^{E}\big/_{F}$ be a finite Galois extension with $G = \mathbf{Gal}_F(E)$. Let L be an intermediate field. For $\psi \in G$, we have

$$\mathbf{Gal}_{\psi(L)}(E) = \psi \mathbf{Gal}_L(E)\psi^{-1}$$

Proof. For any $\alpha \in \psi(L)$, $\phi^{-1}(\alpha) \in L$. If $\phi \in \mathbf{Gal}_L(E)$, we have

$$\phi\psi^{-1}(\alpha) = \psi^{-1}(\alpha) \Longrightarrow \psi\phi\psi^{-1}(\alpha) = \alpha$$

It follows that

$$\psi\phi\psi^{-1} \in \mathbf{Gal}_{\psi(L)}(E), \forall \phi \in \mathbf{Gal}_L(E)$$

Thus, $\psi \in \mathbf{Gal}_L(E)\psi^{-1} \subseteq \mathbf{Gal}_{\psi(L)}(E)$. Since

$$\left|\psi \in \mathbf{Gal}_L(E)\psi^{-1}\right| = [E:L] = [E:\psi(L)] = \left|\mathbf{Gal}_{\psi(L)}(E)\right|$$

We have $\mathbf{Gal}_{\psi(L)}(E) = \psi \in \mathbf{Gal}_L(E)\psi^{-1}$. ■

Theorem 57 Let ${}^{E}\big/_{F}, L, L^*$ be defined as in Theorem 55, then ${}^{L}\big/_{F}$ is a Galois extension if and only if L^* is a normal subgroup of G. In this case,

$$\mathbf{Gal}_F(L) \cong {}^{G}\big/_{L^*}$$

Proof. Note that

$$
\begin{aligned}
{}^{L}\big/_{F} \text{ is normal } &\iff \psi(L) = L, \forall \psi \in \mathbf{Gal}_F(E) \\
&\iff \mathbf{Gal}_{\psi(L)}(E) = \mathbf{Gal}_L(E), \forall \psi \in \mathbf{Gal}_F(E) \\
&\iff \psi \mathbf{Gal}_L(E)\psi^{-1} = \mathbf{Gal}_L(E), \forall \psi \in \mathbf{Gal}_F(E) \\
&\iff L^* = \mathbf{Gal}_L(E) \text{ is a normal subgroup of } G
\end{aligned}
$$

If ${}^{L}\big/_{F}$ is a Galois extension, the restriction map

$$G = \mathbf{Gal}_F(E) \to \mathbf{Gal}_F(L), \psi \mapsto \psi\big|_L$$

is well-defined. Moreover, it is surjective and its kernel is $\mathbf{Gal}_L(E) = L^*$. Thus,

$$\mathbf{Gal}_F(L) \cong {}^{G}\big/_{L^*}$$

■

■ **Example 9.3** For a prime p, let $q = p^n$. Consider the finite field $\mathbb{F}_q$ of q elements which is an extension of $\mathbb{F}_p$ of degree n. The **Frobenius automorphism** of $\mathbb{F}_q$ is defined by (see Assignment 2)

$$\sigma_p : \mathbb{F}_q \to \mathbb{F}_p, \alpha \mapsto \alpha^p$$

For $\alpha \in \mathbb{F}_q$, we ahve $\sigma_p^n(\alpha) = \alpha^{p^n} = \alpha$. Thus, $\sigma_p^n = 1$. For $1 \leq m < n$, we have $\sigma_p^m(\alpha) = \alpha^{p^m}$. Since the polynomial $x^{p^m} - x$ has at most p^m roots in $\mathbb{F}_q$. There exists $\alpha \in \mathbb{F}_q$ such that $\alpha^{p^m} - \alpha \neq 0$. Thus, $\sigma^{p^m} \neq 1$. Hence, σ_p has order n. Let $G = \mathbf{Gal}_{\mathbb{F}_p}(\mathbb{F}_q)$. It follows that

$$n = |\sigma_p| \leq |G| = [\mathbb{F}_q : \mathbb{F}_p] = n$$

Thus, $G = \langle \sigma_p \rangle$ is a cyclic group of order n.
Consider a subgroup H of G order d. Thus,

$$d \big| n \text{ and } [G : H] = \frac{n}{d}$$

By Theorem 55, we have

$$\frac{n}{d} = [G : H] = [H^* : G^*] = [\mathbb{F}_q^H : \mathbb{F}_p^G] = [\mathbb{F}_q^H : \mathbb{F}_p]$$

Thus,

$$H^* = \mathbb{F}_q^H = \mathbb{F}_p^{\frac{n}{d}}$$

we have

$$\begin{tikzcd}
\mathbb{F}_q \arrow[r, leftrightarrow] & \{1\} = \mathbf{Gal}_E(E) \arrow[d] \\
H^* = \mathbb{F}_p^{\frac{n}{d}} \arrow[u] \arrow[r, leftrightarrow] & H, |H| = d \arrow[d] \\
\mathbb{F}_p \arrow[u] \arrow[r, leftrightarrow] & G
\end{tikzcd}$$

■