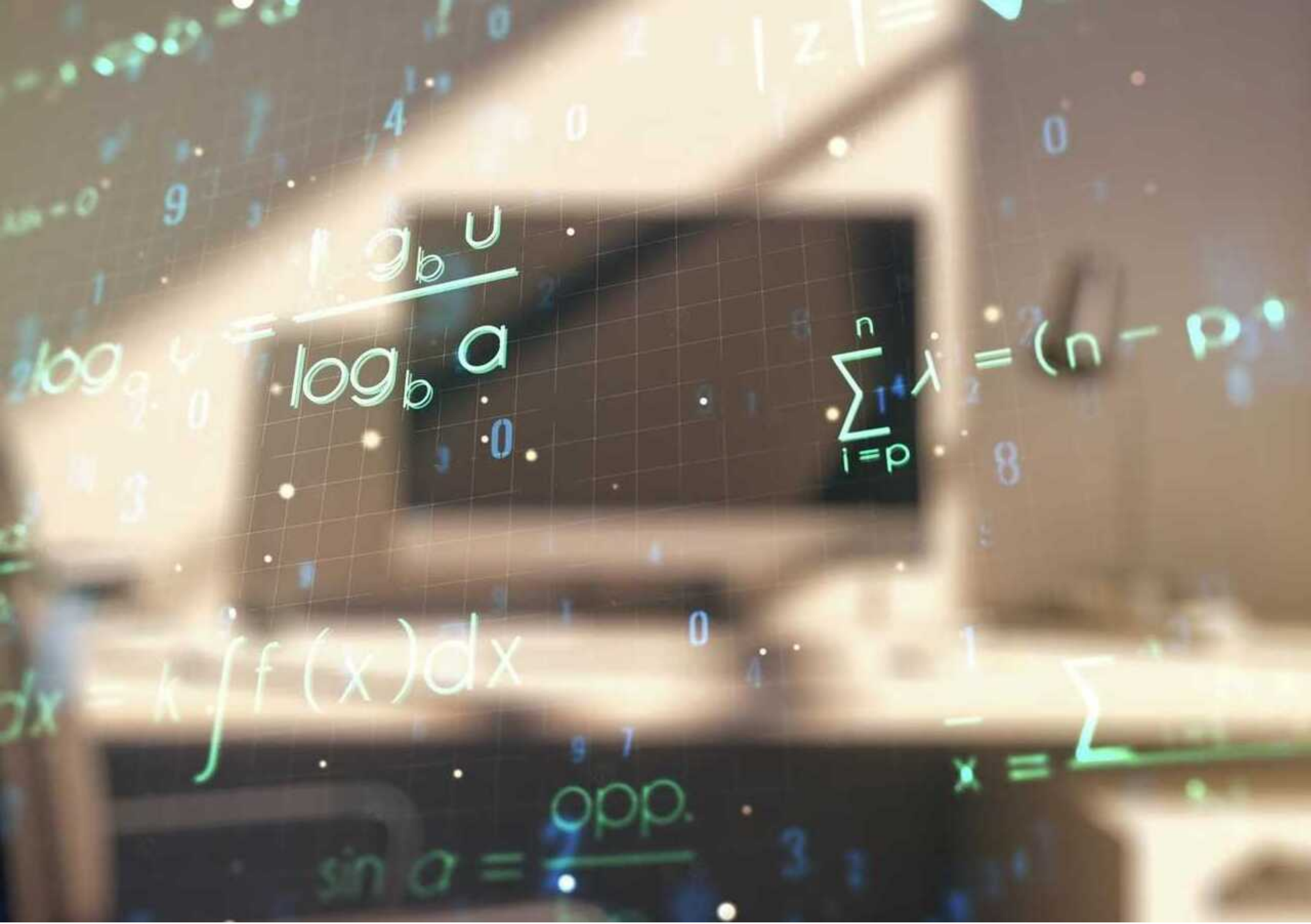

AS.110.411/412: Honors Algebra I & II

Author: Tian Zhou

Institute: Johns Hopkins University

Date: May 8, 2024

Version: 1

Year: Fall 2023, Spring 2024

***Textbook**: Algebra: Chapter 0 - Paolo Aluffi*

Contents

I Algebra I 4

Chapter 1 Preliminaries 5

1.1 Functions 5

1.1.1 Functions 5

1.1.2 Monomorphisms and Epimorphisms 6

1.2 Category 7

1.3 Morphisms 8

1.4 Universal Property 10

Chapter 2 Group Theory I 12

2.1 Definition of Group 12

2.1.1 Group 12

2.1.2 Order 13

2.1.3 Examples of groups 13

2.2 The Category of Grp 15

2.3 Group Homomorphisms 16

2.4 Free Groups 18

2.4.1 Universal Property 18

2.4.2 Free Group Construction 18

2.4.3 Free Abelian Group 19

2.5 Subgroups 20

2.5.1 Subgroups 20

2.5.2 Kernel and Image 21

2.6 Quotient Groups 23

2.6.1 Normal Subgroups and Cosets 23

2.6.2 Quotient Groups 23

2.7 Canonical Decomposition and Lagrange’s Theorem 26

2.7.1 Canonical Decomposition and Isomorphism Theorems 26

2.7.2 The Lagrange Theorem 28

2.7.3 Epimorphisms and Cokernels 28

2.8 Group Actions 30

2.8.1 Group Actions 30

2.8.2 The Category of G-Set 31

Chapter 3 Group Theory II 33

3.1 The Conjugation Action . . . 33
3.1.1 Center, Centralizer, Conjugacy Classes . . . 33
3.1.2 Class Formula . . . 34
3.1.3 Conjugation of Subsets and Subgroups . . . 34
3.2 Symmetric Group . . . 36
3.2.1 Cycles and Types . . . 36
3.2.2 Transposition, Parity, Alternating Group . . . 37
3.2.3 Conjugacy, Simplicity, and Solvability . . . 38
3.3 Sylow Theorems . . . 40
3.4 Products of Groups . . . 43
3.4.1 Direct Product, Exact Sequence . . . 43
3.4.2 Semdirect (Internal) Products . . . 44
3.5 Finite Abelian Groups . . . 46

II Algebra II **49**

Chapter 4 Ring Theory and Module Theory **50**
4.1 Ring . . . 50
4.1.1 Rings and Special Classes of Rings . . . 50
4.1.2 Polynomial Rings . . . 51
4.2 The Category of RING . . . 52
4.2.1 The Category of RING . . . 52
4.2.2 Universal property of polynomial rings . . . 52
4.2.3 Monomorphisms and epimorphisms . . . 53
4.3 Ideals and Quotient Rings . . . 55
4.3.1 Ideals and Quotient Rings . . . 55
4.3.2 PIDs, Prime Ideal, Maximal Ideal . . . 57
4.4 Modules Over a Ring . . . 58
4.4.1 Modules . . . 58
4.4.2 Submodules and Quotients, Kernel and Cokernel . . . 59
4.5 Complexes and Homology . . . 61

Chapter 5 Irreducibility and Factorization in Integral Domains **63**
5.1 Existence of Factorizations . . . 63
5.2 UFDs, PIDs, Euclidean Domains . . . 65
5.2.1 Unique Factorization Domains (UFDs) . . . 65
5.2.2 Principle Ideal Domains (PID) and Euclidean Domain (EDs) . . . 66
5.2.3 Noetherian Ring . . . 67
5.3 Unique Factorization in Polynomial Ring . . . 68

5.3.1 Primitivity and Content, Gauss's Lemma 68
5.3.2 Field of Fractions 69
5.3.3 R UFD Implies R[x] UFD 70
5.4 Irreducibility of Polynomials 72
5.4.1 Roots and Irreducibility 72
5.4.2 Toward Field Extension 73
5.4.3 Irreducibility in the Complex and Real Polynomial Ring 74

Chapter 6 Fields **76**

6.1 Field Extensions, I 76
6.1.1 Simple Extension 76
6.1.2 Algebraic and Transcendantal Extension 79
6.2 Algebraic Closures 81
6.2.1 Algebraic Closures 81
6.3 Field Extension II 83
6.3.1 Splitting Field and Normality 83
6.3.2 Separable Polynomials and Extensions 84
6.4 Field Extensions III 87
6.4.1 Finite Field 87
6.4.2 Separability and Simple Extensions 88
6.5 Introduction to Galois Theory 89
6.5.1 The Galois Correspondence and Extensions 89
6.5.2 The Fundamental Theorems of Galois Theory 91
6.6 Applications of Galois Theory 93
6.6.1 Geometric Impossibilities 93
6.6.2 Cyclomatic Polynomials and Fields 94
6.6.3 Constructibility of n-gons 95

Chapter 7 Homological Algebra **96**

7.1 Categorical Preliminaries 96
7.1.1 Additive Category 96
7.1.2 Abelian Category 97
7.1.3 Images and Canonical Decomposition of Morphisms 98
7.2 Functors 101
7.3 Complexes and Homology 102
7.3.1 Exactness in Abelian Category 102
7.3.2 Complex and Homology 103
7.3.3 Category of Cochain Complexes 103

Part I

Algebra I

Chapter 1 Preliminaries

Introduction

❑ *Naive Set Theory and Functions*
❑ *Morphisms*
❑ *Category*
❑ *Universal Properties*

1.1 Functions

1.1.1 Functions

Function The function $f : A \to B$ is a subset of $A \times B$ for which $(\forall\, a \in A)(\exists!\, b \in B), f(a) = b$. The notation B^A denotes collection of all functions from the set A to B.

If S is a subset of A, we denote by $f(S)$ the subset of B defined by $f(S) = \{b \in B \,|\, (\exists\, a \in A)\, b = f(a)\}$; in particular, $f(A)$ is the image of f, denoted by $\operatorname{im} f$. We denote by $f|_S$ the *restriction* of f to S, $f|_S : S \to B$ is defined by $f|_S(x) = f(x)$ for all $x \in S$.

Composition If $f : A \to B$ and $g : B \to C$, the composition $g \circ f : A \to C$ is defined by $(g \circ f)(x) := g(f(x))$. Note that composition is associative, and the identity function id_A is the identity element in composition.

Definition 1.1 (Injection, Surjections, Bijection)

A function $f : A \to B$ is

- ***injective** (one-to-one) if $a \neq a' \Rightarrow f(a) \neq f(a')$, or equivalently, $f(a) = f(a') \Rightarrow a = a'$;*
- ***surjective** (onto) if $(\forall\, b \in B)(\exists\, a \in A)\, b = f(a)$, or equivalently, $\operatorname{im} f = B$;*
- ***bijective** (one-to-one correspondence) if f is both injective and surjective.*

♣

Proposition 1.1

Assume $f : A \to B$ where $A \neq \varnothing$, then f has a left inverse if and only if it is injective, and f has a right inverse if and only if it is surjective.

♠

Proof For sufficiency, suppose there is $g : B \to A$ such that $g(f(a)) = a$ for all $a \in A$. Suppose $f(a) = f(a')$, then $g(f(a)) = g(f(a'))$, implying that $a = a'$. Then f is injective. For necessity, suppose f is injective. Choose an arbitrary element $a_0 \in A$. Let $g : B \to A$ be defined by $g(b) = a$ if $f(a) = b$ for some $a \in A$, and otherwise $g(b) = a_0$. It is not hard to show g is well-defined by the injectivity of f. For all $a \in A$, $g(f(a)) = a$ by the construction of g, so f has a left inverse. The proof of right inverse is analogous. ■

Remark If f is injective but not surjective, it will have more than one left-inverse, and the similar statement holds if f is surjective but not injective.

Corollary 1.1

A function $f : A \to B$ is a bijection if and only if it has a inverse, denoted by f^{-1}.

For $f : A \to B$ not bijective, we denote by $f^{-1}(T)$, where $T \subset B$, the subset of A of all elements that map to T, namely $f^{-1}(T) = \{a \in A \,|\, f(a) \in T\}$.

Consider the equivalence relation $\sim$ on A as follows: for $a, a' \in A$, $a \sim a'$ if and only if $f(a) = f(a')$, we obtain the canonical decomposition:

Proposition 1.2 (Canonical Decomposition)

Let $f : A \to B$ be a function and define $\sim$ as above. Then f decomposes as the composition of the canonical projection $A \to A/\sim$ (surjection), followed by a bijection $\bar{f} : A/\sim \to$ im f defined by $\bar{f}([a]_\sim) = f(a)$, followed by the inclusion function im $f \to B$ (injection).

Remark The commutative diagram of the canonical decomposition is shown as:

$$\begin{tikzcd}
A \arrow[r, two heads] \arrow[rrr, bend left, "f"] & (A/\sim) \arrow[r, "\sim", "\bar{f}"'] & \text{im}\, f \arrow[r, hook] & B
\end{tikzcd}$$

1.1.2 Monomorphisms and Epimorphisms

Definition 1.2 (Monomorphism, Epimorphism)

*A function $f : A \to B$ is a **monomorphism** if for all sets Z and all functions $\alpha, \alpha' : Z \to A$, $f \circ \alpha = f \circ \alpha' \Rightarrow \alpha = \alpha'$; and f is an **epimorphism** if for all sets Z and all functions $\alpha, \alpha' : B \to Z$, $\alpha \circ f = \alpha' \circ f \Rightarrow \alpha = \alpha'$.*

Proposition 1.3

A function is injective if and only if it is a monomorphism. A function is surjective if and only if it is a epimorphism.

Remark This proposition holds only when f is a set-function.

Proof For sufficiency, suppose f is injective. Let Z be a set, $\alpha, \alpha' : Z \to A$, and $f \circ a = f \circ a'$. For all $x \in Z$, $f(\alpha(x)) = f(\alpha'(x))$, so $\alpha(x) = \alpha'(x)$ by the injectivity of f. That is, $\alpha = \alpha'$.

For necessity, suppose f is a monomorphism and $f(x) = f(x')$. Let $Z = \{p\}$ and define $\alpha, \alpha' : Z \to A$ by $\alpha(p) = x$ and $\alpha'(p) = x'$. Then $(f \circ \alpha)(p) = f(x) = f(x') = (f \circ \alpha')(p)$, so $f \circ \alpha = f \circ \alpha'$, followed $\alpha = \alpha'$ since f is a monomorphism. Therefore, $x = \alpha(p) = \alpha'(p) = x'$, it follows that f is injective.

The proof for surjective functions is analogous. ■

1.2 Category

Definition 1.3 (Category)

*A **category** $\mathcal{C}$ consists of (i) a class Obj($\mathcal{C}$) of **objects** of the category and (ii) for every two objects A, B of $\mathcal{C}$, a set $\hom_{\mathcal{C}}(A, B)$ of **morphisms**, together with the following data:*

- ***identities**: for every object A of $\mathcal{C}$, there exists (at least one) morphism $1_A \in \hom_{\mathcal{C}}(A, A)$, the identity (id$_A$) on A, and*
- ***composition**: two morphisms $f \in \hom_{\mathcal{C}}(A, B)$ and $g \in \hom_{\mathcal{C}}(B, C)$ determine a morphism $gf \in \hom \mathcal{C}(A, C)$, the composite of g with f,*

such that the following laws holds:

- *associativity: composition is associative,*
- *unit: the identity morphism is identity with respect to composition.*

♣

Remark One further requirement is that the sets $\hom_{\mathcal{C}}(A, B)$, $\hom_{\mathcal{C}}(C, D)$ is disjoint unless $A = C$, $B = D$.

The morphism of an object $A \in \mathcal{C}$ to itself is called an *endomorphism*; $\hom_{\mathcal{C}}(A, A)$ is denoted by $\mathrm{End}_{\mathcal{C}}(A)$.

Example 1.1 The sets (as objects), together with set-functions (as morphisms), form a category, and we denote by Set this category. The vector spaces together with linear maps form a category Vect.

Example 1.2 Consider the set $\mathbb{Z}$ and the relation $\leq$, the preorder on $\mathbb{Z}$, which is reflexive and transitive. We can encode this data into a category $\mathcal{C}$: for $x, y \in \mathbb{Z}$, the morphism is $\hom(x, y) = \{(x, y)\}$ if $x \leq y$ and $\hom(x, y) = \varnothing$ otherwise. The identity is defined as $(x, x) \in \hom(x, x)$, and the composition is defined as $(y, z) \circ (x, y) = (x, z)$.

Similarly, every set S along a reflexive and transitive relation forms a category. These are examples of *small categories*, since the objects in this category is a set.

Example 1.3 Let $\mathcal{C}$ be a category, and $A \in \mathrm{ob}(\mathcal{C})$. We define the *slice category*, denoted by $\mathcal{C}_A$, by the category for which:

- the objects of $\mathcal{C}_A$ are morphisms $f \in \hom_{\mathcal{C}}(Z, A)$ for some $Z \in \mathrm{ob}(\mathcal{C})$, and
- the morphisms between $f_1 \in \hom_{\mathcal{C}}(Z_1, A)$ and $f_2 : \hom_{\mathcal{C}_A}(Z_2, A)$ is defined by the triple (Z_1, Z_2, σ) where $\sigma : Z_1 \to Z_2$ satisfies that $g_1 = g_2\sigma$.

1.3 Morphisms

Definition 1.4 (Isomorphism)

A morphism $f \in \hom_{\mathcal{C}}(A, B)$ is an ***isomorphism*** *if it has an inverse under composition: that is, if there exists $g \in \hom_{\mathcal{C}}(B, A)$ such that $gf = 1_A$ and $fg = 1_B$.*

We say A and B are isomorphic, denoted by $A \simeq B$, if there exists an isomorphism $f : A \to B$.

Remark In general, isomorphisms are not the morphisms that are both monomorphism and epimorphism.

Example 1.4

- In the category of Set, the isomorphisms are precisely the bijections.
- In the preorder category $(P, \leq)$, the isomorphisms are (x, x) where $x \in P$, namely the set of identities.
- In the category of matrices Mat, the isomorphisms are square matrices whose determinant is nonzero, this is also known as the general linear group $\mathrm{GL}(\mathbb{R})$.

Proposition 1.4

The inverse of an isomorphism is unique.

Proof Suppose $f \in \hom_{\mathcal{C}}(A, B)$ is an isomorphism, and g_1, g_2 are the inverses of f. Then $g_1 = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = g_2$. ■

Proposition 1.5

- *Each identity 1_A is an isomorphism and is its own inverse.*
- *If f is an isomorphism, the f^{-1} is an isomorphism and further $(f^{-1})^{-1} = f$.*
- *If $f \in \hom_{\mathcal{C}}(A, B)$ and $f \in \hom_{\mathcal{C}}(B, C)$ are isomorphisms, then the composition gf is an isomorphism and $(gf)^{-1} = f^{-1}g^{-1}$.*

An ***automorphism*** of an object A of a category $\mathcal{C}$ is an isomorphism from A to itself. The category of automorphisms of A is denoted $\mathrm{Aut}_{\mathcal{C}}(A)$, endowed with the following structures:

- the composition of $f, g \in \mathrm{Aut}_{\mathcal{C}}(A)$ is an element $gf \in \mathrm{Aut}_{\mathcal{C}}(A)$, and
- the identity is the identity morphism $1_A : A \to A$ in $\mathcal{C}$.

(Notice that $\mathrm{Aut}_{\mathcal{C}}(A)$ is a group.)

Definition 1.5 (Monomorphism, Epimorphism)

Let $\mathcal{C}$ be a category. A morphism $f \in \hom(A, B)$ is a ***monomorphism*** *if for all objects $Z \in ob(\mathcal{C})$ and all morphisms $\alpha', \alpha'' \in \hom(Z, A)$, $f \circ \alpha' = f \circ \alpha'' \Rightarrow a' = a''$; f is an* ***epimorphism*** *if for all objects $Z \in ob(\mathcal{C})$ and all morphisms $\beta', \beta'' \in \hom_(B, Z)$, $\beta' \circ f = \beta'' \circ f \Rightarrow \beta' = \beta''$.* ♣

Remark If a morphism f is an isomorphism, then f is monic and epic. However, the converse does not necessarily holds.

Example 1.5 In **Set**, monomorphism is equivalent to injection, and epimorphism is equivalent to surjection. However, in the category $(\mathbb{Z}, \leq)$ as described in example 1.2, every morphism is both a monomorphism and an epimorphism, but the only isomorphisms are the identities.

1.4 Universal Property

Introduction The universal property generalize constructions, such as cartesian product and quotient, uniquely up to isomorphism. Although the constructions may not exists for arbitrary objects in a general category, it is a more flexible notion.

Definition 1.6 (Initial Objects, Final Objects)

*Let $\mathcal{C}$ be a category. An object I of $\mathcal{C}$ is said to be **initial** if for every object $A \in ob(\mathcal{C})$, there exists an unique morphism in $\hom_{\mathcal{C}}(I, A)$; F is said to be **final** if for all for every object $A \in ob(\mathcal{C})$, there exists an unique morphism in $\hom_{\mathcal{C}}(A, F)$.*

Example 1.6 Initial and final objects do not necessarily exists in a category, consider $(\mathbb{Z}, \leq)$.
In Set, the empty set $\varnothing$ is the unique initial object, and every singleton is final in Set.

Proposition 1.6

Let $\mathcal{C}$ be a category.

- *If I_1, I_2 are both initial objects in $\mathcal{C}$, then $I_1 \cong I_2$.*
- *If F_1, F_2 are both final objects in $\mathcal{C}$, then $F_1 \cong F_2$.*

Further, these isomorphisms are uniquely determined.

Proof Since I_1 and I_2 are initial, $f : I_1 \to I_2$ and $g : I_2 \to I_1$ are unique. Notice that $g \circ f \in \hom(I_1, I_1) = \{\mathrm{id}_{I_1}\}$ since I_1 is initial, so $g \circ f = \mathrm{id}_{I_1}$. Without loss of generality, $f \circ g = \mathrm{id}_{I_2}$. It follows that f is an isomorphism because g is its inverse, so $I_1 \cong I_2$. The proof for final objects is analogous. ■

Example 1.7 Let $A/\sim$ be a quotient set of a set A by equivalence relation $\sim$. Define the category as follows:

- The objects are (Z, φ) where $\varphi : A \to Z$ is a morphism in $\mathcal{C}$ such that for all $a, a' \in A, a \sim a' \Rightarrow \varphi(a) = \varphi(a')$.
- The morphisms $\alpha : (Z_1, \varphi_1) \to (Z_2, \varphi_2)$ are morphisms $\alpha : Z_1 \to Z_2$ such that

$$\begin{tikzcd}
& A \arrow[ld, "\varphi_1"'] \arrow[rd, "\varphi_2"] & \\
Z_1 \arrow[rr, "\alpha"'] & & Z_2
\end{tikzcd}$$

Let $\pi : A \to A/\sim$ be the canonical projection, then $(A/\sim, \pi)$ define an initial object. In other word, $(A/\sim, \pi)$ is universal with the property with respect to the property of mapping A to a set in such a way that equivalent elements have the same image.

$$\begin{tikzcd}
& A \arrow[ld, "\pi"'] \arrow[rd, "\varphi"] & \\
A/\sim \arrow[rr, dashed, "\bar{\varphi}"'] & & Z
\end{tikzcd}$$

Remark The universal property defines the universal morphisms unique up to a unique isomorphism. For instance, in the above example, suppose Z_1, Z_2 both satisfy the universal property,

$$\begin{tikzcd}
 & A \arrow[dl, "\varphi_1"'] \arrow[d, "\varphi_2"] \arrow[dr, "\varphi_1"] & \\
Z_1 \arrow[r, dashed, "\alpha_1"'] & Z_2 \arrow[r, dashed, "\alpha_2"'] & Z_1
\end{tikzcd}$$

Then composition $\alpha_1 \circ \alpha_2$ is unique since Z_1 is an initial object, so $\alpha_1 \circ \alpha_2 = \mathrm{id}_{Z_1}$, hence $Z_1 \cong_{\alpha_1} Z_2$.

Example 1.8 The product of two sets can also be constructed using the universal property.

$$\begin{tikzcd}
A & A \times B \arrow[l, "\pi_A"'] \arrow[r, "\pi_B"] & B \\
 & Z \arrow[ul, "f_A"] \arrow[u, dashed, "\sigma"] \arrow[ur, "f_B"'] &
\end{tikzcd}$$

In other words, products of sets together with projection, namely $(A \times B, \pi_A, \pi_b)$, are final objects in the category $\mathcal{C}_{A,B}$.

Chapter 2 Group Theory I

Introduction

- ❑ *Group*
- ❑ *Free Groups and Subgroups*
- ❑ *Lagrange Theorem*
- ❑ *Group Actions*
- ❑ *Group Homomorphisms*
- ❑ *Normal Subgroup and Quotient Group*
- ❑ *Isomorphism Theorems*

2.1 Definition of Group

2.1.1 Group

Let G be a nonempty set, the **binary operation** endowed in G is a "multiplication" map: $\cdot : G \times G \to G$. We commonly denote $g \cdot h$ or gh by the mapping of (g, h) by $\cdot$.

Definition 2.1 (Group $(G, \cdot)$)

The set, endowed with the binary operation $\cdot$, denoted $(G, \cdot)$, is a ***group*** *if*

(a) ***Associativity****: the operation $\cdot$ is associative, that is, for all $g, h, k \in G$, $(g \cdot h) \cdot k = g \cdot (h \cdot k)$.*

(b) ***Identity****: there exists an identity element e_G for $\cdot$, that is, for all $g \in G$, $e_G \cdot g = g = g \cdot e_G$.*

(c) ***Inverse****: every element in G has an inverse with respect to $\cdot$, that is, for all $g \in G$, there exists $h \in G$ such that $h \cdot g = e_G = g \cdot h$. We usually denote g^{-1} by the inverse of g.*

A group $(G, \cdot)$ is ***abelian*** *(commutative group) if $(G, \cdot)$ is forms a group and the operation $\cdot$ is commutative.* ♣

Example 2.1 $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are common examples of group; indeed, they are abelian groups (commutative group).

The set of $n \times n$ invertible matrices with real entries, denoted by $GL_n(\mathbb{R})$ (general linear group), is an example of non-commutative group.

Proposition 2.1

The identity element and inverse are unique. ♠

Proof (1) Suppose e_G and e'_G are identity elements, then $e_G = e_G e'_G = e'_G$.

(2) Suppose g and g' are inverses of $f \in G$, then $g = g(fg') = (gf)g' = g'$. ■

In addition, the cancellation holds in groups, that is, $ga = ha \Rightarrow g = h$ and $ag = ah \Rightarrow g = h$.

2.1.2 Order

Definition 2.2 (Order)

*An element of g if a group G has **finite order** if $g^n = e$ for some $n \in \mathbb{Z}_{>0}$. In this case, the **order** $|g|$ is the least positive n such that $g^n = e$. If g does not have finite order, we write $|g| = \infty$.*

*If G is a finite set, its **order** $|G|$ is the number of its element, we write $|G| = \infty$ if G is infinite.*

Proposition 2.2

Let $g \in G$ be an element of finite order, then $g^n = e$ if and only if $|g|$ divides n.

Proof Suppose $|g| \nmid n$. We can write $n = q \cdot |g| + r$ for some $q, r \in \mathbb{Z}_{\geq 0}$ such that $0 < r < |g|$. Then

$$g^r = g^{n-q\cdot|g|} = g^n \cdot (g^{|g|})^{-q} = e \cdot e^{-q} = e$$

contradicting that $|g|$ is the order of g. The converse is obvious. ■

Proposition 2.3

Let $g \in G$ be an element of finite order, then g^m has finite order for all $m \geq 0$, and in fact $|g^m| = |g|/\gcd(m, |g|) = lcm(m, |g|)/m$.

Proof Let $d = \gcd(m, |g|)$. By the definition of $|g^m|$, $g^{m\cdot|g^m|} = e$, so $|g| \mid (m\cdot|g^m|)$, thus $(|g|/d) \mid |g^m|$. Conversely, since $d \mid m$, then $(g^m)^{|g|/d} = (g^{|g|})^{m/d} = e^{m/d} = e$, so $|g^m| \mid (|g|/d)$. Hence $|g^m| = |g|/d$. ■

Note ***Proposition**: If $gh = hg$, then $|gh| \mid lcm(|g|, |h|)$.*

2.1.3 Examples of groups

Symmetric Group Let A be a set. The ***symmetric group***, or group of permutation of A, denoted S_A, is the group $\mathrm{Aut}_{\mathsf{Set}}(A)$. The group of permutation of the set $\{1, \cdots, n\}$ is denoted by S_n.

The groups S_A are large, for instance, $|S_n| = n!$. It worth to note that the multiplication fg is defined to be the composition $g \circ f$. In other words, we adopt the convention of writing functions *after* the element, for instance, $(p)(fg) = (g \circ f)(p)$ for $p \in A$. In addition, the commutativity does not necessarily hold.

Dihedral Groups A "symmetry" is a transformation which preserves a structure. The ***dihedral groups*** may be defined as the groups of symmetries for the regular polygons. The dihedral group for regular n-sided polygon, denoted D_{2n}, includes n rotations by $2\pi/n$ radians and n reflections.

Cyclic Groups and Modular Arithmetic Define the ***congruence modulo n*** on $\mathbb{Z}$ by $a \equiv b \pmod{n}$ if and only if $n \mid (b - a)$. The equivalence classes is $\mathbb{Z}_n$.

By defining $[x] + [y] = [x + y]$, the structure $(\mathbb{Z}_n, +)$ becomes an abelian group. The abelian group we obtained is called ***cyclic groups***, denoted C_n, which is the group generated by one element x with the relation $x^n = e$. In $(\mathbb{Z}_+, +)$, a generator is $[1]_n$. It follows immediately from Proposition (2.3) that $|[m]_n| = |m \cdot [1]_n| = n/\gcd(m, n)$, and thus $[m]_n$ generated $\mathbb{Z}_n$ if and only if $\gcd(m, n) = 1$.

By defining $[x] \cdot [y] = [xy]$, and let $\mathbb{Z}_n^\times = \{[m]_n \in \mathbb{Z}_n \mid \gcd(m, n) = 1\}$. We recognize the structure $(\mathbb{Z}_n^\times, \cdot)$ as an abelian group.

2.2 The Category of Grp

For two groups $(G, \cdot)$ and $(H, *)$, a ***group homomorphism*** $\varphi : (G, \cdot) \to (H, *)$ is a function between groups that preserves the structure, and in this case the diagram below commutes.

$$\begin{tikzcd}
G \times G \arrow[r, "\varphi \times \varphi"] \arrow[d, "\cdot"'] & H \times H \arrow[d, "*"] \\
G \arrow[r, "\varphi"] & H
\end{tikzcd}$$

Definition 2.3 (Group Homomorphism)

*The set function $\varphi : (G, \cdot) \to (H, *)$ is a **group homomorphism** if for all $a, b \in G$, $\varphi(a \cdot b) = \varphi(a) * \varphi(b)$.*

Definition 2.4 (Grp)

The category of Grp is a category whose (a) objects of Grp are groups, and (b) for every pair of groups G, H, the morphisms $\hom_{\textsc{Grp}}(G, H)$ are the set of group homomorphisms $G \to H$.

We now need to verify Grp is well-defined. Suppose G, H, K are groups and $\varphi : G \to H$, $\psi : H \to K$ are group homomorphisms, then the composition $\psi \circ \varphi : G \to K$ is a group homomorphism:

$$(\psi \circ \varphi)(a \cdot_G b) = \psi(\varphi(a) \cdot_H \varphi(b)) = (\psi \circ \varphi)(a) \cdot_K (\psi \circ \varphi)(b).$$

It is obvious that composition is associative and that the identity function $\mathrm{id}_G : G \to G$ is a group homomorphism. Therefore, Grp is indeed a category.

Proposition 2.4

Let $\varphi : G \to H$ be a group homomorphism. Then

(a) $\varphi(e_G) = e_H$;

(b) $\forall\, g \in G$, $\varphi(g^{-1}) = \varphi(g)^{-1}$.

Remark The group homomorphism preserves the structure, in particular, the identity element e and the inverse.

Proof (a) $\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G)$, implying that $\varphi(e_G) == e_H$ by the cancellation.

(b) $\varphi(g^{-1}) \cdot \varphi(g) = \varphi(g^{-1} \cdot g) = e_H = \varphi(g)^{-1} \cdot \varphi(g)$, implying that $\varphi(g^{-1}) = \varphi(g)^{-1}$ by the cancellation. ■

Proposition 2.5

With operation defined componentwise, $G \times H$ is a product in Grp.

The category of abelian groups Ab is a category whose objects are abelian groups and whose morphisms are group homomorphism.

2.3 Group Homomorphisms

Example 2.2 Suppose G is a group, the conjugation $\gamma_g : G \to G$, $a \mapsto gag^{-1}$, is a group homomorphism and indeed an isomorphism. The left translation $\lambda_g : G \to G$, $a \mapsto ga$, is a bijection but not a group homomorphism. The group action $\lambda : G \to S_G$, $\lambda : g \mapsto \lambda_g$, is a group homomorphism.

Proposition 2.6

Let $\varphi : G \to H$ be a group homomorphism, and let $g \in G$ be an element of finite order. Then $|\varphi(g)|$ divides $|g|$. ♠

Proof Note that $\varphi(g)^{|g|} = \varphi(g^{|g|}) = \varphi(e_G) = e_H$, then $|\varphi(g)|$ divides $|g|$. ■

Example 2.3 There is no nontrivial homomorphism $\varphi : C_4 \to C_7$. The orders of elements in C_4 divide 4 and the order of elements in C_7 divide 7, so $\varphi(g)$ divides both 4 and 7, implying that $\varphi(g) = e$ for all $g \in C_4$.

Definition 2.5 (Isomorphisms, Isomorphic)

*An **isomorphism** of groups $\varphi : G \to H$ is an isomorphism in Grp, i.e., a group homomorphism admitting an inverse $\varphi^{-1} : H \to G$.*

*Two groups G, H are **isomorphic** in Grp if there is an isomorphism $G \to H$.* ♣

Proposition 2.7

Let $\varphi : G \to H$ be a group homomorphism. Then φ is an isomorphism of groups if and only if it is a bijection. ♠

Proof Suppose φ is an isomorphism, then it is a bijection. Conversely, suppose φ is a bijective homomorphism. There exists an inverse $\varphi^{-1} : H \to G$ of φ in Set. For all $h_1, h_2 \in H$, $h_1 = \varphi(g_1)$ and $h_2 = \varphi(g_2)$ for some g_1, g_2, then

$$\varphi^{-1}(h_1 \cdot h_2) = \varphi^{-1}(\varphi(g_1) \cdot \varphi(g_2)) = \varphi^{-1}(\varphi(g_1 \cdot g_2)) = g_1 \cdot g_2 = \varphi^{-1}(h_1) \cdot \varphi^{-1}(h_2).$$

Thus, φ^{-1} is a homomorphism, so φ is an isomorphism. ■

Definition 2.6 (Cyclic Group)

A group G is cyclic if it is isomorphic to $\mathbb{Z}$ or to $C_n = \mathbb{Z}/n\mathbb{Z}$ for some n. ♣

Remark Equivalently, G is a cyclic group if and only if $G = \{g^n \mid n \in \mathbb{Z}\}$ for some $g \in G$.

Example 2.4 For example, $C_2 \times C_3$ is cyclic of order 6, since $C_2 \times C_3 \simeq C_6$. More generally, $C_m \times C_n$ is cyclic if $\gcd(m, n) = 1$.

If p is prime, the group $(\mathbb{Z}_p^*, \cdot)$ is cyclic.

Proposition 2.8

Let $\varphi : G \to H$ be an isomorphism,

- *For all $g \in G$, $|\varphi(g)| = |g|$.*
- *G is abelian if and only if H is abelian.* ♠

Proof The first assertion follows from $|\varphi|$ divides $|g|$ and $|g| = |\varphi^{-1}(\varphi(g))|$ divides $|\varphi(g)|$ by Proposition (2.6). For the second assertion, suppose $h_1 = \varphi(g_1)$ and $h_2 = \varphi(g_2)$, then $h_1h_2 = \varphi(g_1g_2) = \varphi(g_2g_1) = h_2h_1$ if and only if $g_1g_2 = g_2g_1$. ■

Remark “Homomorphism” in Grp correspond to “continuous” map in topology, and “isomorphism” corresponds to “homeomorphism”. Two groups being isomorphic means that the underlying structure of the groups is identical.

2.4 Free Groups

2.4.1 Universal Property

Motivation The motivation of free groups is that given a set A, we want to construct a smallest group $F(A)$ containing A such that the elements of A have no special group-theoretic property. For instance, if $A = \{a\}$ is a singleton, $F(A) = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ is the infinite cyclic group generated by a.

Universal Property Consider the coslice category $\mathcal{F}^A$ whose objects are pairs (j, G) and the morphisms are group homomorphisms.

In the language of universal property, $F(A)$ is a ***free group*** on set A if there is a set-function $j : A \to F(A)$ such that for all $G \in \textsc{Grp}$ and $f : A \to G$, there exists a unique group homomorphism $\varphi : F(A) \to G$ such that

$$\begin{tikzcd}
F(A) \arrow[r, dashed, "\varphi"] & G \\
A \arrow[u, "j"] \arrow[ur, "f"'] &
\end{tikzcd}$$

That is, the *free group* $F(A)$ on A is an initial object in $\mathcal{F}^A$, up to isomorphism.

Example 2.5 Infinite cyclic groups $\mathbb{Z}$ satisfies the universal property for free groups over a singleton. Indeed, define $j : a \to 1$, for all G and $f : a \mapsto g$, homomorphism condition forces $\varphi(n) = g^n$.

2.4.2 Free Group Construction

Let A be a set, thought as an alphabet consisting of letters $a \in A$. Let $A' = \{a^{-1} \mid a \in A\}$ be the set of formal inverses, we have $A \cong A'$ and $A \cap A' = \varnothing$. A ***word*** over A is a juxtaposition of letters $w = a_1 a_2 \cdots a_n$ where $a_i \in A \cup A'$, and the ***empty word*** is $\varepsilon = ()$. We call $l(w) = n$ the ***length*** of n, and $W(A)$ the set of (finite) words w over A.

Let $r : W(A) \to W(A)$ be the ***elementary reduction map***: suppose $w \in W(A)$, r searches and remove the first occurrence of a pair aa^{-1} or $a^{-1}a$ in w. Note that $r(w) = w$ if and only if w cannot be reduced, we called w a ***reduced word***.

Proposition 2.9

If $w \in W(A)$ has length n, then $r^{\lfloor n/2 \rfloor}(w)$ is a reduced word.

We may define the reduction $R : W(A) \to W(A)$ by $R(w) = r^{\lfloor n/2 \rfloor}(w)$ where n is the length of w. Then the binary operation on $F(A)$ by juxtaposition and reduction can be defined, as $w \cdot w' = R(ww')$. It is not hard to verify $(F(A), \cdot)$ is a group if $F(A) = \operatorname{im} W(A)$.

Proposition 2.10

Let $j : A \to F(A)$ be defined by sending the element $a \in A$ to the word $w = a \in W(A)$. The pair $(j, F(A))$ satisfies the universal property for free groups on A. ♠

Proof We can extend $\varepsilon : F(A) \to G$ to the set-function $\tilde{\varphi} : W(A) \to G$ such that $\tilde{\varphi}(a) = f(a)$ for $a \in A \cup A'$ and compatible with juxtaposition $\tilde{\varphi}(ww') = \tilde{\varphi}(w)\tilde{\varphi}(w')$, and the reduction is invisible $\tilde{\varphi}(R(w)) = \tilde{\varphi}(w)$. Note that φ agrees with $\tilde{\varphi}$ on reduced words, we have $\varphi(w \cdot w') = \tilde{\varphi}(R(ww')) = \tilde{\varphi}(ww') = \tilde{\varphi}(w)\tilde{\varphi}(w') = \varphi(w)\varphi(w')$. ■

Remark We need to extend φ to $\tilde{\varphi}$ because the reduction inside φ is not well-defined, so we cannot conclude $\varphi(R(ww')) = \varphi(w)\varphi(w')$.

Remark Therefore, we can define the set of all reduced words in $W(A)$ to be the free group of set A (up to isomorphism).

2.4.3 Free Abelian Group

Suppose $A = \{1, \cdots, n\}$, denote by $\mathbb{Z}^{\oplus n}$ the direct sum $\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$. We view $\mathbb{Z}^{\oplus n}$ as the coproduct where $j : A \to \mathbb{Z}^{\oplus}$ is defined by $j(i) = (0, \cdots, 0, 1, 0, \cdots, 0)$ (1 is on the i-th index).

Proposition 2.11

For $A = \{1, \cdots, n\}$, $\mathbb{Z}^{\oplus n}$ is a free abelian group on A. ♠

Proof Note that every element of $\mathbb{Z}^{\oplus n}$ can be written uniquely in the form $\sim_{i=1}^{n} m_i j(i)$. Define $\varphi : \mathbb{Z}^{\oplus n} \to G$ by $\varphi(\sum m_i j(i)) = \prod f(i)^{m_i}$. This definition is unique because of the commutativity of the diagram

$$\begin{tikzcd}
\mathbb{Z}^{\oplus n} \arrow[r, dashed, "\varphi"] & G \\
A \arrow[u, "j"] \arrow[ur, "f"'] &
\end{tikzcd}$$

and by the homomorphism condition, as desired. ■

For the general case: if A is a set, define $H^{\oplus A} := \{\alpha : A \to H \mid \alpha(a) = e_H$ for all but finitely many elements $a \in A\}$, that is, $H^{\oplus A}$ is an A-indexed finite tuple. For $H = \mathbb{Z}$, the natural function $j : A \to \mathbb{Z}^{\oplus A}$ is obtained by sending $a \in A$ to $j_a : A \to \mathbb{Z}$ such that

$$j_a(x) := \begin{cases} 1 & \text{if } x = a \\ 0 & \text{if } x \neq a \end{cases}$$

making $H^{\oplus A}$ as a coproduct.

Corollary 2.1

For every set A, $F^{ab}(A) \cong \mathbb{Z}^{\oplus A}$. ♡

2.5 Subgroups

2.5.1 Subgroups

Definition 2.7 (Subgroup)

Let $(G, \cdot)$ be a group and $(H, \cdot)$ be another group whose underlying set H is a subset of G. $(H, \cdot)$ is a ***subgroup*** *of G, denoted by $H \leq G$, if the inclusion function $i : H \to G$ is a group homomorphism.* ♣

Remark The operation of a subgroup H is induced by the operation $\cdot$ in G (by the property of homomorphism). In addition, $(H, \cdot)$ is a subgroup of $(G, \cdot)$ if and only if

(a) H contains the identity element, namely $1 \in H$, and

(b) H is closed under multiplication and inverse.

Theorem 2.1

A nonempty subset H of a group G is a subgroup if and only if $ab^{-1} \in H$ for all $a, b \in H$. ♡

Proof ($\Rightarrow$) This direction is obvious because a subgroup is closed under multiplication and inverse.

($\Leftarrow$) Suppose $ab^{-1} \in H$ for all $a, b \in H$. The associativity in H follows immediately from the associativity in G. H contains the identity element since for an arbitrary $h \in H$, $e_G = hh^{-1} \in H$. Inverse is closed: if $h \in H$, then $h^{-1} = e_G h^{-1} \in H$ for all h. In addition, multiplication is closed: if $h_1, h_2 \in H$, then $h_2^{-1} \in H$, so $h_1 h_2 = h_1(h_2^{-1})^{-1} \in H$. Hence H is a subgroup. ■

Proposition 2.12

Arbitrary intersections of subgroups is a subgroup. In other words, if $\{H_\alpha\}_{\alpha \in A}$ is a family of subgroups of a group G, then $H = \bigcap_{\alpha \in A} H_\alpha$ is a subgroup of G. ♠

Proof H is nonempty because $1 \in H$. The proposition follows immediately from Proposition 2.1 since for all $\alpha \in A$ and $a, b \in H$, $a, b \in H_\alpha$, so $ab^{-1} \in H_\alpha$ for all $\alpha \in A$, thus $ab^{-1} \in H$. ■

Proposition 2.13

Let $\varphi : G \to G'$ be a group homomorphism, and let H' be a subgroup of G'. Then $\varphi^{-1}(H')$ is a subgroup of G. ♠

Proof For all $a, b \in \varphi^{-1}(H')$, $\varphi(a), \varphi(b) \in H'$, so does $\varphi(a)\varphi(b)^{-1} = \varphi(ab^{-1})$, thus $ab^{-1} \in \varphi^{-1}(H')$. The statement therefore follows from Proposition 2.1. ■

Definition 2.8 (Subgroup Generated by a Subset)

*If $A \subset G$ is a subset, there exists a unique homomorphism $\varphi_A : F(A) \to G$ by the universal property of free groups, compatible with the inclusion map. Then im φ_A is the **subgroup generated by A**, denoted by $\langle A \rangle$.*

Note *Equivalently, the subgroup generated by A is the intersection of all subgroups of G containing A, namely $\langle A \rangle = \bigcap_{A \subset H \leq G} H$.*

If $A = \{g\}$ is a singleton, then $\langle A \rangle = \{g^n \mid n \in \mathbb{Z}\}$.

Example 2.6 G is a subgroup of $\mathbb{Z}$ if and only $G = d\mathbb{Z}$ for some $d \in \mathbb{N}$. The proof involves using Euclid division lemma to prove that G is can be generated by a singleton.

Let G be a subgroup of $\mathbb{Z}_n$ for some $n \in \mathbb{Z}_{>0}$, then G is a cyclic subgroup generated by $d + n\mathbb{Z}$ for some $d \mid n$.

2.5.2 Kernel and Image

Definition 2.9 (Kernel, Image)

*The **kernel** of group homomorphism $\varphi : G \to G'$ is a subset of G consisting of elements mapping to the identity in G':* $\ker \varphi := \{g \in G \mid \varphi(g) = e_{G'}\} = \varphi^{-1}(e_{G'})$.

*The **image** is defined to be im* $\varphi = \{g' \in G' \mid \exists\, g \in G,\ \varphi(g) = g'\}$.

Proposition 2.14

Let $\varphi : G \to G'$ be a homomorphism. Then the inclusion $i : \ker \varphi \hookrightarrow G$ is final in the category of group homomorphism $\alpha : K \to G$ such that $\varphi \circ \alpha$ is the trivial map.

That is, there exists a unique $\tilde{\alpha}$ such that the below diagram commutes:

$$\begin{tikzcd}
K \arrow[rr, dashed, "\tilde{\alpha}"] \arrow[dr, "\alpha"] \arrow[ddr, bend right, "0"'] & & \ker \varphi \arrow[dl, "i"'] \arrow[ddl, bend left, "0"] \\
& G \arrow[d, "\varphi"] & \\
& G' &
\end{tikzcd}$$

Proof If $\alpha : K \to G$ us such that $\varphi \circ \alpha = 0$, then $\mathrm{im}(\varphi \circ \alpha) = \{0\}$ implies im $\alpha \subset \ker \varphi$. Therefore, $\tilde{\alpha}$ defined by $\tilde{\alpha}(k) = \alpha(k)$ satisfies the commutativity of the diagram, and it is the only map such that $\tilde{\alpha} \circ i = \alpha$. ■

Proposition 2.15

The following are equivalent:

(a) φ is a monomorphism;

(b) $\ker\varphi = \{e_G\}$*;*

(c) $\varphi : G \to G'$ *is injective (as a set-function).*

Remark For analogous statement of epimorphism, see Proposition 2.25.

Proof $(a) \Rightarrow (b)$: Consider $i : \ker\varphi \to G$ be the inclusion map and $e : \ker\varphi \to G$ be the trivial homomorphism,

$$\begin{tikzcd}
\ker\varphi \arrow[r, bend left, "i"] \arrow[r, bend right, "e"'] & G \arrow[r, "\varphi"] & G'
\end{tikzcd}$$

then $\varphi \circ i = \varphi \circ e$ since both are trivial homomorphisms. The monomorphism condition implies that $i = e$, so $\ker\varphi = \text{im}\, e = \text{im}\, i = \{e_G\}$.

$(b) \Rightarrow (c)$: Suppose $\ker\varphi = \{e_G\}$ and $\varphi(g_1) = \varphi(g_2)$. Then

$$\varphi(g_1) = \varphi(g_2) \Rightarrow \varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = e_{G'} \Rightarrow g_1 g_2^{-1} \in \ker\varphi = \{e_G\} \Rightarrow g_1 = g_2,$$

followed by φ is injective.

$(c) \Rightarrow (a)$: Suppose φ is injective, φ is a monomorphism in Set. Since φ is a group homomorphism, and in particular, $\varphi \circ \alpha = \varphi \circ \alpha' \Leftrightarrow \alpha = \alpha'$ holds if α, α' are homomorphisms, so φ is a monomorphism in Grp. ■

2.6 Quotient Groups

2.6.1 Normal Subgroups and Cosets

Definition 2.10 (Normal Subgroups)

A subgroup N of a group G is ***normal*** *if for all $g \in G$ and $n \in N$, $gng^{-1} \in N$. We denote by $N \trianglelefteq G$ if N is a normal subgroup of G.* ♣

Remark Equivalently, a subgroup is normal if and only if $gN = Ng$ for all $g \in G$.

Proposition 2.16

If $\varphi : G \to G'$ is a group homomorphism, then $\ker \varphi$ is a normal subgroup of G. ♠

Proof Suppose $n \in \ker \varphi$ and $g \in G$, then $\varphi(gng^{-1}) = \varphi(g)\varphi(n)\varphi(g)^{-1} = \varphi(g)e_{G'}\varphi(g)^{-1} = e_{G'}$, so $gng^{-1} \in \ker \varphi$. ■

Proposition 2.17

Suppose $\sim$ is an equivalence relation on G. The operation $[a] \cdot [b] = [ab]$ defines a group structure on $G/\sim$ if and only $a \sim a' \Rightarrow ga \sim ga'$ and $ag \sim a'g$ for all $a, a', g \in G$.

In this case the quotient function $\pi : G \to G/\sim$ is a homomorphism and is universal with respect to homomorphisms $\varphi : G \to G'$ such that $a \sim a' \Rightarrow \varphi(a) = \varphi(a')$. ♠

We say that $\sim$ is *compatible* with the group structure of G if the condition above holds.

Proof Sketch: (a) $a \sim a' \Rightarrow ga \sim ga'$ and $ag \sim a'g$ holds if and only the operation is well-defined, and then it is not hard to verify the group structure.

(b) Since $G/\sim$ satisfies the corresponding universal property in Set, there exists an unique function $\tilde{\varphi} : G/\sim \to G'$ defined by $[a] \to \varphi(a)$, and $\tilde{\varphi}$ is a homomorphism because φ is a homomorphism. Hence $((G/\sim), \pi)$ is initial. ■

Definition 2.11 (Cosets)

The ***left-cosets*** *of a subgroup H in a group are the sets aH, for $a \in G$. The* ***right-cosets*** *of H are the sets Ha, for $a \in G$.* ♣

2.6.2 Quotient Groups

We will analyze the properties of $a \sim a' \Rightarrow ga \sim ga'$ and $a \sim a' \Rightarrow ag \sim a'g$ separately.

Proposition 2.18

Let $\sim$ be an equivalence relation on a group G, satisfying $a \sim b \Rightarrow ga \sim gb$ for all $g, a, b \in G$, then

- *the equivalence class of e_G is a subgroup H of G; and*
- $a \sim b \Leftrightarrow a^{-1}b \in H \Leftrightarrow aH = bH.$

Conversely, if H is a subgroup of G, the relation $\sim_L$ defined by $a \sim_L b \Leftrightarrow a^{-1}b \in H$ is an equivalence relation satisfying $a \sim b \Leftrightarrow ga \sim gb$. ♠

Proof (a) Suppose $a, b \in H$, namely $a \sim b \sim e_G$. Since $b^{-1} = e_G b^{-1} \sim bb^{-1} = e_G$, then multiplying a on left yields $ab^{-1} \sim ae_G \sim e_G$, followed by $ab^{-1} \in H$, so H is a subgroup.

(b) Suppose $a \sim b$, multiply by a^{-1} on the left gives $a^{-1}b \sim e_G$, so $a^{-1}b \in H$. Since the multiplication is closed, $a^{-1}bH \subset H$, thus $aH \subset bH$. Without loss of generality, $bH \subset aH$, so $aH = bH$. Conversely, suppose $aH = bH$, then $a = ae_G \in bH$, so $a^{-1}b \in H$, thus $a \sim b$.

(c) It is trivial to prove $\sim_L$ is an equivalence relation. To prove the it satisfies the given property, $a \sim_L b \Rightarrow a^{-1}b \in H \Rightarrow (ga)^{-1}(gb) = a^{-1}b \in H \Rightarrow ga \sim_L g_b$. ■

Proposition 2.19

There is a one-to-one correspondence between subgroups of G and equivalence relations on G satisfying $a \sim b \Rightarrow ga \sim gb$; for the relation $\sim_L$ corresponding to a subgroup H, $G/\sim_L$ may be described as the set of left-cosets aH of H. ♠

Proof Follows directly from Proposition 2.18. ■

The preceding two proposition for right cosets are analogous.

Proposition 2.20

The relations $\sim_L$ and $\sim_R$ coincides if and only if H is normal. ♠

Definition 2.12 (Quotient Group)

*Let H be a normal subgroup of a group G. The **quotient group** of G modulo H, denoted G/H, is the group $G/\sim$ obtained from the relation $\sim$. In terms of cosets, the product G/H is defined by $(aH)(bH) = (ab)H$, and the identity element $e_{G/H}$ is the coset of the identity.* ♣

Proposition 2.21

Let H be a normal subgroup of a group G, then for every group homomorphism $\varphi : G \to G'$ such that $H \subset \ker\varphi$ there exists a unique group homomorphism $\tilde{\varphi} : G/H \to G'$ so that the diagram

$$\begin{tikzcd}
G/H \arrow[rr, dashed, "\tilde{\varphi}"] & & G' \\
& G \arrow[ul, "\pi"] \arrow[ur, "\varphi"'] &
\end{tikzcd}$$

commutes.

Proof $H \subset \ker\varphi$ implies $a^{-1}b \in H \Rightarrow \varphi(a) = \varphi(b)$. By the definition of relation $\sim$ corresponding to H, then $a \sim b \Rightarrow a^{-1}b \Rightarrow \varphi(a) = \varphi(b)$. Hence by Proposition 2.17 there is an unique desired homomorphism $\tilde{\varphi}$. ■

$$\begin{tikzcd}
G/H \arrow[rr, dashed, "\tilde{\varphi}"] & & G' \\
& G \arrow[ul, "\pi"] \arrow[ur, "\varphi"'] &
\end{tikzcd}$$

2.7 Canonical Decomposition and Lagrange's Theorem

2.7.1 Canonical Decomposition and Isomorphism Theorems

Proposition 2.22

Every group homomorphism $\varphi : G \to G'$ may be decomposed as follows:

$$\begin{tikzcd} G \arrow[r, two heads] \arrow[rrr, bend left, "\varphi"] & G/\ker\varphi \arrow[r, "\sim", "\tilde{\varphi}"'] & \mathit{im}\,\varphi \arrow[r, hook] & G' \end{tikzcd}$$

where the isomorphism $\tilde{\varphi}$ in the middle is the homomorphism induced by φ. ♠

Theorem 2.2 (First Isomorphism Theorem)

Suppose $\varphi : G \to G'$ is a surjective group homomorphism. Then $G' \cong G/\ker\varphi$. ♡

Proof Since $\operatorname{im}\varphi = G'$, it follows that $\tilde{\varphi}$ is an isomorphism between $G/\ker\varphi$ and $\operatorname{im}\varphi = G'$. ■

Proposition 2.23

If $H_1 \trianglelefteq G_1$ and $H_2 \trianglelefteq G_2$, then $H_1 \times H_2 \trianglelefteq G_1 \times G_2$, and $(G_1 \times G_2)/(H_1 \times H_2) \cong (G_1/H_1) \times (G_2/H_2)$. ♠

Proof Define $\pi = \pi_1 \times \pi_2 : G_1 \times G_2 \to (G_1/H_1) \times (G_2/H_2)$ explicitly by $\pi(g_1, g_2) = (g_1H_1, g_2H_2)$, i.e., the product of compositions between projection and morphism to the quotient; $\tilde{\pi}$ is a surjective homomorphism whose kernel is $H_1 \times H_2$, the proposition follows immediately from Theorem 2.2. ■

Example 2.7 The cyclic group C_6 can be identified as $C_2 \times C_3$, so $C_6/C_3 \cong (C_2 \times C_3)/C_3 \cong C_2$.

The cyclic group C_3 can be viewed as a subgroup of the dihedral group C_6. Then C_3 is normal in D_6 and $D_6/C_3 \cong C_2$.

Presentation Every group is a quotient of a free group, and every abelian group is a quotient of a free abelian group. A ***presentation*** of a group G is an explicit isomorphism $G \cong F(A)/R$ where $A \in \textsc{Set}$ and R is a subgroup relations; that is, a presentation is an explicit surjection $\rho : F(A) \twoheadrightarrow G$ of which R is the kernel.

A presentation is usually encoded as a pair $(A \,|\, \mathcal{R})$, where A is a set and $\mathcal{R} \subset F(A)$ is a set of words such that $\ker\rho = R$ is generated by $\mathcal{R}$.

Example 2.8 The symmetry group S_3 can be presents as a quotient of the free group $F(\{x, y\})$ by the smallest normal subgroup containing x^2, y^3, and $yx = xy^2$, namely S_3 is $(x, y \,|\, x^2, y^3, xyxy)$.

Proposition 2.24

Suppose $H \trianglelefteq G$, then for every $K \leq G$ containing H, K/H may be identified with a subgroup G/H. The function

$$u : \{\textit{subgroups } K \textit{ of } G \textit{ containing } H\} \to \{\textit{subgroups of } G/H\}$$

defined by $u(K) = K/H$ is a bijection preserving inclusions. ♠

Remark In other words, every subgroup H' of G/N can be written as $H' = H/N$ for some $H \leq G$.

Proof For every subgroup K containing H, $K/H = \{aH \,|\, a \in K\} \subset G/K$, then it is not hard to verify $K/H \leq G/H$ since $aH, bH \in K/H \Rightarrow a, b \in H \Rightarrow ab^{-1} \in H \Rightarrow (aH)(bH)^{-1} \in K/H$.

u preserves inclusions: if $H \subset K \subset K'$, $u(K) = K/H \subset K'/H = u(K')$. Define $v(K') = \{a \in G \,|\, aH \in K'\}$ for every $K' \leq G/H$. It is not hard to show $v(K')$ is a subgroup and v is the inverse of u. Hence u is a bijection preserving inclusions. ■

Theorem 2.3 (Second Isomorphism Theorem)

Denote by AB the subset $AB := \{ab \,|\, a \in A, b \in B\}$. Let $H \trianglelefteq G$ and $K \leq G$. Then

(a) HK is a subgroup of G, and H is normal in HK;

(b) $H \cap K$ is normal in K, and $HK/H \cong K/(H \cap K)$. ♡

Proof (a) Suppose $k_1h_1, k_2h_2 \in HK$. Note that H is normal, so $k_1(h_1h_2^{-1}) = h'k_1$ for some $h' \in H$. Then $(k_1h_1)(k_2h_2)^{-1} = (k_1h_1h_2^{-1})k_2^{-1} = h'k_1k_2 \in HK$, so HK is a subgroup of G. It is clear that H is normal in $HK \leq G$.

(b) $H \cap K$ is clearly normal in K since $H \trianglelefteq G$. Consider $\varphi : K \to HK/H$ defined by $\varphi(k) = Hk$. φ is surjective: for all $Hhk \in HK/H$, $Hhk = Hk = \varphi(k)$. The kernel of φ is $\ker\varphi = \{k \in K \,|\, \varphi(k) = Hk = H\} = H \cap K$. Hence $K/(H \cap K) \cong HK/H$ by the first isomorphism theorem. ■

Theorem 2.4 (Third Isomorphism Theorem)

Let $H \leq N \leq G$ for which $H \trianglelefteq G$. Then N/H is normal in G/H if and only if N is normal in G, and in this case, $(G/H)/(N/H) \cong G/N$. ♡

Proof N/H is normal if and only if for all $gH \in G/H$ and $nH \in N/H$, $(gH)(nH)(gH)^{-1} = (ghg^{-1})H \in N/H$, which holds if and only if $ghg^{-1} \in N$, namely $N \trianglelefteq G$ by definition.

In this case, define $\varphi : G/H \to G/N$ by $\varphi(gH) = gN$. φ is well-defined because $g_1H = g_2H \implies g_1g_2^{-1} \in H \subset N \implies g_1N = g_2N$. φ is surjective because for all $gN \in G/N$, $\varphi(gH) = gN$. The kernel of φ is $\ker\varphi = \{gH \,|\, gN = N\} = \{gH \,|\, g \in N\} = N/H$. Hence $(G/H)/(N/H) = (G/H)/\ker\varphi \cong G/N$ by the first isomorphism theorem. ■

2.7.2 The Lagrange Theorem

Definition 2.13 (Index)

*The notation G/H denote the set of left-cosets of H, regardless of whether H is normal in G. The **index** of H in G, denoted $[G : H]$, is the number of elements $|G/H|$ of G/H, when this is finite, and ∞ otherwise.* ♣

Theorem 2.5 (Lagrange's Theorem)

If G is a finite group and $H \subset G$ is a subgroup, then $|G| = [G : H] \cdot |H|$. In particular, $|H|$ is a divisor of $|G|$. ♡

Proof For all $g \in G$, the function $\lambda_g : H \to gH$ defined by $\lambda_g(h) = gh$ is clearly a bijection, so $|H| = |gH|$. Note that G is the disjoint union of $[G : H]$ distinct cosets gH, so $|G| = [G : H] \cdot |gH| = [G : H] \cdot |H|$. ■

Example 2.9

- The order $|g|$ if any element g of a finite group G is a divisor of $|G|$, indeed, $|g|$ equals the order of subgroup $\langle g \rangle$ generated by g.
- If $|G|$ is a prime integer p, the necessarily $G \cong \mathbb{Z}_p$.

Note *The index is multiplicative: if $H \leq K \leq G$, then $[G : H] = [G : K][K : H]$, provided that the indices are finite. By second isomorphism theorem, if $H \trianglelefteq G$ and $K \leq G$, then $|HK| = (|H| \cdot |K|)/|H \cap K|$.*

2.7.3 Epimorphisms and Cokernels

Note *Define the cokernel coker φ equipped with a homomorphism $\pi : G' \to$ coker φ to be the universal solution to*

$$\begin{tikzcd}
K & & \text{coker}\,\varphi \arrow[ll, dashed, "\tilde{\alpha}"'] \\
& G' \arrow[ul, "\alpha"] \arrow[ur, "\pi"'] & \\
& G \arrow[u, "\varphi"'] \arrow[uul, bend left, "0"] \arrow[uur, bend right, "0"'] &
\end{tikzcd}$$

In Ab, *im φ is a subgroup and hence a normal subgroup of G', so coker $\varphi \cong G'/$im φ. However, im φ is not necessarily normal in* Grp. *Let's consider the abelian case:*

Proposition 2.25

Let $\varphi : G \to G'$ be a homomorphism of abelian groups. The following are equivalent:

(a) φ is an epimorphism;

(b) coker φ is trivial;

(c) $\varphi : G \to G'$ is surjective (as a set-function); ♠

Remark For analogous statement of monomorphisms, see Proposition 2.15.

Proof $(a) \Rightarrow (b)$: Suppose φ is an epimorphism, consider $\pi : G' \to G'/\mathrm{im}\,\varphi$ defined by $\pi(g) = g\,\mathrm{im}\,\varphi$ and the trivial homomorphism e. The following diagram commutes:

$$\begin{tikzcd}
G \arrow[r] & G' \arrow[r, bend left, "\pi"] \arrow[r, bend right, "e"'] & \text{coker}\,\varphi
\end{tikzcd}$$

so $\pi = e$, it follows that coker φ is trivial.

$(b) \Rightarrow (c)$: Suppose coker $\varphi = G'/\mathrm{im}\,\varphi$ is trivial, im $\varphi = G'$, so φ is surjective.

$(c) \Rightarrow (a)$: Suppose φ is surjective, it is an epimorphism in Set. In particular, $\alpha \circ \varphi = \alpha' \circ \varphi$ implies $\alpha = \alpha'$ if α and α' are homomorphisms, so φ is an epimorphism in Grp. ■

2.8 Group Actions

2.8.1 Group Actions

Definition 2.14 (Group Action)

*An **action** of group G on an object A of a category $\mathcal{C}$ is a homomorphism $\sigma : G \to Aut_{\mathcal{C}}(A)$, it is **faithful** (or **effective**) if $\sigma : G \to Aut_{\mathcal{C}}(A)$ is injective.* ♣

Definition 2.15 (Group Action on a Set)

An action of a group G on a set A is a set-function $\rho : G \times A \to A$ such that

(a) $\rho(e_G, a) = a$ for all $a \in A$, and

(b) for all $g, h \in G$ and for all $a \in A$, $\rho(gh, a) = \rho(g, \rho(h, a))$. ♣

Remark That is, if we denote g acts on a by $g \bullet a$, then (a) $e_G \bullet a = a$ and (b) $(gh) \bullet a = g \bullet (h \bullet a)$.

We can define $\sigma : G \to S_A = \text{Aut}(A)$ by $\sigma(g)(a) = \rho(g, a)$. This function preserves the operation $\sigma(gh)(a) = \sigma(g) \circ \sigma(h)(a)$, and the image of σ consists of invertible set-functions since $\sigma(g^{-1})$ acts as the inverse of $\sigma(g)$. Hence $\sigma : G \to S_A$ is a desired homomorphism. Indeed, there is a bijection between the set of actions and the set of actions on a set, implying that the two definitions are equivalent.

Note *The action is faithful if and only if the identity e_G is the only element g of G such that $g \bullet a = a$ for all $a \in A$.*

Example 2.10

- The *left translation* $\rho : G \times G \to G$ defined by $\rho(g, h) = gh$ is a group action of G on itself.
- The conjugation action defined by $\rho(g, h) = ghg^{-1}$ is another action of G on itself.
- The left translation of left cosets $\rho(g, aH) = (ga)H$ is an action of G on G/H.

Proposition 2.26 (Cayley's Theorem)

Every group acts faithfully on some set. That is, every group may be realized as a subgroup of a permutation group. ♠

Proof The action of left-multiplication $\sigma : G \to \text{Aut}_{\text{Grp}}(G)$ defined by $\sigma(g)(h) = gh$ is a faithful group action. ■

Definition 2.16 (Transitive Action, Free Action)

*An action of a group G on a set A is **transitive** if for all $a, b \in A$, there exists $g \in G$ such that $b = g \bullet a$.*

*An action is **free** if e_G is the only element fixing any element of A.* ♣

Definition 2.17 (Orbit, Stabilizer)

*The **orbit** of $a \in A$ under an action of group G is the set $O_G(a) := \{g \bullet a \,|\, g \in G\}$. The **stabilizer** subgroup of $a \in A$ consists of element of G which fix a, i.e., $Stab_G(a) := \{g \in G \,|\, g \bullet a = a\}$.* ♣

2.8.2 The Category of G-Set

The Category of G-Set For every group G, sets endowed with a G-action form a category G-Set: the objects are pairs (ρ, A) where $\rho : G \times A \to A$ is an action, and morphisms between objects are set-functions which are compatible with the actions. That is, a morphism $(\rho, A) \to (\rho', A')$ in G-Set amounts to a set-function $\varphi : A \to A'$ such that the diagram

$$\begin{tikzcd}
G \times A \arrow[r, "\mathrm{id}_G \times \varphi"] \arrow[d, "\rho"'] & G \times A' \arrow[d, "\rho'"] \\
A \arrow[r, "\varphi"'] & A'
\end{tikzcd}$$

commutes. That is, $g \bullet \varphi(a) = \varphi(g \bullet a)$ (such functions are called ***equivariant***). The isomorphisms of G-Set are indeed the equivariant bijections.

Proposition 2.27

Every transitive left-action of G on a set A is isomorphic to the left-multiplication of G on G/H for $H = Stab_G(a)$ of any $a \in A$. ♠

Proof Define $\varphi : G/H \to A$ by $\varphi(gH) = g \bullet a$. φ is well-defined: $g_1 H = g_2 H \Rightarrow g_1 g_2^{-1} \in H \Rightarrow g_1 g_2^{-1} \bullet a = a \Rightarrow g_1 \bullet a = g_2 \bullet a$. Since $\varphi(g'(gH)) = g' \bullet \varphi(gH)$, φ is equivariant. To verify φ is bijective, define $\psi : A \to G/H$ by $\psi(g \bullet a) = gH$, this is well-defined because the action is transitive, and it is clear that ψ and φ are inverse of each other, so φ is bijective. ■

Remark The above proposition implies that $O_G(a)$ and $G/\mathrm{Stab}_G(a)$ are bijective. Then the Orbit-Stabilizer theorem $|G| = |O_G(a)| \cdot |\mathrm{Stab}_G(a)|$ follows immediately.

Proof: Define $\varphi : G/H \to O_a$ (where $H = \mathrm{Stab}_G(a)$) by $\varphi(g) = g \bullet a$. Note that

$$x_1 H = x_2 H \Leftrightarrow x_1^{-1} x_2 \in H \Leftrightarrow x_1^{-1} x_2 \bullet a = a \Leftrightarrow \varphi(x_1 H) = x_1 \bullet a = x_2 \bullet a = \varphi(x_2 H),$$

thus, the mapping φ is well-defined and injective. It is clearly surjective. Hence φ is a bijection. ■

Corollary 2.2

If $O_G(a)$ is an orbit of the action of a finite group G in a set A, then $O_G(a)$ is finite and $|O_G(a)|$ divides $|G|$. ♡

Proposition 2.28

Suppose a group acts on a set A, and let $a \in A$, $g \in G$, $b = g \bullet a$. Then Stab$_G(b) = g$Stab$_G(a)g^{-1}$. ♠

Proof Suppose $h \in \text{Stab}_G(a)$, note that $a = g^{-1} \bullet b$, then $(ghg^{-1}) \bullet b = gh \bullet a = g \bullet a = b$, so $g\text{Stab}_G(a)g^{-1} \subset \text{Stab}_G(b)$. The inclusion of other direction follows without loss of generality. ■

Remark In other words, the stabilizers of an action are isomorphic if they are in the same class (i.e., they have the same orbit).

Chapter 3 Group Theory II

Introduction

- *Center, Centralizer, and Normalizer*
- *Sylow Theorems*
- *Class Formula*
- *Semidirect Product*
- *Symmetric Group, Alternating Group*
- *Classification of Finite Abelian Group*

3.1 The Conjugation Action

3.1.1 Center, Centralizer, Conjugacy Classes

Definition 3.1 (Center)

The ***center*** *of G, denoted $Z(G)$, is the subgroup $\ker\sigma$ of G, where σ is the conjugate action. In other words, $Z(G) := \{g \in G \mid \forall\, a \in G : ga = ag\}$.* ♣

Remark For conjugate action, the center $Z(G)$ fixes every element $g \in G$ when acting on itself, and they are fixed points G acts on them. That is, for all $a \in G$, $g \bullet a = a$ and $a \bullet g = g$.

Remark $Z(G)$ is abelian and thus normal in G.

Lemma 3.1

Let G be a finite group, if $G/Z(G)$ is cyclic, then G is commutative and hence $G/Z(G)$ is trivial. ♡

Proof Suppose $G/Z(G)$ is generated by $xZ(G)$. For all $g_1 \in G$, $g_1 \in x^m Z(G)$ so $g_1 = x^n h_1$ for some $h_1 \in Z(G)$. Similarly, $g_2 = x^m h_2$ for $h_2 \in Z(G)$. Then

$$g_1 g_2 = (x^n h_1)(x^m h_2) = x^{n+m} h_1 h_2 = (x^m h_2)(x^n h_1) = g_2 g_1,$$

so G is commutative. ■

Definition 3.2 (Centralizer of a)

The ***centralizer*** *of $a \in G$ is its stabilizer under conjugation, namely $Z_G(a) = \{g \in G \mid gag^{-1} = a\} = \{g \in G \mid ga = ag\}$.* ♣

Remark The centralizer $Z_G(a)$ fixes a when acting as conjugate action on itself, and they are fixed when a acts on them. That is, $g \bullet a = a$ and $a \bullet g = g$

Definition 3.3 (Conjugacy Class)

*The **conjugacy class** of $g \in G$ is the orbit $[g]$ of g under the conjugation action. Two elements $g, h \in G$ are **conjugate** if they belong to the same conjugacy class.* ♣

Remark Normal subgroup of a group is a disjoint union of conjugacy classes.

3.1.2 Class Formula

Proposition 3.1 (Class Formula)

Let G be a group acting on a finite set S, and Z be the fixed points of the action. Then $|S| = |Z| + \sum_{a\in A}[G : G_a]$, where $A \subset G$ is a set containing one representative for each nontrivial orbit in G.

In particular, when considering the conjugation action of G on itself, we have

$$|G| = |Z(G)| + \sum_{a\in A}[G : Z_G(a)]$$

*as known as the **class formula**.* ♠

Proof The orbit form a partition of S, and Z collects the trivial orbits, so $|S| = |Z| + \sum_{a\in A}|O_a|$. Note that $|O_a| = |G/G_a| = [G : G_a]$ by Proposition 2.27, this yields the desired formula. ■

Definition 3.4 (p-group)

*A **p-group**, where p is prime, is a finite group G such that $|G| = p^n$ for some $n \in \mathbb{Z}$.* ♣

Corollary 3.1

(a) Let G be a p-group acting on a finite set A, and let Z be the fixed point set, then $|Z| \equiv |S| \pmod{p}$.

(b) Let G is be a nontrivial p-group, then $Z(G)$ is nontrivial. ♡

Proof (a) Since $O_a \cong G/G_a$ is a nontrivial subgroup of S, so p divides $[G : G_a]$. Then $|S| = |Z| + \sum_{a\in A}[G : G_a] \equiv |Z| \pmod{p}$.

(b) By part (a) and the class formula, $|Z(G)| \equiv |G| \equiv 0 \pmod{p}$, so $Z(G)$ is nontrivial. ■

3.1.3 Conjugation of Subsets and Subgroups

The ***conjugation*** of A is the subset gAg^{-1}, and it is not hard to verify that $A \cong gAg^{-1}$.

Definition 3.5 (Centralizer and Normalizer of A)

*The **normalizer** $N_G(A)$ of A is its stabilizer under conjugation, i.e., $N_G(A) := \{g \in G \,|\, gA = Ag\}$. The **centralizer** of A is the subgroup $Z_G(A) \subset N_G(A)$ fixing each element of A, i.e., $Z_G(A) := \{g \in G \,|\, \forall\, a \in$*

$A : ga = ag\}$. ♣

Remark Centralizer and normalizer of a subgroup A of G are subgroups of G, and $Z_G(A)$ is a normal subgroup of $N_G(A)$.

In addition, if A is a subgroup of G, then A is the largest normal subgroup in $N_G(A)$.

Lemma 3.2

Let $H \subset G$ be a subgroup. Then (if finite) the number of subgroups conjugate to H equals the index $[G : N_G(H)]$ of the normalizer of H in G. ♡

Proof Consider the group action defined by $g \bullet A = gAg^{-1}$. Note that $\text{Stab}_G(H) = \{g \in G \,|\, gAg^{-1} = A\} = N_G(H)$, then the orbit-stabilizer theorem gives that $|\{gAg^{-1} \,|\, g \in G\} = ||O_A| = [G : N_G(G)]$. ■

3.2 Symmetric Group

3.2.1 Cycles and Types

Definition 3.6 (Cycle Notation)

A (nontrivial) ***cycle*** *is an element S_n with exactly one nontrivial orbit. For distinct $a_1, \cdots, a_r$, the notation $(a_1 a_2 \cdots a_r)$ denotes the cycle in S_n with nontrivial orbit $\{a_1, \cdots, a_r\}$, acting as $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_r \mapsto a_1$. In this case, r is the length of the cycle, and the cycle is called an* ***r-cycle****.* ♣

That is, $\sigma(a_r) = a_1$, $\sigma(a_i) = a_{i+1}$ for $i < r$, and $\sigma(a) = a$ for all $a \notin \{a_1, \cdots, a_r\}$. Note that $(a_1 a_2 \cdots a_r) = (a_2 \cdots a_r a_1)$, so the notation is determined up to a cyclic permutation.

Property *Disjoint cycles, i.e., cycles whose nontrivial orbits are disjoint, commute.*

Proposition 3.2

Every $\sigma \in S_n$, $\sigma \neq e$, can be written as a product of disjoint nontrivial cycles, in a unique way up to permutation of the factors. ♠

Proof Every $\sigma \in S_n$ determines a partition into orbits under $\langle\sigma\rangle$, and $\langle\sigma\rangle$ has nontrivial orbits. As σ acts as cycles on each orbit, σ may be written as a product of cycles. The proof for uniqueness is omitted. ■

Definition 3.7 (Type)

The ***type*** *of $\sigma \in S_n$ is the partition of n given by the sizes of the orbits of the action of $\langle\sigma\rangle$ on $\{1, \cdots, n\}$.* ♣

Example 3.1 Suppose $\sigma = (18632)(47) \in S_8$, then σ has type $[5, 2, 1]$.

Lemma 3.3

Let $\tau \in S_n$ and let $(a_1, \cdots, a_r)$ be a cycle. Then $\tau(a_1, \cdots, a_r)\tau^{-1} = (a_1\tau^{-1}, \cdots, a_r\tau^{-1})$, where $a_1\tau^{-1}$ denotes the right action of permutation τ^{-1} on a_1. ♡

Proof For $1 \leq i < r$, $(a_i\tau^{-1})(\tau(a_1, \cdots, a_r)\tau^{-1}) = a_i(a_1, \cdots, a_r)\tau^{-1} = a_{i+1}\tau^{-1}$; and $(a_r\tau^{-1})(\tau(a_1, \cdots, a_r)\tau^{-1})$ $= a_1\tau^{-1}$ similarly. On the other hand, for $a' \notin \{a_i\tau^{-1}\}$, $a' = a\tau^{-1}$ for some $a \notin \{a_i\}$, so $a'(\tau(a_1, \cdots, a_r)\tau^{-1}) = a(a_1, \cdots, a_r)\tau^{-1} = a\tau^{-1} = a'$. ■

Remark This formula extends to the product of cycles, regardless whether they are disjoint or not, by inserting identity factors $\tau^{-1}\tau$. That is, $\tau(a_1 \cdots a_n)(b_1 \cdots b_m)\tau^{-1} = (a_1\tau^{-1} \cdots a_n\tau^{-1})(b_1\tau^{-1} \cdots b_m\tau^{-1})$.

Proposition 3.3

Two elements of S_n are conjugate in S_n if and only if they have the same type. ♠

Proof The forward direction follows immediately from Lemma 3.3. Conversely, suppose σ and σ' have the same type, consider their cycle decomposition. For each cycle $(a_1 \cdots a_n)$ in σ, there is a corresponding cycle $(a_1' \cdots a_n')$ in σ'we define $\tau(a_i') = a_i$. τ is well-defined and bijective because orbits form a partition. Then it is clear that $\tau\sigma\tau^{-1} = \sigma'$. ■

Corollary 3.2

The number of conjugacy classes in S_n equals the number of partitions of n. ♡

3.2.2 Transposition, Parity, Alternating Group

For $n \geq 1$, define the polynomial Δ_n by $\Delta_n = \prod_{1\leq i\leq j\leq n}(x_i - x_j)$. We can acts with any σ on Δ_n, by permuting the indices according to σ:

$$\Delta_n\sigma = \prod_{1\leq i\leq j\leq n}(x_{i\sigma} - x_{j\sigma}),$$

and $\Delta_n\sigma = \pm\Delta_n$.

Definition 3.8 (Transposition, Sign)

A ***transposition*** *is a cycle of length 2. The* ***sign*** *of a permutation $\sigma \in S_n$, denoted $(-1)^\sigma$, is determined by the action of σ on Δ_n: $\Delta_n\sigma = (-1)^\sigma\Delta_n$. We say σ is even if $(-1)^\sigma = +1$ and odd if $(-1)^\sigma = -1$.* ♣

Remark The sign function $\epsilon : S_n \to \{\pm 1\}$ defined by $\epsilon(\sigma) = (-1)^\sigma$ is a homomorphism since $\Delta_n(\sigma r) = (\Delta_n\sigma)r$ so that $(-1)^{\sigma r} = (-1)^\sigma(-1)^r$.

Lemma 3.4

Transpositions, namely cycles of length 2, generate S_n. ♡

Proof For all cycles $(a_1 \cdots a_n)$, $(a_1 \cdots a_n) = (a_1a_2)(a_1a_3)\cdots(a_1a_n)$, so the assertion follows immediately from Proposition 3.2. ■

Proposition 3.4

Let $\sigma = \tau_1 \cdots \tau_r$ be a product of transpositions. Then σ if even, resp., odd, according to whether r is even, resp., odd. ♠

Proof For each transposition τ, $\epsilon(\tau) = -1$. Suppose $\sigma = \tau_1 \cdots \tau_r$, the homomorphism implies that $(-1)^\sigma = \epsilon(\tau_1 \cdots \tau_r) = (-1)^r$. ■

Definition 3.9 (Alternating Groups)

The ***alternating group*** *on $\{1, \cdots, n\}$, denoted A_n, consists of all even permutation $\sigma \in S_n$.* ♣

Note *The alternating group A_n is a normal subgroup of S_n, and $[S_n : A_n] = 2$. Indeed, consider the sign function $\epsilon : S_n \to \{\pm 1\}$, the alternating group A_n is the kernel of ϵ.*

Note *The cycle is even, resp., odd, if it has odd, resp., even length. Then a permutation σ belongs to A_n if and only if n and the number of rows in the Young diagram have the same parity, namely n and len(type(σ)) have the same parity.*

3.2.3 Conjugacy, Simplicity, and Solvability

Denote by $[\sigma]_{S_n}$, resp., $[\sigma]_{A_n}$, the conjugacy class of an even permutation σ in S_n, resp., A_n.

Lemma 3.5

Let $n \geq 2$ and $\sigma \in A_n$. Then $[\sigma]_{A_n} = [\sigma]_{S_n}$ or the size of $[\sigma]_{A_n}$ is half the size of $[\sigma]_{S_n}$, according to whether the centralizer $Z_{S_n}(\sigma)$ is not or is contained in A_n.

Proof Suppose $Z_{S_n}(\sigma) \subset A_n$. Note that $Z_{S_n}(\sigma) = Z_{A_n}(\sigma)$, then $|[\sigma]_{S_n}| = [S_n : Z_{S_n}(\sigma)] = 2 \cdot [A_n : Z_{A_n}(\sigma)] = 2 \cdot |[\sigma]_{A_n}|$. Conversely, suppose $Z_{S_n}(\sigma) \cap (S_n \setminus A_n) \neq \varnothing$, let τ be such an element. Then for all $\varphi \notin A_n$, $\alpha\sigma\alpha^{-1} = (\varphi\tau)\sigma(\varphi\tau)^{-1} \in [\sigma]_{A_n}$, so $[\sigma]_{S_n} \subset [\sigma]_{A_n}$, it follows that $[\sigma]_{A_n} = [\sigma]_{S_n}$. ■

Remark Alternatively, by the second isomorphism theorem, $[Z_{S_n} : Z_{S_n} \cap A_n] = [A_n Z_{S_n} : A_n]$. Since $A_n Z_{S_n} \leq S_n$. Also note that $Z_{A_n} = Z_{S_n} \cap A_n$, then $[Z_{S_n} : Z_{A_n}] = [Z_{S_n} : Z_{S_n} \cap A_n]$ divides $[S_n : A_n] = 2$, so the index can only be 1 or 2. The index is one if and only if $Z_{S_n} \subset A_n$. Then the assertion follows from the orbit-stabilizer theorem, i.e., $|[\sigma]_{A_n}| = [A_n : Z_{A_n}]$ and $|[\sigma]_{S_n}| = [S_n : Z_{S_n}]$.

Conjugacy classes of even permutations either are preserved from S_n to A_n or they split into two distinct, equal-sized classes. The conjugacy class $[\sigma]_{S_n}$ splits into $[\sigma]_{A_n}$ and $[\sigma']_{A_n}$ if $\sigma' \notin [\sigma]_{A_n}$ and $\sigma' = \tau\sigma\tau^{-1}$ for some $\tau \notin A_n$.

Proposition 3.5

Let $\sigma \in A_n$, $n \geq 2$. Then the conjugacy class of σ in S_n splits into two conjugacy classes in A_n if and only if the type of σ consists of distinct odd numbers.

Proof It suffices to prove the type of σ contains distinct odd numbers if and only if $Z_{S_n}(\sigma) \subset A_n$, namely $\tau\sigma\tau^{-1} = \sigma$ implies that $\tau \in A_n$, by Lemma 3.5.

($\Rightarrow$) Suppose the type of σ contains distinct odd numbers and $\tau\sigma\tau^{-1} = \sigma$. Then every cycle $(a_1 \cdots a_m)$ in the cycle decomposition must preserved under σ. That is, σ must be a cyclic permutation on $(a_1 \cdots a_m)$, so σ contains $(a_1 \cdots a_m)^r$, which is clearly even given that m is odd. Thus, σ is even as a product of even permutations.

($\Leftarrow$) Conversely, suppose the type contains an even number, i.e., σ contains $(a_1 \cdots a_m)$ for some even m. Consider $\tau = (a_1 \cdots a_m)$ and identity elsewhere. Then $\tau\sigma\tau^{-1} = \sigma$ and τ is odd. On the other hand, suppose two cycles have the same odd length, i.e., $(a_1 \cdots a_m)$ and $(b_1 \cdots b_m)$. Consider τ defined by $\tau = (a_1 b_1)(a_2 b_2) \cdots (a_m b_m)$. Then $\tau\sigma\tau^{-1} = \sigma$ and τ is odd. ■

Corollary 3.3

The alternating group A_5 is a ***simple*** *(a group is simple if the only normal subgroups are trivial subgroup and itself) non-commutative group of order* 60. ♡

Proof The class formula for A_5 is $60 = 1 + 15 + 20 + 12 + 12$ (note that the conjugacy class splits for the type $[5]$). Consider subgroups of A_5, their order must be one of $2, 3, 4, 5, 6, 10, 12, 15, 20, 30$ by Lagrange theorem. Excluding the identity element, the subgroup has order of $1, 2, 3, 4, 5, 9, 11, 14, 19, 29$. We see that none can be written as the sum of orders of conjugacy classes, so they cannot be written as the union of conjugacy classes, so none of them are normal. It implies that A_5 is simple. ■

3.3 Sylow Theorems

Theorem 3.1 (Cauchy's Theorem)

Let G be a finite group, and let p be a prime divisor of $|G|$. Then G contains an element of order p.

Proof Proceed by induction on $|G|$. The case is trivial for $|G| = 1$. Suppose $|G| > 1$. Assume G is abelian, we let $H = \langle g \rangle$ for some $g \neq e_G$.

(1) If $p \mid |H|$, then $|g^{|H|/p}| = p$.

(2) If $p \nmid |H|$, then $p \mid |G/H|$ and G/H is a subgroup with order less than $|G|$. By inductive hypothesis, there exists $xH \in G/H$ such that $|xH| = p$. Note that $(xH)^{|x|} = H$, so $p \mid |x|$. Then $|x^{|x|/p}| = p$.

On the other hand, assume $|G|$ is not abelian, we therefore consider the class formula $|G| = |Z(G)| + \sum [G : G_a]$.

(1) If $p \mid |Z(G)|$, then the desired result follows immediately from the fact that $Z(G)$ is abelian.

(2) If $p \nmid |Z(G)|$, then $p \nmid [G : G_a]$ for some $a \in G$, so $p \mid |G_a|$. Note that $G_a \leq G$, so by inductive hypothesis, there exists $x \in G_a$ such that $|x| = p$.

Hence there exists $x \in G$ such that $|x| = p$. ■

Remark By the class formula, p divides the order of either (i) a stabilizer G_a or (ii) the center $Z(G)$. In the later case, we let $H := \langle g \rangle \trianglelefteq G$ for some $g \in Z(G)$. Since p divides $|H| \cdot |G/H| = |G|$, then p divides the order of (ii.1) H or (ii.2) G/H. In either cases, we may proceed by induction.

Proof Sketch of Alternative Proof: Let $H = \{(a_1, \cdots, a_p) \mid a_1 \cdots a_p = e\}$, then $|H| = |G|^{p-1}$ is is divisible by p^{p-1} because $a_1, \cdots a_{p-1}$ can be chosen arbitrarily. Consider $\mathbb{Z}/p\mathbb{Z}$ acts on H by left translation, it is well-defined because $a_k \cdots a_p a_1 \cdots a_{k-1} = e$ for all k. Note that $[H : H_x]$ is divisible by p since $|H_x|$ divides p, so then the class formula implies that $|Z(H)| \equiv |H| \equiv 0 \pmod p$, and Z is nonempty. Then Z is nontrivial, i.e., there exists $x \in G$ such that $(x, \cdots, x) \in Z$, and hence $|x| = p$. ■

Definition 3.10 (Simple Group)

*A group G is **simple** if its only normal subgroups are $\{e\}$ and G itself.*

Definition 3.11 (p-Sylow group)

*Let p be a prime integer. A **p-Sylow subgroup** of a finite group G is a subgroup of order p^r where $|G| = p^r m$ and $\gcd(p, m) = 1$.*

Theorem 3.2 (First Sylow Theorem)

Every finite group contains a p-Sylow subgroup, for all primes p.

The first Sylow theorem follows from the stronger statement

Proposition 3.6

If p^k divides the order of G, then G has a subgroup of order p^k. ♠

Proof We may assume $p \,|\, |G|$ and $k \geq 1$. We proceed by induction on k. The $k = 1$ case follows immediately from Theorem 3.1. Suppose $k > 1$. Assume $p \,|\, Z(G)$, then there exists $x \in Z(G)$ such that $|x| = p$, so $N := \langle x \rangle$ is a normal subgroup that has order of p. Consider the quotient group G/N. Since $p^{k-1} \,|\, |G/N|$, the inductive hypothesis implies that there exists $H' \leq G/N$ such that $|H'| = p^{k-1}$. By the structure of subgroups of a quotient (Theorem 2.24), $H = H'/N$ for some $H \leq G$. Then $|H| = |H/N||N| = p^k$.

On the other hand, assume $p \nmid Z(G)$, the class formula implies that $p \nmid [G : G_a]$ for some $a \notin Z(G)$, so $p^k \,|\, |G_a|$. By inductive hypothesis, there exists a subgroup $H \leq G_a \leq G$ such that $|H| = p^k$. ■

Remark Suppose $|G| = p^r n$. If $p \,|\, Z(G)$, then $|G/N| = p^{r-1}n$ using quotient group by setting $N = \langle g \rangle$ for $p \,|\, |g|$. On the other hand, if $p \nmid Z(G)$, then $|G_a| = p^r m$ $(m < n)$ for some G_a, since $p \nmid [G : G_a]$ by class formula.

Theorem 3.3 (Second Sylow Theorem)

Let G be a finite group, let P be a p-Sylow subgroup, and let $H \subseteq G$ be a p-group. Then H is contained in a conjugate of P, i.e., there exists $g \in G$ such that $H \subseteq gPg^{-1}$. ♡

Proof Consider the left multiplication action by H on the left cosets G/P. Suppose $Z \subset G/P$ is the set of fixed points, then $|G/P| = |Z| + \sum [H : H_{gP}] \equiv |Z| \pmod p$ by Corollary 3.1. Since P is a p-Sylow subgroup, p does not divide $|G/P|$, so $|Z|$ is nonempty. Suppose $gP \in Z$, then $HgP = gP$, followed by $g^{-1}Hg \subset P$, hence $H \subset gPg^{-1}$. ■

Corollary 3.4 (Weaker Form of Theorem 3.3)

(a) All p-Sylow subgroups are conjugate of each other.

(b) Every maximal p-group in G is a p-Sylow subgroup. ♡

Remark The first Sylow theorem implies that some maximal p-group in G attains the largest size (i.e., p-Sylow subgroup), and the second Sylow theorem extends that every maximal p-group is a p-Sylow subgroup.

Proposition 3.7

Let H be a p-group contained in a finite group G. Then $[N_G(H) : H] \equiv [G : H] \pmod p$. ♠

Proof Consider the left multiplication action of H on G/H. Corollary 3.1 implies that $|G/H| = |Z| + \sum [H : H_{gH}] \equiv |Z| \pmod p$. Notice that $Z = \{gH \,|\, HgH = gH\} = \{gH \,|\, Hg = gH\} = N_G(H)/H$. Then $[G : H] \equiv |Z| = [N_G(H) : H] \pmod p$. ■

Proposition 3.8

Let H be a p-subgroup of a finite group G, and assume H is not a p-Sylow subgroup. Then there exists a p-subgroup H' of G containing H, such that $[H' : H] = p$ and H is normal in H'.

Remark This proposition, combined with first and second Sylow theorem, implies that for every G such that $|G| = p^r m$ and every H, there exists a chain $\{e\} \subset H_1 \subset H_2 \cdots H_r$ containing H, and for which $|H_k| = p^k$ and $H_k \trianglelefteq H_{k+1}$ for all k.

Proof Since H is a p-subgroup which is not p-Sylow, p divides $[G : H]$ and thus divides $[N_G(H) : H]$ by above proposition, so there exists $gH \in N_G(H)/H$ such that $|gH| = p$ by Cauchy Theorem. The subgroup $\langle gH \rangle \leq N_G(H)/H$ is of order p, and $\langle gH \rangle = H'/H$ for some $H' \leq N_G(H)$ by the structure of quotient group. Then $[H' : H] = |\langle gH \rangle| = p$, and $H \trianglelefteq H'$ because $H' \subset N_G(H)$. ■

Theorem 3.4 (Third Sylow Theorem)

Let p be a prime integer, and let G be a finite group of order $|G| = p^r m$. Assume that p does not divide m. Then the number of p-Sylow subgroups of G divides m and is congruent to 1 modulo p.

Proof Suppose K_p denotes the number of p-Sylow subgroups. According to second Sylow theorem (3.3), assume P is a p-Sylow subgroup, then Q is a p-Sylow subgroup if and only if it is conjugate to P, followed by K_p is precisely $[G : N_G(P)]$ by the orbit-stabilizer theorem.

It follows that $m = [G : P] = [G : N_G(P)][N_G(P) : P] = K_p[N_G(P) : P]$, so K_p divides m.

Indeed, $m = K_p[N_G(P) : P] \equiv K_p[G : P] = K_p m \pmod{p}$ by Proposition 3.7. Since $\gcd(m, p) = 1$, the cancellation law implies that $K_p \equiv 1 \pmod{p}$. ■

3.4 Products of Groups

3.4.1 Direct Product, Exact Sequence

Definition 3.12 (Commutator)

*The **commutator** $[A, B]$ of two subsets A, B of G is the subgroup generated by all commutators $[a, b] := aba^{-1}b^{-1}$.* ♣

Proposition 3.9

Let N, H be normal subgroups of a group G, then $[N, H] \subseteq N \cap H$. ♠

Proof It suffices to verify this on generators $[n, h]$: note that $[n, h] = (nhn^{-1})h^{-1} \in Hh^{-1} = H$ and $[n, h] = n(hn^{-1}h^{-1}) \in nN = N$, then $[n, h] \in N \cap H$. ■

Corollary 3.5

Let N, H be normal subgroups of a group G. If $N \cap H = \{e\}$, then N, H commute with each other: $nh = hn$ for every $n \in H$, $h \in H$. ♡

Proof It follows immediately from the above proposition that $[N, H] = \{e\}$, so $[n, h] = nhn^{-1}h^{-1} = e$, followed by $nh = hn$, for every $n \in H, h \in H$.

Proposition 3.10

Let N, H be normal subgroups of G, such that $N \cap H = \{e\}$, then $NH \cong N \times H$. ♠

Proof Consider $\varphi : N \times H \to NH$ defined by $\varphi(n, h) = nh$. It is a homomorphism because $\varphi((n_1, h_1) \cdot (n_2, h_2)) = \varphi(n_1 n_2, h_1 h_2) = n_1 n_2 h_1 h_2 = n_1 h_1 n_2 h_2 = \varphi(n_1, h_1)\varphi(n_2, h_2)$. φ is clearly surjective by the definition of NH; φ is injective since $\varphi(n, h) \in \ker \varphi$ if and only if $nh = e$, followed by $h = n^{-1} \in N \Rightarrow h \in N \cap H = \{e\} \Rightarrow h = e$, and $n = e$ without loss of generality. Hence φ is an isomorphism. ■

Definition 3.13 (Short Exact Sequence, Group Extension)

*A **(short) exact sequence** of groups is a sequence of groups and group homomorphisms*

$$1 \longrightarrow N \xrightarrow{\varphi} G \xrightarrow{\psi} H \longrightarrow 1$$

where φ is injective, ψ is surjective, and $\operatorname{im} \varphi = \ker \psi$. That is, the sequence is exact if $N \trianglelefteq G$ and ψ induces an isomorphism $G/N \to H$.

*Given an (short) exact sequence, we say that G is an **extension** of H by N.* ♣

Remark In the general case, a sequence $G_1 \xrightarrow{\varphi_1} G_2 \cdots \xrightarrow{\varphi_n} G_{n+1}$ is exact at G_i if $\operatorname{im}(\varphi_i) = \ker(\varphi_{i+1})$ by definition, and the sequence is an exact sequence if it is exact at every G_i.

In particular, consider the short sequence $1 \longrightarrow N \xrightarrow{\varphi} G \xrightarrow{\psi} H \longrightarrow 1$. Then the sequence is exact if and only if φ is injective, ψ is surjective, and $\operatorname{im}(\varphi) = \ker(\psi)$.

Hence every short exact sequence of groups is equivalent to a short exact sequence of the form $1 \longrightarrow \ker\varphi \hookrightarrow G \twoheadrightarrow G/\ker\varphi \longrightarrow 1$.

Example 3.2 For example, $1 \longrightarrow N \longrightarrow N \times H \longrightarrow H \longrightarrow 1$ is an exact sequence by defining $\varphi : n \to (n, e_H)$ and $\psi : (n,h) \to (e_N, h)$. However, G is not necessarily isomorphic to $N \times H$, for instance, $1 \longrightarrow C_3 \longrightarrow S_3 \longrightarrow C_2 \longrightarrow 1$ is an exact sequence, yet $S_3 \ncong C_3 \times C_2$. Indeed, in this case, there are two extensions of C_2 by C_3: $C_6 \cong C_3 \times C_2$ and S_3.

Definition 3.14 (Split Extension)

An exact sequence of groups $1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1$ (or the corresponding extension) is said to ***split*** *if H may be identified with a subgroup of G so that $N \cap H = \{e\}$.* ♣

Lemma 3.6

Let N be a normal subgroup of a group G, and let H be a subgroup of G such that $G = HN$ and $N \cap H = \{e\}$. Then G is a split extension of H by N. ♡

Proof By the second isomorphism theorem, $G/N = NH/N \cong H/(N \cap H) \cong H$, so G is an extension of H by N. Since H is a subgroup of G, the extension is a split extension. ■

3.4.2 Semdirect (Internal) Products

Suppose N is normal, then every subgroup H of G acts on N by conjugation, i.e., $\gamma : H \to \mathrm{Aut}_{\mathrm{GRP}}(N), h \mapsto \gamma_h$, where $\gamma_h(n) = hnh^{-1}$. The subgroup H and N commutes precisely when γ is trivial.

If the conditions in the above lemma are met, then the extension G of H by N may be reconstructed from the conjugation action: $n_1 h_1 n_2 h_2 = (n_1(h_1 n_2 h_1^{-1}))(h_1 h_2)$.

In the general discussion, suppose N, H are two groups, and θ is an arbitrary homomorphism $\theta : H \to \mathrm{Aut}_{\mathrm{GRP}}(N)$, $h \mapsto \theta_h$. Define the operation $\cdot_\theta$ on the set $N \times H$ as follows:

$$(n_1, h_1) \cdot_\theta (n_2, h_2) := (n_1, \theta(h_1, n_2), h_1 h_2).$$

Note *The resulting structure $(N \times H, \cdot_\theta)$ is a group, with identity element (e_N, e_H).*

Definition 3.15 (Semidirect product)

The group $(N \times H, \cdot_\theta)$ is a ***semidirect product*** *of N and H and is denoted by $N \rtimes_\theta H$.* ♣

Proposition 3.11

Let N, H be groups, and let $\theta : H \to \mathrm{Aut}_{\textsc{Grp}}(N)$ be a homomorphism; let $G = N \rtimes_\theta H$ be the corresponding semidirect product. Then

(i) *G contains isomorphic copies of N and H;*

(ii) *the natural projection $G \to H$ is a surjective homomorphism, with kernel N; thus N is normal in G, and the sequence $1 \longrightarrow N \longrightarrow N \rtimes_\theta H \longrightarrow H \longrightarrow 1$ is (split) exact.*

(iii) *$N \cap H = \{e_G\}$;*

(iv) *$G = NH$;*

(v) *the homomorphism θ is realized by conjugation in G; that is, for $h \in H$ and $n \in N$ we have $\theta_h(n) = hnh^{-1}$ in G.* ♠

Proof (i) Consider the inclusion function $i_N : N \to N \rtimes H$ defined by $i_N(n) = (n, e_H)$. i_N is obviously an injective homomorphism, so we may identifies N with $N \rtimes \{e\} \leq N \rtimes H$. The analogous statement holds for H.

(ii)-(iv) By identifying $N, H \leq G$, it is clear that $N \cap H = \{e_G\}$, and $G = NH$ since $(n, e_H) \cdot_\theta (e_N, h) = (n, h)$. Define the projection $\pi_H : G \to H$ by $(n, h) \mapsto h$. It is naturally a surjective homomorphism, and the kernel is given by $\ker \pi_H = N$. Therefore, $1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1$ is split exact.

(v) Note that $hnh^{-1} \leftrightarrow (e_N, h) \cdot_\theta (n, e_H) \cdot_\theta (e_N, h^{-1}) = (\theta_h(n)\theta_h(e_N), hh^{-1}) = (\theta_h(n), e_H) \leftrightarrow \theta_h(n)$, so θ is realized by conjugation. ■

Proposition 3.12

Let N, H be subgroups of a group G, with N normal in G. Assume that $N \cap H = \{e\}$, and $G = NH$. Let $\gamma : H \to \mathrm{Aut}_{\textsc{Grp}}(N)$ be defined by conjugation: for $h \in H$, $n \in N$, $\gamma_h(n) = hnh^{-1}$. Then $G \cong N \rtimes_\gamma H$. ♠

Proof Consider the function $\varphi : N \rtimes_\theta H \to G$ defined by $\varphi(n, h) = nh$. φ is clearly a bijection by definition, and it is a homomorphism since

$$\varphi((n_1, h_1)(n_2, h_2)) = \varphi(n_1\gamma_{h_1}(n_2), h_1h_2) = n_1(h_1n_2h_1^{-1})h_1h_2 = n_1h_1n_2h_2 = \varphi(n_1, h_1)\varphi(n_2, h_2).$$

Therefore, $N \rtimes_\gamma H \cong_\varphi G$. ■

Remark Proposition 3.11 implies that every (external) semi-direct product gives rise to a short exact sequence that splits, and Proposition 3.12 implies that a split extension can be realize through a (internal) semi-direct product.

3.5 Finite Abelian Groups

Note that we will denote the operation by "+", the identity by 0, and the direct product (direct sums) by $\oplus$.

Proposition 3.13

Let G be an abelian group, and let H, K be abelian subgroups such that $|H|$, $|K|$ are relatively prime. Then $H + K \cong H \oplus K$.

Proof By Lagrange's theorem, $H \cap K = \{0\}$. The statement follows immediately from Proposition 3.10 since subgroups are normal in an abelian group. ■

Corollary 3.6

Every finite abelian group is the direct sum of its nontrivial Sylow subgroups.

Proof Suppose $|G| = p_1^{r_1} \cdots p_n^{r_n}$. The Sylow theorems states that for each p_i, there is an unique p_i-Sylow subgroup H_i, i.e., $|H_i| = p_i^{r_i}$. The above proposition implies that $\bigoplus_{i=1}^n H_i \cong \sum_{i=1}^n H_i$. Since $|\bigoplus_{i=1}^n H_i| = |G|$ and $\bigoplus_{i=1}^n H_i \cong \sum_{i=1}^n H_i \subset G$, hence $G = H_1 \oplus \cdots \oplus H_n$. ■

Proposition 3.14

Let p be a prime integer and $r \geq 1$. Let G be a noncyclic abelian group of order p^{r+1}, and let $g \in G$ be an element of order p^r. Then there exists an element $h \in G$, $h \notin \langle g \rangle$ such that $|h| = p$.

Proof Denote by $N = \langle g \rangle$. By Cauchy's theorem, there exists $hN = G/N$ such that $|hN| = p$, it is obvious that $h \notin N$ and $ph \in N$ so that $ph = m'g$. Notice that $|ph|$ divides pr and does not equal to pr because otherwise $G = \langle h \rangle$ is cyclic, thus we can write $ph = pmg$ for some m. Consider $h' = h - mg$, it is obvious that $h' \notin N$. Since $h - mg$ divides p since $p(h - mg) = 0$ and $|h - mg| \neq 1$, it follows that $|h'| = p$. ■

Proposition 3.15

Let G be an abelian p-group, and let $g \in G$ be an element of maximal order. Then the exact sequence $1 \longrightarrow \langle g \rangle \longrightarrow G \longrightarrow G/\langle g \rangle \longrightarrow 1$ splits.

Remark In other words, there is a subgroup L of G such that $L \cong G/\langle g \rangle$ via canonical projection, that is, such that $\langle g \rangle \cap L = \{0\}$ and $\langle g \rangle + L = G$.

Proof We proceed by strong induction on $|G|$. The case $|G| = p^0 = 1$ is trivial. For nontrivial group G, assume the statement holds for every p-group smaller than G. Suppose $g \in G$ such that $|g| = p^r$ is the maximal order, consider $K = \langle g \rangle \trianglelefteq G$. The statement is obvious if $G = K$, so we therefore assume $G \neq K$. There is element in G/K of order p by Cauchy's theorem, it then generates G'/K for some $G' \leq G$ where $|G'| = p^{r+1}$. The previous proposition (3.14) implies that there exists $h \in G' \setminus K$ such that $|h| = p$. Let $H = \langle h \rangle$, then $G' = H \oplus K$ since $|hK| = p$.

Apply inductive hypothesis using the fact that $g + H$ has the maximal order in G/H, there is a split extension $0 \longrightarrow G'/H \longrightarrow G/H \longrightarrow L' \longrightarrow 0$ for some $L' \leq G/H$, and $L' = L/H$ for some $L \leq G$ by the structure of quotient group. In other words, $G'/H + L/H = G/H$ and $G'/H \cap L/H = \{H\}$. It is clear that $G'/H \cong K$. We want to prove $G = K \oplus L$ by verifying the following properties:

- Suppose $a \in G$, i.e., $a + H \in G/H$, then there exist $mg + H \in G'/H$ and $l + H \in L/H$ such that $a + H = mg + l + H$. Then $a \in mg + (l + H) \in K + L$. It follows that $G = K + L$.
- Suppose $a \in K \cap L$, then $a + H \in G'/H \cap L/H = \{H\}$, followed by $a \in H$. Then $a \in H \cap K$, forcing $a = 0$. That is, $K \cap L = \{0\}$.

Hence $G = K \oplus L$ as desired. ■

Corollary 3.7

Let G be a finite abelian group, Then G is a direct sum of cyclic groups, which may be assumed to be cyclic p-groups. ♡

Proof It suffices to prove every p-subgroup is a direct product of cyclic groups, then the desired statement follows immediately by Corollary 3.6. We proceed by induction on $|P|$. The case is trivial if P is trivial. Suppose P is a nontrivial p-group, let g be its element with maximal order. Proposition 3.15 implies that $P = \langle g \rangle + P'$ for some proper subgroup P'. P' is a direct sum of cyclic subgroups by inductive hypothesis, concluding the proof. ■

Theorem 3.5

Let G be a finite nontrivial abelian group. Then there exists prime integers $p_1, \cdots, p_r$ and positive integers $n_{i,j}$ such that $|G| = \prod_{i,j} p_i^{n_{i,j}}$ and

$$G \cong \bigoplus_{i,j} \mathbb{Z}/p^{n_{i,j}}\mathbb{Z}.$$

Equivalently, there exist positive integers $1 < d_1 \mid \cdots \mid d_s$ such that $|G| = d_1 \cdots d_s$ and

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \mathbb{Z}/d_s\mathbb{Z}.$$

Furthermore, these decompositions are uniquely determined by G. ♡

Remark The first form follows immediately from the above corollary. For the second form, the integers d_i are called ***invariant factors***. To obtain the invariant factors, collect the element divisors in a table, listing prime powers to increasing primes in the horizontal direction and decreasing exponents in the vertical direction, then the invariant factors are obtained as products of the factors in each row:

$d_r =$	$p_1^{n_{1,1}}$	$p_2^{n_{2,1}}$	$\cdots$
$d_{r-1} =$	$p_1^{n_{1,1}}$	$p_2^{n_{2,1}}$	$\cdots$
$d_{r-2} =$	$p_1^{n_{1,1}}$	$p_2^{n_{2,1}}$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\ddots$

Example 3.3 All abelian groups of order $360 = 2^3 \times 3^2 \times 5$ are

$$\begin{array}{lll} \mathbb{Z}/360\mathbb{Z}, & \mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/180\mathbb{Z}, & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z}, \\ \mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/6\mathbb{Z} \otimes \mathbb{Z}/30\mathbb{Z}, & \mathbb{Z}/3\mathbb{Z} \otimes \mathbb{Z}/120\mathbb{Z}, & \mathbb{Z}/6\mathbb{Z} \otimes \mathbb{Z}/60\mathbb{Z}, \end{array}$$

up to isomorphisms.

Part II

Algebra II

Chapter 4 Ring Theory and Module Theory

Introduction

- ❑ *Ring, Polynomial Ring*
- ❑ *Ideals and Quotient Rings*
- ❑ *Complexes*
- ❑ *Category* Ring
- ❑ *Module Over a Ring*

4.1 Ring

4.1.1 Rings and Special Classes of Rings

Definition 4.1 (Ring)

A ***ring*** *is a set R equipped with two operations $+$ and $\cdot$ satisfying*

(1) $(R, +)$ *is an abelian group,*

(2) $(R, \cdot)$ *is a monoid (i.e., associativity holds and identity exists), and*

(3) Multiplication is distributive with respect to addition, i.e., $a \cdot (b + c) = a \cdot b + a \cdot c$ *and* $(a + b) \cdot c = a \cdot c + b \cdot c$ *for all* $a, b, c \in R$*.*

♣

Proposition 4.1

(a) Absorption: For all $r \in R$, $0 \cdot r = 0 = r \cdot 0$.

(b) For all $r \in R$, $r + (-1)r = 0$*; that is,* $(-1)r = -r$.

♠

Proof (a) For all $r \in R$, $0 \cdot r = (0 + 0) \cdot r = 0 \cdot r + 0 \cdot r$, then $0 \cdot r = 0$ by cancellation. The equality $r \cdot 0 = 0$ holds wlog.

(b) For all $r \in R$, $r + (-1)r = 1r + (-1)r = (1 + (-1))r = 0r = 0$. ■

Example 4.1 Examples of rings are:

- The *trivial ring* (*zero ring*) is the ring consists of one element $\{*\}$ (often denoted by 0). Note that in the trivial ring, $0 = 1$.
- The integers $\mathbb{Z}$.
- The rational numbers $\mathbb{Q}$, the real number $\mathbb{R}$, the complex number $\mathbb{C}$.
- $n \times n$ matrices $M_n(R) := R^{2\times 2}$ where R is a ring.
- The integers $\mathbb{Z}/n\mathbb{Z}$ modulo n.

Definition 4.2 (Commutative Ring)

*A ring R is **commutative** if multiplication is commutative, i.e., $rs = sr$ for all $r, s \in R$.* ♣

Example 4.2 Examples of commutative ring is $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ (note that $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields, i.e., multiplication is commutative and inverse exists). An example of non-commutative ring is $M_2(\mathbb{R})$, the ring of $n \times n$ matrices with real entries.

Definition 4.3 (Integral Domain)

*A nonzero commutative ring R is an **integral domain** if $rs = 0$ implies $r = 0$ or $s = 0$ for all $r, s \in R$.* ♣

4.1.2 Polynomial Rings

Definition 4.4 (Polynomial, Degree)

*A **polynomial** $f(x)$ in the **indeterminate** x over a ring R is a finite linear combination of nonnegative 'powers' of x with coefficients in R: $f(x) = a_0 + a_1x + a_2x^2 + \cdots$, where every coefficient $a_i \in R$, and $a_i = 0$ whenever $i \geq N$ for some N.*

*The **degree** of a nonzero polynomial, denoted $\deg f(x)$, is the largest integer d for which $a_d \neq 0$; the degree of polynomial 0 is defined to be $-\infty$.* ♣

Note *Two polynomials are said to equal if all the coefficients are equal. We define the addition and multiplication between $f(x) = \sum_{i\geq 0} a_i x^i$ and $g(x) = \sum_{i\geq 0} b_i x^i$ by*

$$f(x) + g(x) := \sum_{i\geq 0}(a_i + b_i)x^i \qquad \text{and} \qquad f(x)g(x) := \sum_{i\geq 0}\left(\sum_{j+k=i} a_j b_k\right)x^i.$$

Definition 4.5 (Polynomial Ring)

*The set of polynomial in x over R, endowed with addition and multiplication stated above, is the **polynomial ring** over R, denoted $R[x]$.* ♣

Remark Rings of power series $\{\sum_{i=0}^{\infty} a_i x^i\}$ over a ring R is denoted $R[[x]]$. Polynomial rings in more indeterminates may be obtained by iterating the above construction: $R[x_1, \cdots, x_n]$= $R[x_1][x_2]\cdots[x_n]$.

4.2 The Category of RING

4.2.1 The Category of RING

Definition 4.6 (Ring homomorphism, The category of RING)

If R, S are rings, a function $\varphi : R \to S$ is a ***ring homomorphism*** *if*

(1) φ preserves addition: $\varphi(a+b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$,

(2) φ preserves multiplication: $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$, and

(3) φ preserves multiplicative identity: $\varphi(1_R) = 1_S$.

The ***RING category*** *is the category whose objects are rings and whose morphisms are ring homomorphisms.*

Remark Equivalent, φ is a ring homomorphism if φ is a group homomorphism with respect to addition, and φ is a monoid homomorphism with respect to multiplication.

Ring homomorphisms preserve units and inverse.

Remark The condition $\varphi(0_R) = 0_S$ can be omitted because $\varphi(0_R) = \varphi(0_R) + \varphi(0_R)$ by definition yields the desired statement by cancellation law.

Note *The trivial ring $\{0\}$ is final in RING since the only ring homomorphism $R \to \{0\}$ is the trivial homomorphism. However, it is not initial because there exists no homomorphism from $\{0\}$ to nonzero ring R (since $1 \mapsto 1_R$ contradicts to $1 = 0 \mapsto 0_R$).*

The ring of integers $\mathbb{Z}$ is initial in RING. For every ring R, the only homomorphism is defined to be $\varphi(n) = n \cdot 1_R = 1_R + \cdots + 1_R$.

4.2.2 Universal property of polynomial rings

Proposition 4.2 (Universal property of polynomial ring)

Suppose R and S are rings, let $\alpha : R \to S$ be a ring homomorphism, and let $s \in S$ be an element such that $\alpha(r) \cdot s = s \cdot \alpha(r)$ for all $r \in R$. Then there exists a unique ring homomorphism $\tilde{\alpha} : R[x] \to S$ such that $\tilde{\alpha}(x) = s$ and $\tilde{\alpha}$ extends s, i.e., $\tilde{\alpha} \circ j = \alpha$.

$$\begin{tikzcd}
R[x] \arrow[r, dashed, "\tilde{\alpha}"] & S \\
R \arrow[u, "j"] \arrow[ru, "\alpha"']
\end{tikzcd}$$

Proof The commutativity of the diagram implies $\tilde{\alpha}(r) = \alpha(r)$ for all $r \in R$. Since $\tilde{\alpha} = s$, the homomorphism condition forces $\tilde{\alpha}(\sum_{n\geq 0} a_n x^n) = \sum_{i\geq 0} \alpha(a_n) s^n$, which proves the uniqueness if such homomorphism exists. It suffices to verify $\tilde{\alpha}$ is a homomorphism. Suppose $f = \sum_{n\geq 0} a_n x^n$ and $g = \sum_{n\geq 0} b_n x^n$, then

$$\tilde{\alpha}(f+g)=\sum_{n\geq 0}\alpha(a_n+b_n)s^n=\sum_{n\geq 0}\alpha(a_n)s^n+\sum_{n\geq 0}\alpha(b_n)s^n=\tilde{\alpha}(f)+\tilde{\alpha}(g)$$

$$\tilde{\alpha}(fg)=\sum_{n\geq 0}\sum_{i+j=n}\alpha(a_ib_j)s^{i+j}=\left(\sum_{i\geq 0}\alpha(a_i)s^i\right)\left(\sum_{j\geq 0}\alpha(b_j)s^j\right)=\tilde{\alpha}(f)\tilde{\alpha}(g),$$

so $\tilde{\alpha}$ preserves addition and multiplicative. In addition, $\tilde{\alpha}$ preserves multiplicative identity since $\tilde{\alpha}(1_R)=\alpha(1_R)=1_S$. Hence $\tilde{\alpha}$ is a homomorphism. ■

Proposition 4.3

Let $A=\{a_1,\cdots,a_n\}$, $i:A\to\mathbb{Z}[x_1,\cdots,x_n]$ be a set-function defined by $i(a_i)=x_i$. For every commutative ring R and set-function $j:A\to R$, there exists an unique homomorphism $\varphi:R_1\to R_2$ such that the diagram commutes:

$$\begin{tikzcd}
\mathbb{Z}[x_1,\cdots,x_n] \arrow[r, dashed, "\varphi"] & R \\
A \arrow[u, "i"] \arrow[ur, "j"'] &
\end{tikzcd}$$

♠

Remark Let $\mathscr{R}_A$ be a category whose objects are pairs (j,R), where R is a commutative ring, and morphisms $(j_1,R_1)\to(j_2,R_2)$ are ring homomorphisms such that $\varphi\circ j_1=j_2$:

$$\begin{tikzcd}
R_1 \arrow[r, "\varphi"] & R_2 \\
A \arrow[u, "j_1"] \arrow[ur, "j_2"'] &
\end{tikzcd}$$

Then $(i,\mathbb{Z}[x_1,\cdots,x_n])$ is initial in $\mathscr{R}_A$.

Proof Suppose (j,R) is an object, and assume $\varphi:\mathbb{Z}[x_1,\cdots,x_n]\to R$ is a homomorphism such that the diagram commutes. The commutativity implies that $\varphi(x_i)=j(a_i)$, and the homomorphism condition forces that $\varphi(\sum m_{i_1,\cdots,i_n}x_1^{i_1}\cdots x_n^{i_n})=\sum\imath(m_{i_1,\cdots,i_n})j(a_1)^{i_1}\cdots j(a_n)^{i_n}$, where $\imath:\mathbb{Z}\to R$ is the unique homomorphism. It is not hard to verify φ is a homomorphism, and it is unique as shown above, hence $(i,\mathbb{Z}[x_1,\cdots,x_n])$ is initial. ■

4.2.3 Monomorphisms and epimorphisms

Proposition 4.4

Suppose $\varphi:R\to S$ is a ring homomorphism, the following are equivalent

(a) φ is a monomorphism;

(b) $\ker\varphi=\{0\}$;

(c) $\varphi:G\to G'$ is injective (as a set-function).

♠

Proof $(a)\Rightarrow(b)$: Suppose φ is a monomorphism, and $r\in\ker\varphi$. Consider homomorphism $e_r,e_0:\mathbb{Z}[x]\to R$ for which $e_r(x)=r$ and $e_0(x)=0$.

$$\begin{tikzcd} \mathbb{Z}[x] \arrow[r, shift left, "e_r"] \arrow[r, shift right, "e_0"'] & R \arrow[r, "\varphi"] & S \end{tikzcd}$$

Notice that $\varphi \circ e_r = \varphi \circ e_0$ because they agree on $\mathbb{Z}$ and x, then $e_r = e_0$, namely $r = e_r(x) = 0$. $(b) \Rightarrow (c)$ and $(c) \Rightarrow (a)$ are analogous to Proposition 2.15. ■

Remark Warning: It is not necessary that every epimorphism is surjective (unlike in Grp), and in addition, φ is not necessarily an isomorphism even it is both a mono- and epi-morphism in Ring.

For instance, consider the inclusion map $\imath : \mathbb{Z} \hookrightarrow \mathbb{Q}$. It is both a monomorphism and an epimorphism in Ring, but it is neither surjective nor an isomorphism.

4.3 Ideals and Quotient Rings

4.3.1 Ideals and Quotient Rings

Definition 4.7 (Ideal)

Let R be a ring. A subgroup I of $(R, +)$ is a ***left-ideal*** *of R if $rI \subset I$ for all $r \in R$ (left-absorption), it is a* ***right-ideal*** *if $Ir \subset I$ for all $r \in R$ (right-absorption). An (two-sided)* ***ideal*** *is a subgroup I which is both a left- and right-ideal.* ♣

Remark In general, an ideal $I \subset R$ is not a subring of ring R: I is closed under multiplication, but it usually does not contain 1_R, otherwise $I = R$.

Proposition 4.5

Let $\varphi : R \to S$ be any ring homomorphism. Then $\ker \varphi$ is an ideal of R. ♠

Proof The kernel is a subgroup of $(R, +)$. In addition, the left absorption holds because for all $r \in R$, $a \in \ker \varphi$, we have $\varphi(ra) = \varphi(r) \cdot 0 = 0$; and the right absorption holds without loss of generality. Hence $\ker \varphi$ is an ideal. ■

Proposition 4.6 (Ideal generated by an element)

Suppose R is a ring and $a \in R$. The set $Ra = \{ra \mid r \in R\}$ is a left ideal of R, and similarly $aR = \{ar \mid r \in R\}$ is a right ideal. If R is commutative, then $(a) = Ra = aR$ is the ***ideal generated by*** *a.* ♠

Proposition 4.7

Suppose $\{I_\alpha\}$ is a family of ideals in R.

(a) The sum of the ideals $\sum_{\alpha\in A} I_\alpha := \left\{\sum_{\alpha\in A} r_\alpha \,\middle|\, r_\alpha \in I_\alpha, \text{and } r_\alpha = 0 \text{ for all but finite } \alpha\right\}$ is the smallest ideal containing all I_α.

(b) The intersection of the ideals $\bigcap_{\alpha\in A} I_\alpha$ is the largest ideal contained in all I_α.

(c) The product of two ideals $IJ := \{\sum_{\alpha\in A} r_\alpha s_\alpha \mid r_\alpha \in I, s_\alpha \in J, \text{ and } r_\alpha = s_\alpha = 0 \text{ for all but finite } \alpha\}$ is an ideal of R. ♠

Definition 4.8 (Quotient ring)

Suppose I be an ideal of the ring $(R, +, \cdot)$. Let the quotient ring R/I be consisting of cosets $r + I$, endowed with addition $(r + I)(s + I) = rs + I$ and multiplication $(r + I)(s + I) = rs + I$. The ring R/I is called the ***quotient ring of*** *R* ***modulo*** *I.* ♣

Proof The multiplication in the quotient ring is well-defined: suppose $r + I = r' + I$ and $s + I = s' + I$, then $r' - r, s' - s \in I$, it follows that $r's' - rs = r'(s' - s) - s(r' - r) \in I$ by absorption property, i.e., $rs + I = r's' + I$.

Then it is not hard to verify that R/I is a ring by definition. ■

Example 4.3 It is essential that I is an ideal. Consider $\mathbb{Z}$ as a subgroup of $\mathbb{Q}$, let addition and multiplication be defined as above, then $0+\mathbb{Z}=1+\mathbb{Z}$, whereas $(0+\mathbb{Z})(1/2+\mathbb{Z})=0+\mathbb{Z}\neq 1/2+\mathbb{Z}=(1+\mathbb{Z})(1/2+\mathbb{Z})$.

Remark Similar to quotient group, suppose R is a ring and $I \trianglelefteq R$, then $J/I \trianglelefteq R/I$ is an ideal of the quotient ring if and only if $J \trianglelefteq R$.

Note *The canonical projection $\pi : R \to R/I$ defined by $r \mapsto r+I$ is a ring homomorphism, and its kernel is I.*

Remark In addition, note that every ideal I can be realized as the kernel of the canonical projection map $R \to R/I$. Hence there is an equivalence: ideal $\Longleftrightarrow$ kernel of ring homomorphism.

Example 4.4 For every $n \in \mathbb{Z}_{\geq 0}$, it is not hard to verify that $n\mathbb{Z}$ is an ideal of the integers $\mathbb{Z}$, then it follows direct that $\mathbb{Z}/3\mathbb{Z}$ is a quotient ring of $\mathbb{Z}$ modulo $n\mathbb{Z}$.

Proposition 4.8 (Universal property of quotient ring)

Let I be an ideal of a ring R. Then for every ring homomorphism $\varphi : R \to S$ such that $I \subset \ker\varphi$ there exists a unique ring homomorphism $\tilde{\varphi} : R/I \to S$ such that the diagram commutes

$$\begin{tikzcd}
R/I \arrow[rr, dashed, "\tilde{\varphi}"] & & S \\
& R \arrow[ul, "\pi"] \arrow[ur, "\varphi"'] &
\end{tikzcd}$$

Proof Proposition 2.21 forces $\tilde{\varphi}(r+I) := \varphi(r)$ in order to preserve addition. It suffices to prove $\tilde{\varphi}$ preserves multiplication and multiplicative identity, which are trivial according to the definition of multiplication in the quotient ring.

Analogous to the group isomorphism theorem, the following theorem holds:

Theorem 4.1 (Ring isomorphism theorems)

(a) First isomorphism theorem: Suppose $\varphi : R \to S$ is a surjective ring homomorphism, then $S \simeq R/\ker\varphi$.

(b) Second isomorphism theorem: Suppose I, J be ideals of R, then $I+J$ and $I \cap J$ are ideals, and $(I+J)/I = J/(I\cap J)$.

(c) Third isomorphism theorem: Let I, J be ideals of a ring R for which $I \subset J$. Then J/I is an ideal of R/I, and $(R/I)/(J/I) \simeq R/J$.

4.3.2 PIDs, Prime Ideal, Maximal Ideal

Definition 4.9 (Principle Ideal Domain (PID))

*An integral domain is a **PID (Principal Ideal Domain)** if every ideal of R is **principal**, i.e., every ideal is generated by one element.*

Definition 4.10 (Prime Ideal, Maximal Ideal)

Let $I \neq R$ be an ideal of a commutative ring R,

*(a) I is a **prime ideal** if R/I is an integral domain, i.e., $ab = 0 \implies (a = 0$ or $b = 0)$ for all $a, b \in R$.*

*(b) I is a **maximal ideal** if R/I is a field.*

Proposition 4.9 (Equivalent definition of prime and maximal ideals)

(a) I is prime if and only if for all $a, b \in I$: $ab \in I \implies (a \in I)$ or $(b \in I)$.

(b) I is maximal if and only if for all $J \trianglelefteq R$ such that $I \subsetneq J$: $J = R$.

(c) Every maximal ideal is prime.

Proposition 4.10 (Prime ideal is maximal in PID)

Let R be a PID, then a non-zero ideal $I \trianglelefteq R$ is maximal if and only if I is prime.

Proof Suppose I is a prime ideal, then $I = (r)$ is generated by a prime element r. Assume there is an ideal $I' = (r')$ s.t. $I \subsetneq I'$, then $r = cr'$ for some $c \in R$. Note that r is irreducible because it is prime, and c is not a unit, since otherwise $r \sim r'$ thus $I = (r) = (r') = I'$. Therefore, r' is a unit, so $I' = (r') = R$. Hence I is a maximal ideal. ■

Definition 4.11 (Characteristic)

*For a ring R, let $f : \mathbb{Z} \to R$ be the unique ring homomorphism defined by $a \mapsto a \cdot 1_R$, then $\ker f = n\mathbb{Z}$ for some $n \in \mathbb{Z}_{\geq 0}$. The **characteristic** of a ring R is defined to be n.*

Remark Equivalently, the characteristic of R is $n > 0$ if n is the least positive integer such that $n \cdot 1_R = 0$, and R is characteristic zero if the order of 1_R is ∞.

4.4 Modules Over a Ring

4.4.1 Modules

The left-module can be viewed as an abelian group M, endowed with a left-action of a ring R, i.e., a homomorphism of rings $\sigma : R \to \text{End}_{\text{Ab}}(M)$

Definition 4.12 (Module)

*A **left-R-module** structure on an abelian group M consists of a map $R \times M \to M$, $(r, m) \mapsto rm$, such that*

(1) $r(m + n) = rm + rn$;

(2) $(r + s)m = rm + sm$;

(3) $(rs)m = r(sm)$; and

(4) $1m = m$.

A right-R-module is defined analogously. ♣

Remark Condition (2) and (3) corresponds to the definition of action σ (ring homomorphism), and condition (1) and (4) corresponds to the group homomorphism σ_r.

Example 4.5 Every homomorphism of rings $\alpha : R \to S$ give arises to a R-module on S by defining $\rho : R \times S \to S$ by $\rho(r, s) := \alpha(r)s$.

Proposition 4.11

Every abelian group is a $\mathbb{Z}$-module, in exactly one way. ♠

Proof For every $\text{End}_{\text{Ab}}(G)$ corresponding to the abelian group G, there exists an unique homomorphism $\mathbb{Z} \to \text{End}_{\text{Ab}}(G)$ since $\mathbb{Z}$ is initial in Ring. Hence there exists an unique $\mathbb{Z}$-module structure on G. ■

Definition 4.13 (R-Mod)

*A **homomorphism** of R-modules is a homomorphism of (abelian) groups which is compatible with the module structure. That is $\varphi : M \to N$ is a homomorphism of R-modules if $\varphi(x + y) = \varphi(x) + \varphi(y)$ and $\varphi(rx) = r\varphi(x)$ for all $r \in R$, $x, y \in M$.*

***R-Mod** is the category whose objects are R-modules and morphisms are homomorphisms between R-modules.* ♣

Remark Equivalently, $\varphi : M \to N$ is a (R-module) homomorphism if and only if $\varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2)$ and $\varphi(rm) = r\varphi(m)$.

Remark Let $\varphi : L \to M$ be an R-module homomorphism, then $\ker\varphi$ and $\operatorname{im}\varphi$ are R-submodule of L and M, resp.

Example 4.6 If $R = k$ is a field, R-modules are called k-vector spaces (the corresponding category is k-Vect), and the morphisms are called linear maps.

Example 4.7 The trivial group 0 is both initial and final in R-Mod.

Note *The canonical decomposition and isomorphism theorem hold.*

4.4.2 Submodules and Quotients, Kernel and Cokernel

Definition 4.14 (Submodule)

*A subset $N \subset M$ is a R-**submodule** of M if (1) $N \leq M$ is an (additive) subgroup, and (2) N is closed under the action of R, i.e., $RN \subset N$.*

Proposition 4.12

Let N be a submodule of an R-module M, then the set $M/N := \{m + N \,|\, m \in M\}$ of cosets, endowed with addition $(m + N) + (n + N) = (m + n) + N$ and multiplication $(m + N)(n + N) = mn + N$, is an R-module.

Remark Suppose N is a R-submodule of M, the canonical projection $\pi : M \to M/N$, $x \mapsto x + N$, is an R-module homomorphism, with $\ker \pi = N$. Then every R-submodule of a given module arises as the kernel of a homomorphism.

In the category R-Mod, suppose $\varphi : M \to N$ is a homomorphism of R-modules, then $\ker \varphi$ is final with respect to the property of factoring R-module homomorphisms $\alpha : P \to M$ such that $\varphi \circ \alpha = 0$:

$$\begin{tikzcd}
P \arrow[r, "\alpha"'] \arrow[rr, bend left, "0"] \arrow[dr, dashed, "\tilde{\alpha}"'] & M \arrow[r, "\varphi"'] & N \\
& \ker \varphi \arrow[u, hook, "\imath"'] &
\end{tikzcd}$$

while $\operatorname{coker} \varphi := N/\operatorname{im} \varphi$ is initial with respect to the property of factoring R-module homomorphisms $\beta : N \to P$ such that $\beta \circ \varphi = 0$:

$$\begin{tikzcd}
N \arrow[r, "\varphi"'] \arrow[rr, bend left, "0"] & M \arrow[r, "\beta"'] \arrow[d, two heads, "\pi"'] & P \\
& \operatorname{coker} \varphi \arrow[ur, dashed, "\tilde{\beta}"'] &
\end{tikzcd}$$

Proposition 4.13

The following hold in R-Mod:

(a) *kernels and cokernels exists;*

(b) φ *is monomorphism* $\iff$ $\ker\varphi$ *is trivial* $\iff$ φ *is injective as a set-function;*

(c) φ *is epimorphism* $\iff$ *coker* φ *is trivial* $\iff$ φ *is surjective as a set-function;* ♠

4.5 Complexes and Homology

Definition 4.15 (Complexes, Exactness)

*A **chain complex** of R-modules is a sequence of R-modules and R-module homomorphisms*

$$\cdots \xrightarrow{d_{i+2}} M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \xrightarrow{d_{i-1}} \cdots$$

such that $d_i \circ d_{i+1} = 0$ for all i (i.e., im $d_{i+1} \subset \ker d_i$). The notation $(M_\bullet, d_\bullet)$ (or $M_\bullet$) is used to denote a complex.

*A complex is **exact at** M_i if im $d_{i+1} = \ker d_i$, and a complex is **exact** if it is exact at all its modules.*

Example 4.8 A complex $\cdots \longrightarrow 0 \longrightarrow L \xrightarrow{\alpha} M \longrightarrow \cdots$ is exact at L if and only if α is a monomorphism (injective).

A complex $\cdots \longrightarrow L \xrightarrow{\beta} N \longrightarrow 0 \longrightarrow \cdots$ is exact at N if and only if β is a epimorphism (surjective).

Definition 4.16 (Short Exact Sequence)

*A **short exact sequence** (SES) is an exact complex of the form $0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$; that is, α being injective, β being surjective, and im $\alpha = \ker \beta$.*

Example 4.9 A short exact sequence $0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow \cdots$ give rise to an isomorphism $N \cong M/\ker\beta \cong M/\text{im}\,\alpha = \text{coker}\,\alpha$.

Definition 4.17 (Split (Short) Exact Sequence)

*A short exact sequence **splits** if it is isomorphic to a short exact sequence induced by direct sum:*

$$\begin{tikzcd}
0 \arrow[r] & M_1 \arrow[r] \arrow[d, "\sim"] & N \arrow[r] \arrow[d, "\sim"] & M_2 \arrow[r] \arrow[d, "\sim"] & 0 \\
0 \arrow[r] & M_1' \arrow[r] & M_1' \oplus M_2' \arrow[r] & M_2' \arrow[r] & 0
\end{tikzcd}$$

Remark The short exact sequence splits if M_2 may be identified as the submodule of N for which $M_1 \cap M_2 = 0$.

Definition 4.18 (Homology)

*The i-th **homology** of a complex*

$$M_\bullet : \cdots \xrightarrow{d_{i+2}} M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \xrightarrow{d_{i-1}} \cdots$$

if R-modules is the R-module $H_i(M_\bullet) := \ker d_i/\text{im}\, d_{i+1}$.

Remark Homology measures the "difference of a complex from being exact". $H_i(M_\bullet) = 0$ if and only if $M_\bullet$ is exact at M_i.

Example 4.10 Suppose $\varphi : M_1 \to M_2$ is a R-module homomorphism, then it give rises to the complex $M_\bullet : 0 \longrightarrow M_2 \xrightarrow{\varphi} M_1 \longrightarrow 0$ of R-modules, and $H_2(M_\bullet) = \ker\varphi$ and $H_1(M_\bullet) = \operatorname{coker}\varphi$.

Proposition 4.14 (Snake Lemma)

Suppose two short exact sequences are linked by homomorphisms

$$\begin{tikzcd}
0 \arrow[r] & L_1 \arrow[r, "\alpha_1"] \arrow[d, "\lambda"] & M_1 \arrow[r, "\beta_1"] \arrow[d, "\mu"] & N_1 \arrow[r] \arrow[d, "\nu"] & 0 \\
0 \arrow[r] & L_0 \arrow[r, "\alpha_0"'] & M_0 \arrow[r, "\beta_0"'] & N_0 \arrow[r] & 0
\end{tikzcd}$$

then there is an exact sequence

$$0 \longrightarrow \ker\lambda \longrightarrow \ker\mu \longrightarrow \ker\nu \xrightarrow{\delta} coker\ \lambda \longrightarrow coker\ \mu \longrightarrow coker\ \nu.$$

♠

We first construct the morphism $\delta : \ker\nu \to \operatorname{coker}\lambda$.

- Definition of δ: Suppose $a \in \ker\nu$, there exists $b \in M_1$ such that $\beta_1(b) = a$ since β_1 is surjective. Since $(\beta_0 \circ \mu)(b) = (\nu \circ \beta_1)(b) = \nu(a) = 0$, we have $b \in \ker\beta_0 = \operatorname{im}\alpha_0$, namely there exists $c \in L_0$ such that $\alpha_0(c) = \mu(b)$. Hence every $a \in \ker\nu$ give rises to an element $c \in L_0$, and we may define $\delta(a) = c + \operatorname{im}\lambda$.

$$\begin{tikzcd}
 & {} \arrow[r, dotted] \arrow[d, hook, dotted] & \ker\nu \arrow[d, hook] \\
{} \arrow[r, dotted, "\alpha_1"] \arrow[d, dotted, "\lambda"'] & M_1 \arrow[r, "\beta_1"] \arrow[d, "\mu"] & N_1 \arrow[d, dotted, "\nu"] \\
L_0 \arrow[r, "\alpha_0"] \arrow[d, two heads, "\pi"'] & M_0 \arrow[r, dotted, "\beta_0"] \arrow[d, dotted] & {} \\
\operatorname{coker}\lambda \arrow[r, dotted] & {} &
\end{tikzcd}$$

- Well-definedness: Suppose a gives rise to $b' \in M_1$. Since $b' - b \in \ker\beta_1 = \operatorname{im}\alpha_1$, there exists $g \in L_1$ such that $\alpha(g) = b' - b$. The commutativity od the diagram implies $\lambda(g) = \mu(b' - b)$, and the injectivity then yields that $\lambda(g)$ is the unique element lifted by $b' - b$. Therefore, $b' = b + (b' - b)$ gives rise to $c' = c + \lambda(g)$, then $\pi(c') = c + \operatorname{im}\lambda = \pi(c)$. Hence $\delta(a)$ is independent of the choice of b, followed by δ is well-defined.
- Homomorphism condition: Suppose a gives rise to b and c, and a' gives rise to b' and c'. Then $\beta(b+b') = a+a'$ implies that $a + a'$ give rise to $b + b'$, and $\alpha_0(c + c') = \mu(b + b')$ implies that $b + b'$ gives rises to $a + a'$. It follows that $\delta(a + a') = c + c' = \delta(a) + \delta(a')$, and the statement for preserving multiplication is analogous.

The remaining proof is omitted and will be discussed later.

Chapter 5 Irreducibility and Factorization in Integral Domains

Introduction

- ❑ *Divisibility, Factorization*
- ❑ *Content, Gauss's Lemma*
- ❑ *Irreducible polynomials*
- ❑ *Unique Factorization Domain (UFD)*
- ❑ *Factorization in Polynomial Ring*
- ❑ *Intro. to field extension and algebraic closure*

5.1 Existence of Factorizations

Definition 5.1 (Divisibility, Associates)

*Let R be a commutative ring and $a, b \in R$. We say that a **divides** b (b is a multiple of a) if $b \in (a)$, i.e., there exists $c \in R$ such that $b = ac$, we use the notation $a \mid b$.*

*Two elements are **associates** if $(a) = (b)$, i.e., $a \mid b$ and $b \mid a$.* ♣

Remark Equivalently, $a \mid b$ holds if and only if $(b) \subset (a)$.

Proposition 5.1 (Characterization for associates)

Let R be an integral domain and $a, b \in R$, then a, b are associates if and only if $a = ub$ for a unit $u \in R$. ♠

Proof Suppose $a = ub$ where u is a unit. Then $b \mid a$, and $b = u^{-1}a$ implies that $a \mid b$; we therefore have a, b are associates. Conversely, suppose a, b are associates, namely $b = c_1 a$ and $a = c_2 b$ for $c_1, c_2 \in R$. Then $b = c_1 a = c_1 c_2 b$ implies that $(1 - c_1 c_2)b = 0$, followed by $1 - c_1 c_2 = 0$, namely $c_1 c_2 = 1$ since R is an integral domain. Hence c_2 is a unit and $a = c_2 b$ as desired. ■

Definition 5.2 (Prime Element, Irreducible Element)

Let R be an integral domain.

*(a) An element $a \in R$ is **prime** if the ideal is prime, i.e., a is not a unit and $a \mid bc \implies (a \mid b$ or $a \mid c)$.*

*(b) An element $a \in R$ is **irreducible** if a is not a unit and $a = bc \implies$ either (b or c is a unit). An element $a \in R$ is **reducible** if it is not irreducible.* ♣

Remark Equivalently, an element $a \in R$ is reducible if it is a unit or it can be written as the product $a = bc$ of non-unit elements.

Proposition 5.2 (Characterization of irreducible elements)

Let R be an integral domain and let $a \in R$. The following are equivalent:

(a) The element a is irreducible.

(b) $a = bc$ implies a is an associate of b or of c, i.e., $(a) = (b)$ or $(a) = (c)$.

(c) a is maximal among proper principle ideals, i.e., $(a) \subsetneq (b) \implies (b) = R$.

Proof $(a) \Rightarrow (b)$: Suppose a is irreducible and $a = bc$, then WLOG b is a unit, so a is an associate of c.

$(b) \Rightarrow (c)$: Suppose $(a) \subsetneq (b)$, then $a = bc$ for some $c \in R$. Since $(a) \neq (b)$, the hypothesis implies that $(a) = (c)$, so there exists d such that $a = dc$ for some unit d. Then $c = d^{-1}a = d^{-1}bc \Rightarrow (1 - d^{-1}b)c = 0 \Rightarrow d^{-1}b = 1 \Rightarrow b = d$, hence b is a unit.

$(c) \Rightarrow (a)$: Suppose $a = bc$ and b is not a unit. Then $(a) \subsetneq (c)$, and by the hypothesis, $(c) = R$, so c is a unit. ■

Proposition 5.3 (Prime elements are irreducible)

Let R be an integral domain and $a \in R$ is a nonzero prime element, then a is irreducible.

Proof Suppose a is prime and $a = bc$. WLOG, $a \mid b$ since a is prime, then $(a) = (c)$, followed by $a = bd$ for some unit d. Then $a = bc = ad^{-1}c \Rightarrow a(1 - d^{-1}c) = 0 \Rightarrow d^{-1}c = 1 \Rightarrow c = d$, hence c is a unit. ■

Example 5.1 The converse does not hold in general, it holds only when R is a UFD. Consider $\mathbb{Z}[\sqrt{-5}] = \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$ as a subring of $\mathbb{C}$. Define the norm map $N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$, $a + bi\sqrt{5} \mapsto a^2 + 5b^2$; N is multiplicative. Using the norm map, it is not hard to prove that the units are ± 1, and 3 is irreducible. Notice that $3 = (2 + \sqrt{5}i)(2 - \sqrt{5}i)$, but $3 \nmid (2 \pm \sqrt{5}i)$, we conclude 3 is not prime. Therefore, a irreducible element is not necessarily prime.

5.2 UFDs, PIDs, Euclidean Domains

5.2.1 Unique Factorization Domains (UFDs)

Definition 5.3 (Factorizations, Unique Factorization Domain (UFD))

Let R be an integral domain.

- *An element $r \in R$ has a* ***factorization*** *(or decomposition) into irreducibles if there exist irreducible elements $q_1, \cdots, q_n$ such that $q = q_1 \cdots q_n$. The factorization is said to be* ***unique*** *if the q_i are determined uniquely up to the order and associates.*
- *We say R is a* ***domain with factorizations*** *if every nonzero, non-unit element $r \in R$ has a factorization into irreducibles. If all such factorizations are unique, R is called the* ***unique factorization domain (UFD)****.*

Remark In a UFD, we can write any nonzero element r as $r = \varepsilon q_1 \cdots q_n$ where ε is unit.

Note *Suppose $r = q_1 \cdots q_n$ is a factorization, we may assign to r a multiset $\{q_1, \cdots, q_n\}$ of its irreducible factors. Consider an equivalence relation that modulo out permutations and associates, then the factorization is uniquely determined up to equivalence in UFD.*

Example 5.2 Suppose α is a unit. Then there is no decomposition $\alpha = xy$ where x is irreducible, since $x(\alpha^{-1}y) = 1$ implies x is a unit. It follows that α has no decomposition, i.e., the corresponding multiset is $\varnothing$.

Suppose x is irreducible. Then $x = yz$ and y being irreducible implies z is a unit by the definition of irreducibility, hence the corresponding multiset is $\{x\}$ under equivalence relation.

Lemma 5.1

Let R be a UFD, and let a, b, c be nonzero elements of R. Then

(a) $(a) \subset (b)$ if and only if the multiset of irreducible factors of b is contained in the multiset of irreducible factors of a;

(b) a and b are associates if and only if the two multisets coincide.

(c) the irreducible factors of a product bc are the collection of all irreducible factors of b and of c.

Definition 5.4 (gcd)

Let R be an integral domain, and let $a, b \in R$. An element $d \in R$ is a ***greatest common divisor (gcd)*** *of a and b if $(a, b) \subset (d)$ and (d) is the smallest principal ideal in R with this property.*

Remark Equivalently, d is the gcd of a, b if and only if $a \mid d$, $b \mid d$, and $(a \mid e,\ b \mid e) \Rightarrow d \mid e$ for all e.

The greatest common divisor is unique up to associates.

Proposition 5.4 (UFDs are GCD domain)

Let R be a UFD, and let a, b be nonzero elements of R. Then a, b have a greatest common divisor. ♠

Proof Sketch: Given that R is a UFD, we may write $a = \mu q_1^{\alpha_1} \cdots q_n^{\alpha_n}$ and $b = \nu q_1^{\beta_1} \cdots q_n^{\beta_n}$, where μ, ν are units, $\alpha_i, \beta_i \geq 0$ for all i, and q_i and q_j are not associates if $i \neq j$. Let

$$d = q_1^{\min(\alpha_1,\beta_1)} \cdots q_n^{\min(\alpha_n,\beta_n)}.$$

It is clear that $d \,|\, a$ and $d \,|\, b$. Suppose c such that $c \,|\, a$ and $c \,|\, b$, then $c = \omega q_1^{\gamma_1} \cdots q_n^{\gamma_n}$. Note that the irreducible factors must be contained in both multisets of a and b, so $\gamma_i \leq \min(\alpha_i, \beta_i)$ for all i, followed by $c \,|\, d$. ■

Lemma 5.2 (Irreducible elements are prime in UFD)

Let R be a UFD, and let a be an irreducible element of R. Then a is prime. ♡

Proof Suppose a is irreducible and $a \,|\, bc$. Since $(bc) \subset (a)$, a is contained in the irreducible factors of bc by Lemma 5.1. Then a must be contained in the irreducible factor of b or c because the irreducible factors of bc is the union of factors of b and factors of c. Hence a divides b or c, followed by a is prime. ■

Proposition 5.5

Let R be an integral domain. Show that R is a UFD if and only if both the following conditions are satisfied:

(1) R satisfies the ascending chain condition (a.c.c.) for principal ideals (i.e., any ascending chain of principal ideals stabilizes).

(2) Every irreducible element of R is prime. ♠

Remark See Noetherian ring (Definition 5.6) for a.c.c.

Proposition 5.6

If R is a PID, then it is a UFD. ♠

5.2.2 Principle Ideal Domains (PID) and Euclidean Domain (EDs)

Proposition 5.7

A ring R is a field if and only if $R[x]$ is a PID. ♠

Definition 5.5 (Euclidean Domain)

*A **Euclidean valuation** on an integral domain R is a valuation $v : R \to \mathbb{N}$ such that for all $a \in R$ and nonzero $b \in R$ there exist $q, r \in R$ such that $a = qb + r$, with either $r = 0$ or $v(r) < v(b)$. An integral domain R is a **Euclidean domain** if it admits a Euclidean valuation.* ♣

Proposition 5.8

Let R be a Euclidean domain, then R is a PID. ♠

Proof Sketch: Similar to proving $\mathbb{Z}$ is a PID, we may use Euclidean division lemma to show that the element $a \in I$ such that $v(a) = \min v(R)$ satisfy that $b \in R$ implies $b = ab'$ for some $b' \in R$, hence $I = (r)$.

Lemma 5.3

Let $a = bq + r$ in a ring R, then $(a, b) = (b, r)$. In particular, a, b have a gcd if and only if b, r have one, and in this case $\gcd(a, b) = \gcd(b, r)$. ♡

Proof Note that $a = bq + r \in (b, r)$, so $(a, b) \subset (b, r)$; and $r = a - bq \in (a, b)$ implies $(b, r) \subset (a, b)$. Hence $(a, b) = (b, r)$. ■

Note *We may use Euclidean algorithm (with Euclidean valuation) to compute* gcd.

5.2.3 Noetherian Ring

Definition 5.6 (Noetherian Ring)

*A commutative ring R is said to be **Noetherian** if every ideal of R is finitely generated.* ♣

Proposition 5.9

*The commutative ring R is Noetherian if and only if the **ascending chain condition (a.c.c.)** holds for all ideals, i.e., every chain*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

stabilizes, *meaning that for every such chain there exists $N \in \mathbb{N}$ such that $I_n = I_N$ for all $n \geq N$.* ♠

5.3 Unique Factorization in Polynomial Ring

5.3.1 Primitivity and Content, Gauss's Lemma

Lemma 5.4

Suppose R is a ring and $I \trianglelefteq R$, let $IR[x] := \{a_0 + a_1x + \cdots a_dx^d \in R[x] \,|\, a_i \in I\}$, the $R[x]/(IR[x]) \cong (R/I)[x]$.

If I is a prime ideal of R, then $IR[x]$ is a prime ideal of $R[x]$.

Definition 5.7 (Primitive Polynomial)

*Let R be a commutative ring, and $f \in R[x]$. The polynomial f is said to be **primitive** if $f \notin \mathfrak{p}R[x]$ for every prime principle ideal $\mathfrak{p}$; and it is said to be **very primitive** is the above statement holds for all prime ideals $\mathfrak{p}$.*

Proposition 5.10

Let R be a commutative ring and $f, g \in R[x]$, then fg is primitive if and only if both f and g are primitive.

Proof f, g is not primitive iff $fg \in \mathfrak{p}R[x]$ for some principle prime ideal $\mathfrak{p}$, iff either $f \in \mathfrak{p}R[x]$ or $g \in \mathfrak{p}R[x]$ (given that $\mathfrak{p}R[x]$ is a prime ideal), iff f or g is not primitive. ■

Proposition 5.11 (Equivalent definition of primitivity)

Let R be a commutative ring and $f = a_0 + a_1x + \cdots + a_dx^d \in R[x]$. Then

(a) f is very primitive if and only if $(a_0, \cdots, a_d) = (1)$.

(b) If R is a UFD, then f is primitive if and only if $\gcd(a_0, \cdots, a_d) = 1$.

Proof (a) Suppose $(a_0, \cdots, a_d) \neq R$, then they are contained in a maximal ideal thus a prime ideal, so f is not very primitive. Conversely, suppose $(a_0, \cdots, a_d) = R$, then no prime ideals contain all $a_0, \cdots, a_d$, so f is not very primitive.

(b) Suppose $d := \gcd(a_0, \cdots, a_d) \neq 1$, then $f \in (d)R[x] \subset (d_0)R[x]$ for any irreducible (thus prime) factor d_0 of d, so f is not primitive since (d_0) is a principle prime ideal. Conversely, suppose f is not primitive, i.e., $f \in (p)R[x]$ for some prime p. Then p divides $\gcd(a_0, \cdots, a_d)$, so the gcd is not 1. ■

Definition 5.8 (Content)

*Let R be a UFD. The **content** of a nonzero polynomial $f \in R[x]$, denoted $cont_f$, is the $\gcd$ of its coefficients.*

Note *The polynomial f is primitive if and only if $(cont_f) = (1)$*

Proposition 5.12

Let R be a UFD, and let $f \in R[x]$. Then

(a) $(f) = (\mathrm{cont}_f)(f')$, where f' is primitive.

(b) If $(f) = (c)(g)$, with $c \in R$ and g primitive, then $(c) = (\mathrm{cont}_f)$.

Proof (a) Let $a_i' := a_i/\mathrm{cont}_f$, and put $f' = a_0' + \cdots a_d'x^d$. Note that f' is primitive since $\gcd(a_0', \cdots, a_d') = \gcd(a_0, \cdots, a_d)/\mathrm{cont}_f = 1$, and $f = \mathrm{cont}_f f'$, hence $(f) = (\mathrm{cont}_f)(f')$.

(b) Since f and cg are associates given that $(f) = (cg)$, $f = ucg$ for some unit u. Then $\mathrm{cont}_f = \mathrm{cont}_{ucg} = uc\mathrm{cont}_g = uc$ by the property of gcd, so cont_f and c are associates, followed by $(\mathrm{cont}_f) = (c)$. ■

Theorem 5.1 (Gauss's Lemma)

Let R be a UFD, and let $f, g \in R[x]$. Then $(\mathrm{cont}_{fg}) = (\mathrm{cont}_f)(\mathrm{cont}_g)$.

Proof $fg = (\mathrm{cont}_f)(f')(\mathrm{cont}_g)(g') = (\mathrm{cont}_f)(\mathrm{cont}_g)(f'g')$ where $f', g' \in R[x]$ are primitive. Notice that $f'g'$ is primitive by Proposition 5.10, $(\mathrm{cont}_{fg}) = (\mathrm{cont}_f)(\mathrm{cont}_g)$ follows from Proposition 5.12. ■

Corollary 5.1

Let R be a UFD, and let $f, g \in R[x]$. Assume $(f) \subset (g)$, then $(\mathrm{cont}_f) \subset (\mathrm{cont}_g)$.

5.3.2 Field of Fractions

Given an integral domain R, consider the category $\mathscr{R}$ whose objects are (i, K) where K is a field and $i : R \hookrightarrow K$ is an *injective* ring homomorphism, and the morphisms are field homomorphism $\alpha : K \to L$.

Definition 5.9 (Field of Fraction)

*The **field of fractions** $K(R)$ of R is an initial object of the category $\mathscr{R}$, i.e., $K(R)$ is the smallest field containing R.*

The field of fraction $K(R)$ may be constructed as $R \times R^*$ over an equivalence relation, $K(R) := \{a/r \mid a \in R, r \in R^*\}/\sim$, where $a/r \sim b/s$ if $as - br = 0$ (note that R is an integral domain). The operations defined as follows

$$\frac{a}{r} + \frac{b}{s} = \frac{as + br}{rs}, \qquad \frac{a}{r} \cdot \frac{b}{s} = \frac{ab}{rs}$$

make $K(R)$ a field.

Example 5.3 The field of fraction of $\mathbb{Z}$ is $K(\mathbb{Z}) = \mathbb{Q}$.

Definition 5.10 (Field of Rational Functions)

*The **field of rational functions** with coefficients in R is the field of fractions of the ring $R[x]$, denoted $R(x)$. The elements of $R(x)$ are fractions of polynomials $p(x)/q(x)$, where $p(x), q(x) \in R[x]$ and $q(x) \neq 0$.*

5.3.3 R UFD Implies R[x] UFD

Proposition 5.13

Let R be a UFD, and $F = K(R)$ be its field of fractions. For nonzero $f, g \in R[x]$, if $(\text{cont}_g) \subset (\text{cont}_f)$ and $(g)_F \subset (f)_F$, then $(g) \subset (f)$.

Proof Since $(g)_F \subset (f)_F$, $g = (a/b)f$ for some $a/b \in F$, taking content yields $\text{cont}_g = (a/b)\text{cont}_f$. By $(\text{cont}_g) \subset (\text{cont}_f)$, $\text{cont}_g = c \cdot \text{cont}_f$ for some $c \in R$, so $c \cdot \text{cont}_f = \text{cont}_g = (a/b)\text{cont}_f$. It follows that $a/b = c \in R$, so $g = (a/b)f = cf$, hence $(g) \subset (f)$. ■

Proposition 5.14

Let R be a UFD, and let F be its field of fraction. Let $f \in R[x]$ be a nonconstant polynomial. Then f is irreducible in $R[x]$ if and only if f is primitive and irreducible in $F[x]$.

Proof The if direction is trivial. Suppose $f \in R[x]$ is irreducible. Then f is primitive, otherwise $f = \text{cont}_f f'$ is a decomposition. Assume f is reducible in $F[x]$ for the sake of contradiction, i.e., $f = gh$ for $g, h \in F[x]$. We can write $g = cg'$ and $h = dh'$ for some $c, d \in F$ and some primitive polynomials $g', h' \in R[x]$[1]. Note that $f = cdf'g'$, so $(cd) = (\text{cont}_f) = (1)$ since f is primitive, followed by $f = uf'g'$ for some unit $u \in R$. Hence $f = (uf')(g')$ is a desired decomposition of f in $R[x]$, and both $uf' \in R[x]$ and $g' \in R[x]$ are not unit, contradicting that f is irreducible, therefore f is irreducible in $F[x]$. ■

[1]: this can be done by taking $c = \gcd(a_0, \cdots, a_d)/\text{lcm}(b_0, \cdots, b_d)$ for $g = \sum (a_i/b_i)x^i$, and d is defined analogously.

Theorem 5.2 (R UFD $\Rightarrow R[x]$ UFD)

Let R be a UFD, then $R[x]$ is a UFD.

Proof (*Existence*) Since $F := \text{Frac}(R)$ is a field, its polynomial ring is a UFD (since it is a PID), so $f \in R[x]$ has a factorization $f = uf_1' \cdots f_n'$ where $u \in F$ and f_i''s are irreducible. Each f_i' can be written as $f_i' = u_i f_i$ for some $u_i \in F$ and primitive polynomial $f_i \in R[x]$ (by multiplying some constant); note that each f_i is irreducible in $K[x]$ since u_i is a unit in $K[x]$, therefore f_i is irreducible in $R[x]$. Then $f = (uu_1 \cdots u_n)f_1 \cdots f_n$, and $v := uu_1 \cdots u_n \in R$ by taking content. Since R is a UFD, we may decompose v in R to $v = d_1 \cdots d_m$. Hence $f = u_1 \cdots u_m f_1 \cdots f_n$ is a factorization in $R[x]$ since all u_i's and f_i's are irreducible.

(*Uniqueness*) Suppose $f = d_1' \cdots d_{m'}' f_1' \cdots f_{n'}'$. Since $(d_1 \cdots d_m) = (d_1' \cdots d_{m'}') = \text{cont}_f$, $\{d_i\}$ and $\{d_i'\}$ are equivalent under ordering and associates. Since $K[x]$ is a UFD and $f_1 \cdots f_n \sim f_1' \cdots f_{n'}'$, $\{f_i\}$ and $\{f_i'\}$ are equivalent under ordering and associates in $K[x]$; in addition, the factor u_i s.t. $f_i = u_i f'_i$ is a unit in R by the content consideration, so the equivalence extends to $R[x]$. Hence the factorization of f is unique. ■

Remark The motivation is that we may write $f = \text{cont}_f f'$ where f' is primitive, then we can decompose cont_f in R and f' in $K[x]$ (which is a UFD). Since factorization of primitive f' in $F[x]$ is equivalent compare to $R[x]$, combining the factorizations of cont_f and f' gives the desired, and indeed unique, factorization.

Note *We may also use Proposition 5.5 (a.c.c. of principle ideals) to prove the existence of factorization.*

5.4 Irreducibility of Polynomials

5.4.1 Roots and Irreducibility

Definition 5.11 (Root)

Suppose $f \in R[x]$, we say $a \in R$ is a ***root*** *of f if $\text{ev}_a(f) = 0$, the root a has a* ***multiplicity*** *r if $(x-a)^r \mid f$ but $(x-a)^{r+1} \nmid f$.*

Remark $a \in R$ is a root of f if and only if $(x-a) \mid f$.

Proof: Note that $R[x]/(x-a) \cong R$ by the evaluation homomorphism $\text{ev}_a(f)$, so a is a root iff $f \in \ker \text{ev}_a$, iff $f \in (x-a)R[x]$, iff $(x-a) \mid f$. ■

Lemma 5.5

Let R be an integral domain, and let $f \in R[x]$ be a polynomial of degree n. Then the number of roots of f, counted with multiplicity, is at most n.

Proof Let $K = \text{Frac}(R)$ and consider $f \in K[x]$. Since $K[x]$ is a UFD, roots of f in K corresponds to irreducible factors of degree 1 in $K[x]$, so f has at most n roots in K. Hence f has at most n roots in R. ■

Alternative Proof: We proceed by strong induction on $n = \deg f$. The case is trivial for $n = 1$. Suppose $n > 1$ and a is a root of f with multiplicity of r. Then $(x-a)^r \mid f$, $f = (x-a)^r g$ for some g s.t. $\deg g = n - r$ (note that $\deg fg = \deg f + \deg g$ in an integral domain). By inductive hypothesis, g has at most $n-r$ roots with multiplicity, then $(x-a)^r g$ has at most n roots. ■

Example 5.4 The integral domain condition is necessary. Consider $f = 2x$ in $\mathbb{Z}/4\mathbb{Z}$ and $f = (x+2)(x+3)$ in $\mathbb{Z}/6\mathbb{Z}$.

Corollary 5.2

Let R be an infinite integral domain, and $f, g \in R[x]$. Then $f = g$ if and only if their evaluation $r \mapsto f(r)$ and $r \mapsto g(r)$ agrees.

Proof The evaluation agrees iff every $r \in R$ is a root of $f - g$, but nonzero polynomial cannot have infinitely many roots, so $f - g = 0$, namely $f = g$. ■

Proposition 5.15

Let R be a UFD and $K = \text{Frac}(R)$ be its field of fractions. Let $f(x) = a_0 + a_1 x + \cdots a_n x^n \in R[x]$, and let $c = p/q \in K$ be a root of f with $\gcd(p, q) = 1$. Then $p \mid a_0$ and $q \mid a_n$ in R.

Proof Since $f(\frac{p}{q}) = a_0 + a_1 \frac{p}{q} + \cdots + a_n \frac{p^n}{q^n} = 0$, then $a_0 q^n + a_1 p q^{n-1} + \cdots + a_n p^n = 0$. Note that $a_0 q^n = -p(a_1 q^{n-1} + \cdots + a_n p^{n-1})$, then $p \mid a_0 q^n$. Since p, q are relatively prime in a UFD, the multiset of irreducibles factors of p belongs to the multiset of a_0, followed by $p \mid a_0$. $q \mid a_n$ follows analogously. ■

5.4.2 Toward Field Extension

Definition 5.12 (Field Extension)

*Suppose the inclusion map $i : k \to F$ is a homomorphism of fields, then we say that F is an **extension** of k, denoted by $k \subseteq F$ (or F/k).* ♣

Remark Homomorphisms of field are defined to be the ring homomorphism between fields, and they are necessarily injective.

Proposition 5.16 (Extension by adjoining a root)

Let k be a field, let $f(t) \in k[t]$ be a nonzero irreducible polynomial. Then

(a) $F := k[t]/(f(t))$ is a field, endowed with a natural homomorphism $i : k \hookrightarrow F$ (obtained as the composition $k \to k[x] \to F$) realizing it as an extension of k.

(b) $f(x) \in k[x] \subseteq F[x]$ has a root in F, namely the coset of t.

(c) If $k \subseteq K$ is any extension in which f has a root, then there exists a homomorphism $j : F \to K$ such that the diagram

$$\begin{tikzcd} k \arrow[rr] \arrow[dr, hook, "i"'] & & K \\ & F \arrow[ur, dashed, "j"'] & \end{tikzcd}$$

commutes. ♠

Proof (a) $f(t)$ is irreducible thus prime in $k[t]$ since it is UFD, therefore $(f(t))$ is a prime ideal thus a maximal ideal since $k[t]$ is PID, followed by $F = k[t]/(f(t))$ is a field.

(b) Let $\bar{h} = h + (f(t)) \in F$ be the coset of h in F. Since $\mathrm{ev}_{\bar{t}}(f) = f(\bar{t}) = \overline{f(t)} = \bar{0}$, then $\bar{t} \in F$ is a root of $f(x) \subseteq F[x]$.

(c) Suppose $u \in K$ is a root of f, and consider the evaluation homomorphism $\mathrm{ev}_u : k[t] \to K$. Note that $(f(t)) \subseteq \ker \mathrm{ev}_u$ since $f(u) = 0$, then by the universal property there exists an homomorphism $F = k[t]/(f(t)) \to K$. ■

Example 5.5 By Proposition 5.15, note that $i \in \mathbb{C}$ is a root of x^2+1, there is a homomorphism $\widetilde{\mathrm{ev}}_i : \mathbb{R}[x]/(x^2+1) \hookrightarrow \mathbb{C}$ induced by $\mathrm{ev}_i : \mathbb{R}[x] \to \mathbb{C}$, i.e., $\widetilde{\mathrm{ev}}_i : f + (x^2+1) \mapsto \mathrm{ev}_i(f)$. It is not hard to verify that $\widetilde{\mathrm{ev}}_i$ is bijective and thus an isomorphism. Hence $\mathbb{C} \cong \mathbb{R}[x]/(x^2+1)$.

Definition 5.13 (Algebraically Closed Field)

*A field k is **algebraically closed** if all irreducible polynomials in $k[x]$ have a degree 1.* ♣

Lemma 5.6 (Characterization of algebraically closedness)

A field k is algebraically closed if and only if every polynomial $f \in k[x]$ factors completely as a product of linear factors, if and only if every nonconstant polynomial $f \in k[x]$ has a root in k. ♡

Proposition 5.17

Algebraically closed fields are infinite. ♠

Proof Assume $F = \{c_1, \cdots, c_n\}$ be a finite field for contraposition. Consider the polynomial $f(x) = (x - c_1) \cdots (x - c_n) + 1 \in F[x]$. It is clear that $f \neq 0$ and $f(x)$ has no roots in F, so F is not algebraically closed. ■

5.4.3 Irreducibility in the Complex and Real Polynomial Ring

Theorem 5.3 (Fundamental Theorem of Algebra)

$\mathbb{C}$ is algebraically closed. ♡

Proposition 5.18 (Irreducibility of polynomials in $\mathbb{R}[x]$)

(a) Every polynomial $f \in \mathbb{R}[x]$ with $\deg(f) \geq 3$ is reducible.

(b) The nonconstant irreducible polynomials in $\mathbb{R}[x]$ are precisely the polynomials of degree 1 and the quadratic polynomials $f = ax^2 + bx + c$ with $b^2 - 4ac < 0$. ♠

Proof (a) Let $f = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{R}[x]$ for which $\deg f \geq 3$. Consider $f \in \mathbb{C}[x]$, f has a root z in $\mathbb{C}$ by the algebraic closedness. If $z \in \mathbb{R}$, then $f = (x - z)g$ and $\deg g \geq 2$, so f is reducible. On the other hand, if $z \notin \mathbb{R}$, consider its conjugate $\bar{z}$. Note that $a_i \in \mathbb{R}$,

$$f(\bar{z}) = a_0 + a_1\bar{z} + \cdots + a_n\bar{z}^n = \overline{a_0} + \overline{a_1z} + \cdots + \overline{a_nz^n} = \overline{f(z)} = 0,$$

it follows that $\bar{z}$ is a root of f. That is, f is divisible by $(x - z)(x - \bar{z}) = (x^2 + \text{Re}(z)) + \text{Im}(z)^2 \in \mathbb{R}[x]$. Since $\deg(x - z)(x - \bar{z}) = 2 < \deg f$, then f is reducible in $\mathbb{R}[x]$.

(b) follows from part (a) and the fact that the roots of $ax^2 + bx + c$ in $\mathbb{C}$ are not real if and only if $b^2 - 4ac < 0$. ■

Proposition 5.19 (Eisenstein Criterion)

Let R be a (commutative) ring, and let $\mathfrak{p}$ be a prime ideal of R. Let $f = a_0 + a_1x + \ + a_nx^n \in R[x]$ be a polynomial, and assume that (i) $a_n \notin \mathfrak{p}$; (ii) $a_i \in \mathfrak{p}$ for $i = 0, \cdots, n-1$; and (iii) $a_0 \notin \mathfrak{p}^2$. Then f is not the product of polynomials of degree $< n$ in $R[x]$. ♠

Proof Assume $f = (b_0 + \cdots + b_jx^j)(c_0 + \cdots + c_kx^k)$, where $j + k = n$, for the sake of contradiction. Let $\gamma_n(f)$ denotes the i-th term coefficient. Note that $b_0c_0 = \gamma_0(f) = a_0 \in \mathfrak{p}$, then by the definition of prime ideal, we may assume $b_0 \in \mathfrak{p}$ w.l.o.g., and $c_0 \notin \mathfrak{p}$ since $a_0 \notin \mathfrak{p}^2$. We proceed by induction on $i < j$ to prove $b_i \in \mathfrak{p}$: assume $b_0, \cdots, b_{i-1} \in \mathfrak{p}$ and $c_0 \notin \mathfrak{p}$, then

$$\mathfrak{p} \ni a_i = \gamma_i(f) = b_0c_i + b_1c_{i-1} + \cdots + b_ic_0 \quad \Longrightarrow \quad b_ic_0 \in \mathfrak{p} \quad \Longrightarrow \quad b_i \in \mathfrak{p}.$$

Therefore, $b_j \in \mathfrak{p}$ implies $a_n = b_jc_k \in \mathfrak{p}$, contradiction. ■

Chapter 6 Fields

Introduction

- *The category of field*
- *Simple extensions*
- *Algebraic and transcendental extensions*
- *Splitting fields*
- *Separable extensions and separable degree*
- *Galois correspondence and Galois groups*
- *Geometric impossibilities*
- *Field extensions*
- *k-automorphisms*
- *Algebraic closure $\bar{k}$*
- *Normal fields*
- *Finite extensions*
- *The fundamental theorem of Galois theory*
- *Cyclotomic fields*

6.1 Field Extensions, I

Definition 6.1 (The Category of Fields, $\textsc{Fld}$)

The category $\textsc{Fld}$ is the category of fields with field homomorphisms (namely ring homomorphism). We denote by $\textsc{Fld}_n$, for $n = 0$ or $n = p$ where p is a nonnegative prime, the category of fields with characteristic n. ♣

Note *Let $k \subseteq F$ be a field extension, then the characteristic of k is equal to the characteristic of F.*

Example 6.1 The ***initial*** object of $\textsc{Fld}_0$ is $\mathbb{Q}$ and the initial object of $\textsc{Fld}_p$ is $\mathbb{Z}/p\mathbb{Z}$ for nonnegative prime p. However, $\textsc{Fld}$ has no initial objects.

6.1.1 Simple Extension

Definition 6.2 (Degree of an Extension)

*A field extension $k \subseteq F$ is finite, of **degree** n, if F has (finite) dimension $\dim F = n$ as a vector space over k, we write $[F : k] = n$. The extension is infinite otherwise, denoted by $[f : k] = \infty$.* ♣

Remark The degree of the field extension $F = k[t]/(p(t))$, where $p(t)$ is a monic irreducible polynomial, through adjoining a root is $n = \deg p(x)$, since the cosets of $1, t, \cdots, t^{n-1}$ form a basis of the vector space over k.

Definition 6.3 (Simple Extension)

Let $k \subseteq F$ be a field extension, and let $\alpha \in F$. The smallest subfield of F containing both k and α is denoted $k(\alpha)$; that is, $k(\alpha)$ is the intersection of all subfields of F containing k and α.

*A field extension $k \subseteq F$ is **simple** if there exists an element $\alpha \in F$ such that $F = k(\alpha)$.* ♣

Remark The characterization of the simple extension $k(\alpha)$ is the fraction field of the (finite) sum $k + k\alpha + k\alpha^2 + \cdots$ if the extension is infinite, and it is $k + k\alpha + \cdots + k\alpha^{n-1}$ if the extension has degree n.

Proposition 6.1

Let $k \subseteq k(\alpha)$ be a simple extension. Consider the evaluation map: $\epsilon : k[t] \to k(\alpha)$, defined by $f(t) \to f(\alpha)$. Then we have the following:

(a) ϵ is injective if and only if $k \subseteq k(\alpha)$ is an infinite extension. In this case, $k(\alpha)$ is isomorphic to the field of rational functions $k(t)$.

(b) ϵ is not injective if and only if $k \subseteq k(\alpha)$ is finite. In this case there exists a unique monic irreducible nonconstant polynomial $p(t) \in k[t]$ of degree $n = [k(\alpha) : k]$ such that

$$k(\alpha) \cong k[t]/(p(t))$$

Via this isomorphism, α corresponds to the coset of t. The polynomial $p(t)$ is the monic polynomial of smallest degree in $k[t]$ such that $p(\alpha) = 0$ in $k(\alpha)$. ♠

Proof Suppose $\epsilon : k[t] \to k(\alpha)$ is injective, then the universal property of field of fraction implies the existence of field homomorphism $k(x) \hookrightarrow k(\alpha)$. Since the (isomorphic) image of $k(x)$ contains k and α, hence $k(x) \cong k(\alpha)$ by the definition of $k(\alpha)$. The extension is infinite because $1, \alpha, \alpha^2, \cdots \in k(\alpha)$ are linearly independent.

Suppose ϵ is not injective, then its kernel is $\ker \epsilon = (p(t))$ for some $p(t) \in k[t]$ (unique if restricted to monic polynomials), since $k[x]$ is a PID. The first isomorphism theorem implies $k[t]/(p(t)) \cong \operatorname{im} \epsilon \subset k(\alpha)$, therefore $k[t]/(p(t)) \cong k(\alpha)$ since the image of $k[t]/(p(t))$ contains k and α, and $[k(\alpha) : k] = \deg p$ is finite. ■

Example 6.2 $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}\}$ is a simple extension of $\mathbb{Q}$, whose primitive elements are $\pm\sqrt{2}$, minimal polynomial is $x^2 - 2$, and the degree of extension is 2.

$\mathbb{C}$ is a simple extension of $\mathbb{R}$, whose primitive elements are $\pm i$, minimal polynomial is $x^2 + 1$,and the degree of extension is 2.

Proposition 6.2

Let $k_1 \subseteq F_1 = k_1(\alpha_1)$, $k_2 \subseteq F_2 = k_2(\alpha_2)$ be two finite simple extensions. Let $p_1(t) \in k_1[t]$, resp., $p_2(t) \in k_2[t]$ be the minimal polynomials of α_1, resp., α_2. Let $i : k_1 \to k_2$ be an isomorphism, such that $i'(p_1(t)) = p_2(t)$, where $i' : k_1[t] \to k_2[t]$ is induced by i. Then there exists a unique isomorphism $j : F_1 \to F_2$ agreeing with i on k_1 and such that $j(\alpha_1) = \alpha_2$. ♠

Remark

$$\begin{tikzcd}
k_1 \arrow[r, hook] \arrow[d, "i"] & k_1(\alpha_1) \arrow[d, dashed, "j"'] \\
k_2 \arrow[r, hook] & k_2(\alpha_2)
\end{tikzcd}$$

Proof The function $i' : k_1[t] \to k_2[t]$ induced by i is clearly an isomorphism. By the universal property of quotient, since $(p_1(x)) = \ker(\pi_2 \circ i')$, there exists an unique homomorphism $j : k_1[t]/(p_1) \to k_2[t]/(p_2)$ such that

$$\begin{tikzcd}
k_1[t] \arrow[r, two heads, "\pi_1"'] \arrow[d, "i'"', "\sim"] & k_1[t]/(p_1) \arrow[d, dashed] \\
k_2[t] \arrow[r, two heads, "\pi_2"] & k_2[t]/(p_2)
\end{tikzcd}$$

j is an isomorphism since i' is an isomorphism, hence there is an unique isomorphism $j : F_1 \to F_2$. ■

Definition 6.4 (k-Automorphism Group)

Let $k \subseteq F$ be a field extension. The group of automorphisms of the extension, denoted $Aut_k(F)$, is the group of field automorphisms $j : F \to F$ such that $j|_k = id_k$.

Proposition 6.3

Let $k \subseteq F = k(\alpha)$ be a simple finite extension, and let $p(x)$ be the minimal polynomial of α over k. Then $|Aut_k(F)|$ equals the number of distinct roots of $p(x)$ in F.

In particular, $|Aut_k(F)| \leq [F : k]$, with equality if and only if $p(x)$ factors over F as a product of distinct linear polynomials.

Proof We associate with each k-automorphism σ the image $\sigma(\alpha)$. Let $p(t) = p_0 + p_1 t + \cdots + p_n t^n \in k[t]$. Since σ extends identity on k, $p(\sigma(\alpha)) = p_0 + p_1\sigma(\alpha) + \cdots + p_n\sigma(\alpha)^n = \sigma(p(\alpha)) = \sigma(0) = 0$, followed by $\sigma(\alpha)$ is a root of $p(x)$. Every root β uniquely determines an k-automorphism such that $j(\alpha) = \beta$ by the above proposition,

$$\begin{tikzcd}
 & k(\alpha) \arrow[dd, dashed] & \alpha \arrow[dd, dashed, mapsto] \\
k \arrow[ur] \arrow[dr] & & \\
 & k(\beta) & \beta
\end{tikzcd}$$

hence $|\text{Aut}_k(F)|$ equals the number of distinct roots of $p(x)$ in F. ■

Example 6.3 There are exactly one embedding of $\mathbb{Q}[t]/(t^2 - 2)$ in $\mathbb{R}$. There are exactly three embeddings of $\mathbb{Q}[t]/(t^3 - 2)$ in $\mathbb{C}$.

6.1.2 Algebraic and Transcendantal Extension

Definition 6.5 (Algebraic and Transcendantal Extension)

Let $k \subseteq F$ be a field extension, and let $\alpha \in F$. Then α is ***algebraic*** *over k, of degree n if $n = [k(\alpha) : k]$ is finite; α is* ***transcendantal*** *over k otherwise.*

The extension F/k is ***algebraic*** *if every $\alpha \in F$ is algebraic.*

Proposition 6.4

$\alpha \in F$ is algebraic over k if and only if there exists a nonzero polynomial $f(x) \in k[x]$ such that $f(\alpha) = 0$.

Proof By the characterization of finite simple extension, $k(\alpha) \cong k[t]/(p(t))$ for a unique monic irreducible polynomial by Proposition 6.1. Then it is not hard to see that $p(\alpha) = 0$. ■

Proposition 6.5

Let $k \subseteq E \subseteq F$ be field extensions. Then $k \subseteq F$ is finite if and only if both $k \subseteq E$ and $E \subseteq F$ are finite. In this case, $[F : k] = [F : E][E : k]$.

Proof Suppose F/k is finite, then E/k is finite since it is a subspace of F/k, and F/E is finite because every basis of F/k spans F/E. Conversely, suppose F/E and E/k are finite, let $(e_1, \cdots, e_n)$ and $(k_1, \cdots, k_m)$ be their bases, resp. Consider the product $(e_i k_j)_{i,j}$. It is not hard to prove they are linearly independent in F/k and spans F/k. Therefore, F/k is finite; indeed, $[F : k] = nm = [F : E][E : k]$. ■

Proposition 6.6

Let $k \subseteq F = k(\alpha_1, \cdots, \alpha_n)$ be a finitely generated field extension. Then the following are equivalent:

(i) $k \subseteq F$ is a finite extension.

(ii) $k \subseteq F$ is an algebraic extension.

(iii) Each α_i is algebraic over k.

If these conditions are satisfied, then $[F : k] \leq$ the product of the degrees of α_i over k.

Proof $(i) \Rightarrow (ii)$ It follows immediately that $[k(\alpha_i) : k] \leq [F : k]$ since $k(\alpha_i) \subseteq F$.

$(ii) \Rightarrow (iii)$ This statement is trivial by definition.

$(iii) \Rightarrow (i)$ Suppose F/k is algebraic, and let $k_m := k(\alpha_1, \cdots, \alpha_m)$. For each m, $[k_m : k_{m-1}] = [k_{m-1}(\alpha_m) : k_{m-1}] \leq [k(\alpha_m) : k]$ is no greater than the degree of α_i, in particular, is finite. Therefore, $[F : k] = \prod_{m=1}^{n} [k_m : k_{m-1}] \leq$ product of degrees of α_i, in particular, is finite. ■

Corollary 6.1

Let $k \subseteq F$ be a field extension. Let $E = \{\alpha \in F \,|\, \alpha$ is algebraic over $k\}$. Then E is a field. ♡

Proof Suppose $\alpha, \beta \in F$ are algebraic over k, then $k(\alpha, \beta)/k$ is an algebraic extension (Proposition 6.6), followed by $\alpha \pm \beta$, $\alpha\beta^{-1}$ are algebraic. ■

Proposition 6.7

Let $k \subseteq E \subseteq F$ be field extensions. Then $k \subseteq F$ is algebraic if and only if both $k \subseteq E$ and $E \subseteq F$ are algebraic. ♠

6.2 Algebraic Closures

6.2.1 Algebraic Closures

Definition 6.6 (Algebraically Closed, Algebraic Closure)

*A field K is **algebraically closed** if all irreducible polynomials in $K[x]$ have degree 1.*

*An **algebraic closure** of a field k is an algebraic extension $k \subseteq \bar{k}$ such that $\bar{k}$ is algebraically closed.* ♣

Proposition 6.8

Suppose K is a field, the following are equivalent

(i) K is algebraically closed.

(ii) K has no nontrivial algebraic extensions.

(iii) If $K \subseteq L$ is any extension and $\alpha \in L$ is algebraic over K, then $\alpha \in K$. ♠

Theorem 6.1

Every field k admits an algebraic closure $k \subseteq \bar{k}$; this extension is unique up to isomorphism. ♡

Lemma 1: Let k be a field. Then there exists an extension $k \subseteq K$ such that every nonconstant polynomial $f(x) \in k[x]$ has at least one root in K.

Proof: Let $\mathcal{F}$ denotes nonconstant polynomials of $k[t]$, and define $\mathcal{T} := (t_f)_{f \in \mathcal{F}}$. Consider the polynomial ring $k[\mathcal{T}]$ in all the indeterminates t_f and the ideal I generated by all polynomials of the form $f(t_f)$. I is a proper ideal, because $1 \in I$ implies $\sum_{i=1}^{n} a_i f_i(t_{f_i})$, then the evaluation at the roots $t_{f_1} = \alpha_1, \cdots, t_{f_n} = \alpha_n$ yields $1 = \sum_{i=1}^{n} a_i f_i(\alpha_i) = 0$, which is a clear contradiction. That is, there exists a maximal ideal $\mathfrak{m} \supseteq I$, then $K := k[\mathcal{T}]/\mathfrak{m}$ is a field. Each polynomial $f \in \mathcal{F}$ has a root $t_f + \mathfrak{m}$ in K.

Lemma 2: Consider the chain of extensions $k =: K_0 \subseteq K_1 \subseteq \cdots$, where each K_{n+1} is obtained from K_n by the above construction. Let $L = \bigcup K_i$, then the field L is algebraically closed.

Proof: For all $f \in L$, $f \in K_n$ for some n, so f has a root in $K_{n+1} \subset L$. Therefore, L is algebraically closed.

Lemma 3 *(Existence of Algebraic Closure)*: Let $k \subseteq L$ be a field extension, with L algebraically closed. Let $\bar{k} := \{\alpha \in L \,|\, \alpha \text{ is algebraic over } k\}$. Then $\bar{k}$ is an algebraic closure of k.

Proof: For all $\alpha, \beta \in \bar{k}$ (algebraic number over k), since $k(\alpha, \beta)$ is a algebraic extension, $\alpha \pm \beta, \alpha\beta^{-1} \in L$ are algebraic over k thus in $\bar{k}$, so $\bar{k}$ is a field. For every root $\alpha \in L$ algebraic over $\bar{k}$, α is algebraic over k because $\bar{k}(\alpha)/\bar{k}$ and $\bar{k}/k$ are both algebraic, then $\alpha \in \bar{k}$.

Lemma 4: Let $k \subseteq L$ be a field extension, with L algebraically closed. Let $k \subseteq F$ be any algebraic extension. Then there exists a morphism of extensions $i : F \to L$.

Proof: Define a partial order on $Z := \{(K, i_K) \,|\, k \subseteq K \subseteq F,\, i_K : K \to L \text{ s.t. } i_K|_k = \mathrm{id}_k\}$ by $(K, i_K) \leq (K', i_{K'})$

if $K \subset K'$ and $i_{K'}|_K = i_K$. Every chain in Z has an upper bound $K = \bigcup K_i$ and $i_K(a) := i_{K_i}(a)$ for any i s.t. $a \in K_i$. By *Zorn's lemma*, Z admits a maximal element (G, i_G). We claim that $G = F$, otherwise F/G is an algebraic extension, so we may further extend (G, i_G), contradicting the fact that it is maximal. Hence there exists a homomorphism $i_F = i_G : F \to L$ extending the identity on k.

Lemma 5 *(Uniqueness of Algebraic Closures)*: Let $k \subseteq \bar{k}$, $k \subseteq \bar{k}'$ be two algebraic closures of k, then exists an isomorphism $\bar{k}' \to \bar{k}$ extending the identity on k.

Proof: By Lemma 4, there exists a homomorphism $i : \bar{k} \to \bar{k}'$ extending the identity on k, this map is clearly injective. i is also surjective, otherwise $\bar{k}'/\bar{k}$ is a nontrivial algebraic extension, contradicting that $\bar{k}$ is algebraically closed. Hence i is an isomorphism extending the identity on k. ■

6.3 Field Extension II

6.3.1 Splitting Field and Normality

Definition 6.7 (Splitting Field)

Let k be a field, and let $f(x) \in k[x]$ be a polynomial of degree d. The splitting field for $f(x)$ over k is an extension F of k such that $f(x) = c\prod_{i=1}^{d}(x - \alpha_i)$ in $F[x]$, and further $F = k(\alpha_1, \cdots, \alpha_d)$ is generated over k by the roots of $f(x)$ in F. ♣

Proposition 6.9 (Existence and Uniqueness of Splitting Field)

Let k be a field, and let $f(x) \in k[x]$. Then the splitting field F for $f(x)$ over k is unique up to isomorphism, and $[F : k] \leq (\deg f)!$.

In fact, if $i : k' \to k$ is any isomorphism of fields and $g(x) \in k'[x]$ is such that $f(x) = i(g(x))$, then i extends to an isomorphism of any splitting field of $g(x)$ over k' to any splitting field of $f(x)$ over k. ♠

Proof Let $\alpha \in F$ be a root of $f(x)$. Since the minimal polynomial of α is a factor of f, $[k(\alpha) : k] \leq \deg f$. By induction, we see that $[F : k(\alpha)] \leq (\deg f - 1)!$ because every other roots of $f(x)$ divides $f(x)/(x - \alpha) \in k(\alpha)[x]$, whose degree is $\deg f - 1$. Then $[F : k] = [F : k(\alpha)][k(\alpha) : k] \leq (\deg f)!$.

Suppose F, G are splitting field of $f(x) \in k[x]$, $g(x) \in k'[x]$, resp.

$$\begin{tikzcd}
k \arrow[r, hook] \arrow[d, "i"', "\sim"] & F \arrow[r, hook] \arrow[d, dashed] & \bar{k} \\
k' \arrow[r, hook] & G \arrow[ur] &
\end{tikzcd}$$

For each root α_1 of $f(x)$, let $p(x) \in k[x]$ be the minimal polynomial of α_1. For any root β_1 of $\iota(p(x))$, there is an isomorphism $k(\alpha_1) \to k'(\beta_1)$ extending ι on k by Proposition 6.2. Repeating this process, we obtain an isomorphism $F := k(\alpha_1, \cdots, \alpha_n) \to k'(\beta_1, \cdots, \beta_n) =: G$ extending ι. In particular, the splitting field is unique up to isomorphism. ■

Proposition 6.10 (Minimality of the splitting field)

Let k be a field with $f(x) \in k[x]$ and F be the splitting field for $f(x)$ over k. Suppose K/k is an extension such that $f(x)$ splits as a product of linear factors over K, then there is a homomorphism $F \to K$ extending the identity on k. ♠

Definition 6.8 (Normal Extension)

A field extension $k \subset F$ is ***normal*** *if for every irreducible polynomial $f(x) \in k[x]$, $f(x)$ has a root in F if and only if $f(x)$ splits as a product of linear factors over F.* ♣

Proposition 6.11

A field extension $k \subseteq F$ is finite and normal if and only if F is the splitting field of some polynomial $f(x) \in k[x]$.

Proof Suppose F/k is finite and normal, then F is a finitely generated $F = k(\alpha_1, \cdots, \alpha_n)$. Let $p_i(x)$ be the minimal polynomial of α_i, then F is the splitting field of $\prod_{i=1}^n p_i(x)$.

Conversely, suppose F is the splitting field of f. Let $p(x)$ be a irreducible polynomial such that a root α of it is contained in F, and let β be another root of $p(x)$. There is an isomorphism $k(\alpha) \to k(\beta)$ by Proposition 6.2. Note that F and $F(\beta)$ are splitting fields of $f(x)$ over $k(\alpha)$ and $k(\beta)$, resp, Proposition 6.9 implies an isomorphism $\tilde{\iota} : F \to F(\beta)$ extending i,

$$\begin{tikzcd}
 & k(\alpha) \arrow[r] \arrow[dd, "\sim"', "\iota"] & F \arrow[dd, dashed] \\
k \arrow[ur] \arrow[dr] & & \\
 & k(\beta) \arrow[r] & F(\beta)
\end{tikzcd}$$

Combine with the fact that $F \subseteq F(\beta)$, we see that $F = F(\beta)$, thus $\beta \in F$. Hence F contains every root of $p(x)$, thus F is normal. ■

6.3.2 Separable Polynomials and Extensions

Definition 6.9 (Separability (of polynomial))

Let k be a field. A polynomial $f(x) \in k[x]$ is ***separable*** *if it has no multiple factors over its splitting field, otherwise $f(x)$ is* ***inseparable****.*

Definition 6.10 (Formal Derivative)

Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in k[x]$ is a polynomial over k, we define its ***derivative*** *by $f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$.*

Remark The formal derivative is a purely formal operation (with no limiting process). Regardless, the expected properies od derivatives holds, in particular, $(fg)' = f'g + fg'$.

Proposition 6.12

Let k be a field, and let $f(x) \in k[x]$. Then $f(x)$ is separable if and only if $f(x)$ and $f'(x)$ are relatively prime (in $k[x]$).

Proof Proof by contraposition. For the sufficiency, assume $\gcd(f, f') \neq 1$, $f(x)$ and $f'(x)$ have a common factor $x - \alpha$ where $\alpha \in \bar{k}$. Let $f(x) = (x-\alpha)g(x)$, then $f'(x) = g(x) + (x-\alpha)g'(x)$. Since $(x-\alpha) \mid f'(x)$ by definition, we see that $(x-\alpha) \mid g(x)$, followed by $(x-\alpha)^2 \mid f(x)$ thus f is inseparable.

For the necessity, assume $f(x)$ is inseparable, namely $f(x) = (x-\alpha)^2 g(x)$ for some $\alpha \in \bar{k}$. Then $x - \alpha$ divides $f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x)$, followed by $(x-\alpha) \mid \gcd(f, f')$ thus f and f' are coprime. ■

Proposition 6.13

Let k be a field, and let $f(x) \in k[x]$ be an inseparable irreducible polynomial. Then $f'(x) = 0$. ♠

Proof By Proposition 6.12, $g(x) := \gcd(f, f') \neq 1$ is non-unit. The irreducibility of f implies $f(x) = cg(x)$ for some constant $c \in k$. Note that $g(x)$ divides $f'(x) = cg'(x)$, and $\deg g' < \deg g$, this forces $g'(x) = 0$, hence $f'(x) = 0$. ■

Definition 6.11 (Perfect Field)

*A field k is **perfect** if char $k = 0$ or if char $k > 0$ and the Frobenius homomorphism $x \mapsto x^p$ is surjective.* ♣

Lemma 6.1

Suppose k is a field of characteristic p, then $(a \pm b)^p = a^p \pm b^p$ for all $a, b \in k$. ♡

Proposition 6.14

Let k be a field. Then k is perfect if and only if all irreducible polynomials in $k[x]$ are separable. ♠

Proof We first prove the sufficiency by contradiction, assume $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ is irreducible and inseparable. Suppose char $k = 0$. Apply Proposition 6.13, $f'(x) = \sum_{i=1}^n i a_i x^{i-1} = 0$, then $ia_i = 0$ thus $a_i = 0$ for all i. Then $f(x) = 0$, contradicting that f is irreducible.

On the other hand, suppose char $k = p$ and the Frobenius homomorphism σ is surjective. Again apply Proposition 6.13, $ia_i = 0$ for all i, so $a_i = 0$ for $p \nmid i$; that is, $f(x) = \sum_{i=1}^n a_i x^{pi}$. Since σ is surjective, for each a_i $b_i \in k$ s.t. $b_i^p = a_i$. Then $f(x) = \sum_i (b_i x^i)^p = (\sum_i b_i x^i)^p$ by Lemma 6.1, contradicting that $f(x)$ is irreducible.

Conversely, we now prove the necessity. Suppose irreducible polynomials are separable, and char $k = p \neq 0$, it suffices to prove σ is surjective. Let $\alpha \in k$, consider $f(x) = x^p - \alpha$. Choose a root $\beta \in \bar{k}$, we can write $f(x) = x^p - \beta^p = (x-\beta)^p$, so $f(x)$ is inseparable. Then $f(x) = (x-\beta)^p$ is reducible by the hypothesis, and similarly $(x-\beta)^c$ $(1 < c \leq p)$ are reducible, followed by $\beta \in k$. Therefore, $\sigma(\beta) = \beta^p = \alpha$, it follows that σ is surjective. ■

Corollary 6.2

Finite fields are perfect. In particular, irreducible polynomials are separable over finite field. ♡

Definition 6.12 (Separability (of extension), Separable degree)

An algebraic extension $k \subseteq F$ is ***separable*** *if every $\alpha \in F$ is separable (i.e., the minimal polynomial of α is separable) over k. The* ***separable degree*** *of F over k, denoted by $[F : k]_s$, is defined to be the number of different homomorphisms $F \to \bar{k}$ extending the identity on k.* ♣

Proposition 6.15

A field k is perfect if and only if every algebraic extension of k is separable. ♠

Proof The statement is equivalent to Proposition 6.14.

Lemma 6.2

Let $k \subseteq k(\alpha)$ be a simple algebraic extension. Then $[k(\alpha) : k]_s$ equals the number of distinct roots in k of the minimal polynomial of α. In particular, $[k(\alpha) : k]_s \leq [k(\alpha) : k]$, with equality if and only if α is separable over k. ♡

Proof The proof is analogous to Proposition 6.3 (k-automorphism). Let $p(x)$ be the minimal polynomial of α. Each desired $\varphi : F \to \bar{k}$ maps α to a root of p since $p(\varphi(\alpha)) = \varphi(p(\alpha)) = \varphi(0) = 0$. On the other hand, each root β induces a unique $\varphi : F \to \bar{k}$ extending the identity on k and $\varphi(\alpha) = \beta$. ■

Lemma 6.3 (Multiplicative of separable degree)

Let $k \subseteq E \subseteq F$ be algebraic extensions. Then $[F : k]_s$ is finite if and only if both $[F : E]_s$, $[E : k]_s$ are finite, and in this case $[F : k]_s = [F : E]_s[E : k]_s$. ♡

Proposition 6.16

Let $k \subseteq F$ be a finite extension. Then $[F : k]_s \leq [F : k]$, and the following are equivalent:

(i) $F = k(\alpha_1, \cdots, \alpha_r)$*, where each* α_i *is separable over* k*;*

(ii) $k \subseteq F$ *is separable;*

(iii) $[F : k]_s = [F : k]$. ♠

6.4 Field Extensions III

6.4.1 Finite Field

For every finite field F of characteristic p, F may be viewed as an extension $\mathbb{F}_p \subseteq F$. Let $[F : \mathbb{F}_p] = d$, then $F \cong \mathbb{F}_p^d$ as a vector space, namely $|F| = p^d$ is a power of p.

Theorem 6.2

Let $q = p^d$ be a power of prime p. Then splitting field of the polynomial $x^q - x$ over $\mathbb{F}_p$ is a field with precisely q elements.

Conversely, let F be a field with exactly q elements, then F is a splitting field for $x^q - x$ over $\mathbb{F}_p$. ♡

Proof Let $f(x) := x^q - x$. Since $f'(x) = qx^{q-1} - 1 = -1$, then $\gcd(f, f') = 1$, followed by $f(x)$ is separable over $\mathbb{F}_p$. We claim the roots E of $f(x)$ is a field: for $\alpha, \beta \in E$, we know $\alpha^q = \alpha$ and $\beta^q = \beta$, then $0 \in E$,

$$\alpha - \beta = \alpha^q - \beta^q = (\alpha - \beta)^q \qquad \text{and} \quad \alpha\beta^{-1} = \alpha^q\beta^{-q} = (\alpha\beta^{-1})^q \text{ for } \beta \neq 0;$$

that is, E is closed under subtraction and division. Hence the splitting field of $f(x)$ contains precisely q elements.

Conversely, suppose F contains q elements. Note that $F^\times$ forms a group (under multiplication) and $|F^\times| = q - 1$, we see that $\alpha^{q-1} = 1$, i.e., $\alpha^q = \alpha$, for $\alpha \neq 0$. It is clear that $0^q = 0$, so F contains q roots of $f(x)$. Hence F is the splitting field. ■

Corollary 6.3

For every prime power q there exists one and only one finite field of order q, up to isomorphism. ♡

Proposition 6.17 (Extension of finite fields)

Let p be a prime integer, and let $0 < d \leq e$ be integers. Then there exists an extension $\mathbb{F}_{p^e}/\mathbb{F}_{p^d}$ if and only if $d \mid e$.

In the case that $d \mid e$, the extension $\mathbb{F}_{p^e}/\mathbb{F}_{p^d}$ is simple. That is, all extensions of finite fields are simple. ♠

Proposition 6.18

The factorization of $x^{q^n} - x$ in $\mathbb{F}_q[x]$ consists of all irreducible monic polynomials of degree d such that $d \mid n$. ♠

6.4.2 Separability and Simple Extensions

Proposition 6.19

An algebraic extension $k \subseteq F$ is simple if and only if the number of distinct intermediate fields $k \subseteq E \subseteq F$ is finite. ♠

Proof For sufficiency, suppose E is an intermediate field, then $F = E(\alpha)$. Let $q_k(x)$ denotes the minimal polynomial of α over k, analogously for $q_E(x)$. Note that $q_k(\alpha) = 0$ considering $q_k \in E[x]$, then $q_E(x) \mid q_k(x)$ in $E[x]$. We want to show $q_E(x)$ determines E: let $E' \subseteq E$ be the field generated by the coefficients of $q_E(x)$, then $q_E(x)$ is irreducible in $E'[x]$, so $\deg q_E = [F : E'] = [F : E][E : E'] = \deg q_E \cdot [E : E']$, followed by $[E : E'] = 1$, namely $E' = E$, as needed. Apply this claim to the fact that there is finitely-many factors of $q_k(x)$, it follows that there is finitely-many intermediate fields.

Conversely, for necessity, we may assume k is infinite (finite case follows from Proposition 6.17). Let $F = k(\alpha, \beta)$. There exists $c \neq c' \in k$ such that $k(c\alpha+\beta) = k(c'\alpha+\beta)$ because the number if intermediate field $k \subseteq k(c\alpha+\beta) \subset F$ is finite but $c \in k$ is infinite. Then

$$\alpha = \frac{(c\alpha + \beta) - (c'\alpha - \beta)}{c - c'} \in F, \text{ and also } \beta = (c\alpha - \beta) - c\alpha \in F.$$

Therefore, we see that $F = k(c\alpha + \beta)$ is simple, and the original statement follows from induction. ■

Proposition 6.20

Every finite separable extension is simple. ♠

Proof Assume $F = k(\alpha, \beta)$ with α, β separable and k infinite (Again, finite case follows from Proposition 6.17). Let I be the set of field homomorphisms $\iota : F \to \bar{k}$ extending the identity on k; fix ι and define

$$f(x) := \prod_{\iota' : \iota \neq \iota'} \left[(\iota(\alpha)x - \iota(\beta)) - \left(\iota'(\alpha)x - \iota'(\beta)\right) \right].$$

The polynomial is nonzero, because the multiplicand being zero implies $\iota(\alpha) = \iota'(\alpha)$ and $\iota(\beta) = \iota'(\beta)$, forcing $\iota = \iota'$.

Since $f(x)$ has finitely-many roots while k is infinite, there exists $c \in k$ s.t. $f(c) \neq 0$. Let $\gamma = c\alpha + \beta$. Since $f(c) \neq 0$, then $\iota(\gamma) = \iota(\alpha)c + \iota(\beta)$ are distinct for $\iota \in I$. Notice that each $\iota(\gamma)$ is a root of the minimal polynomial p_γ of γ because $p(\iota(\gamma)) = \iota(p(\gamma)) = 0$, then we see that $[F : k]_s \leq [k(\gamma) : k] \leq [F : k]$. Since $[F : k]_s = [F : k]$ because α, β are separable, $[k(\gamma) : k] = [F : k]$, so $F = k(\gamma)$. The desired statement follows immediately from induction. ■

Corollary 6.4

Let $k \subseteq F$ be a finite, separable extension. Then $|Aut_k(F)| \leq [F : k]$, with equality if and only if $k \subseteq F$ is a normal extension. ♡

6.5 Introduction to Galois Theory

6.5.1 The Galois Correspondence and Extensions

Definition 6.13 (Fixed Field)

Let $k \subseteq F$ be a field extension, and let $G \subseteq \mathrm{Aut}_k(F)$ be a group of automorphisms of the extension. The ***fixed field*** *of G is the intermediate field*

$$F^G := \{\alpha \in F \,|\, \forall\, g \in G,\ g(\alpha) = \alpha\}.$$

The notion of fixed field allows us to set up the ***Galois correspondence***

$$\{\textit{intermediate field } E:\ k \subseteq E \subseteq F\} \leftrightharpoons \{\textit{subgroups of } \mathrm{Aut}_k(F)\}.$$

♣

Proposition 6.21

The Galois correspondence is inclusion-reversing. Further, for all subgroups G of $\mathrm{Aut}_k(F)$ and all intermediate fields $k \subseteq E \subseteq F$:

- $E \subseteq F^{\mathrm{Aut}_E(F)}$;
- $G \subseteq \mathrm{Aut}_{F^G}(F)$.

Further still, denote by E_1E_2 the smallest subfield of F containing two intermediate fields E_1, E_2, and denote by $\langle G_1, G_2\rangle$ the smallest subgroup of $\mathrm{Aut}_k(F)$ containing two subgroups G_1, G_2. Then

- $\mathrm{Aut}_{E_1E_2}(F) = \mathrm{Aut}_{E_1}(F) \cap \mathrm{Aut}_{E_2}(F)$;
- $F^{\langle G_1, G_2\rangle} = F^{G_1} \cap F^{G_2}$.

♠

Example 6.4 The Galois correspondence is not necessarily bijective. Consider the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, and embed $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$. The minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2$, it contains only one root in $\mathbb{R}$, so $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))$ is a singleton. Note that there are two intermediate fields of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, so the Galois correspondence is not bijective.

Proposition 6.22

Let $k \subseteq F$ be a finite extension, and let G be a subgroup of $\mathrm{Aut}_k(F)$. Then $F^G \subseteq F$ is a finite, simple, normal, separable extension.

♠

Remark Suppose $\alpha \in F$ and $g \in G$, then $g(\alpha)$ is a root of the minimal polynomial of α, it follows that the G-orbit of α is finite, denoted $\alpha_1, \cdots, \alpha_n$. Define $q_\alpha(t) := \prod_{i=1}^n (t - \alpha_i)$. Note that for all $g \in G$, $q_\alpha(t) = \prod_{i=1}^n (t - g(\alpha_i)) = g(q_\alpha(t))$, so $q_\alpha(t) \in F^G[t]$. In particular, $q_\alpha(t)$ is separable and $\deg q_\alpha \leq |G|$.

Proof (a) Since $[F : F^G] \leq [F : k] < +\infty$, then F/F^G is finite. (b) For all $\alpha \in F$, α is a root of a separable polynomial $q_\alpha(t) \in F^G[t]$, so α separable in F, followed by F/k is separable. (c) F/k is simple because it is finite and separable. (d) Let α be the generator of F/F^G, then F is the splitting field of $q_\alpha(t)$, thus it is normal. ■

Proposition 6.23 (Surjectivity of Galois correspondence)

Let $k \subseteq F$ be a finite extension, and let $G \leq Aut_k(F)$. Then $G = Aut_{F^G}(F)$ and $|G| = [F : F^G]$. In particular, the Galois correspondence (from intermediate fields to automorphism groups) is surjective for a finite extension.

Proof Let α denotes the generator of the simple extension F/F^G, then $|\text{Aut}_{F^G}(F)|$ is the number of distinct roots of the minimal polynomial of α, so $|\text{Aut}_{F^G}(F)| \leq \deg q_\alpha \leq |G|$. We may establish the equality $G = \text{Aut}_{F^G}(F)$ by the cardinality consideration given that $G \leq \text{Aut}_k(F)$. In addition, since F/F^G is finite, separable, and normal, then $|G| = |\text{Aut}_{F^G}(F)| = [F : F^G]$. ■

Definition 6.14 (Galois extension, Galois group)

A finite extension $k \subseteq F$ is a ***Galois extension*** *if it is normal and separable.*

If $k \subseteq F$ is a ***Galois extension****, the corresponding automorphism group $Aut_k(F)$, denoted $Gal(F/k)$ or $Gal_k(F)$, is called the* ***Galois group*** *of the extension.*

Theorem 6.3 (Characterization of Galois extension)

Let F/k be a finite field extension, then the following are equivalent:

(i) F is the splitting field of a separable polynomial $f(t) \in k[t]$ over k.

(ii) F/k is Galois (i.e., normal and separable).

(iii) $|Aut_k(F)| = [F : k]$

(iv) $k = F^{Aut_k(F)}$ is the fixed field of $Aut_k(F)$.

(v) The Galois correspondence for F/k is a bijection.

(vi) F/k is separable, and if K/F is an algebraic extension and $\sigma \in Aut_k(K)$, then $\sigma(F) = F$.

Remark Suppose F/k is *not* Galois, then the equivalence between (ii) and (vi) implies that k may be embedded into F via automorphisms with different images; on the other hand, if F/k is Galois, the images must coincide and the embedding $k \subset F$ is unique.

Proposition 6.24

Any extension of finite field $\mathbb{F}_{p^e}/\mathbb{F}_{p^d}$ is a Galois extension, and $Gal(\mathbb{F}_{p^e}/\mathbb{F}_{p^d})$ is cyclic, generated by $\sigma^d : x \mapsto x^{p^d}$ where σ is the Frobenius homomorphism.

6.5.2 The Fundamental Theorems of Galois Theory

Theorem 6.4 (The fundamental theorem of Galois theory I)

Let $k \subseteq F$ be a Galois extension. The Galois correspondence is an inclusion-reversing isomorphism of the lattice of intermediate subfields of $k \subseteq F$ with the lattice of subgroups of $\mathrm{Aut}_k(F)$. ♡

Remark That is, the Galois extension F/k satisfies the following:

(1) The function

$$\{\text{intermediate field } E \mid k \subseteq E \subseteq F\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \{\text{subgroup of } \mathrm{Aut}_k(F)\}$$

defined by $\Phi := \mathrm{Aut}_{(-)}(F)$ and $\Psi := F^{(-)}$ are inclusion reversing bijections, i.e.,

- $k \subseteq E \subseteq E' \subseteq F$ implies $\mathrm{Aut}_{E'}(F) \subseteq \mathrm{Aut}_E(F)$
- $G_1 \leq G_2 \leq \mathrm{Aut}_k(F)$ implies $F^{G_2} \subseteq F^{G_1}$
- $\mathrm{Aut}_{F^G}(F) = G$ for $G \leq \mathrm{Aut}_k(F)$
- $F^{\mathrm{Aut}_E(F)} = E$ for intermediate fields $k \subseteq E \subseteq F$

(2) For every intermediate $k \subseteq E \subseteq F$, we have F/E is Galois, $[F : E] = |\mathrm{Aut}_E(F)|$, and $[E : k] = [\mathrm{Aut}_k(F) : \mathrm{Aut}_E(F)]$.

(3) If E_1, E_2 are intermediate fields and G_1, G_2 are the corresponding subgroups of $\mathrm{Aut}_k(F)$, then $\mathrm{Aut}_{E_1E_2}(F) = G_1 \cap G_2$, and $F^{\langle G_1, G_2\rangle} = E_1 \cap E_2$.

Example 6.5 Note that E/k is not necessarily Galois even if F/k is Galois. Let F be the splitting field of the minimal polynomial of $\sqrt[3]{2}$, and consider $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq F$. We see that $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois because it is not normal, whereas $F/\mathbb{Q}(\sqrt[3]{2})$ and $F/\mathbb{Q}$ are Galois.

Let F/k be a Galois extension, and let I be the set of k-homomorphisms $E \to \bar{k}$. Then

(a) For all $\iota \in I$, $\iota(E) \subseteq F$.

(b) The assignment $(g, \iota) \mapsto g \circ \iota$ defines an action of $\mathrm{Gal}(F/k)$ on I.

(c) The action is transitive.

(d) As a $\mathrm{Gal}(F/k)$-set, I is isomorphic to the set of left cosets $\mathrm{Gal}(F/k)/\mathrm{Gal}(F/E)$.

Proof (a) For all k-automorphism ι and $\alpha \in E$, ι maps α to another root of its minimal polynomial. Since F is normal, we see that $\iota(\alpha) \in F$, hence $\iota(E) \subseteq F$.

(b) We define the composition $g \circ \iota : E \to \bar{k}$ by composing ι with the restriction $g|_{\iota(E)} : \iota(E) \subseteq F \to F$ of g. Then it is not hard to verify this defines an action of $\mathrm{Gal}(F/k)$ on I.

(c) Let $\iota_1, \iota_2 \in I$. Consider $g' := \iota_2 \circ \iota_1^{-1} : \iota_1(E) \to F$. Since F is normal, g may be extended to a k-homomorphism $g : F \to F$. Then g acts on ι_1 is given by $g \circ i_1 = (\iota_2 \circ \iota_1^{-1}) \circ \iota_1 = \iota_2$. Hence the action is transitive.

(d) Given $\iota \in I$, its orbit is I and its stabilizer is given by $\mathrm{Stab}(\iota) = \mathrm{Aut}_{\iota(E)}(F)$.

Choosing $\iota = \mathrm{id}_E$, then $\mathrm{Stab}(\iota) = \mathrm{Aut}_E(F) = \mathrm{Gal}(F/E)$. Apply the orbit-stabilizer theorem, we see that $I \cong \mathrm{Gal}(F/k)/\mathrm{Gal}(F/E)$. ■

Remark The above bijection interpret the equality $[E : k] = [E : k]_s = |I| = [\mathrm{Aut}_k(F) : \mathrm{Aut}_E(F)]$ discovered using Lagrange's theorem.

Theorem 6.5 (The fundamental theorem of Galois theory II)

Let $k \subseteq F$ be a Galois extension, and let E be an intermediate field. Then $k \subseteq E$ is Galois if and only if $Aut_E(F)$ is normal in $Aut_k(F)$; in this case, there is an isomorphism $Aut_k(E) \cong Aut_k(F)/Aut_E(F)$. ♡

Proof For the sufficiency, E/k being Galois implies $g(E) = E$ for all $g \in \mathrm{Aut}_k(F)$ (Theorem 6.3 (6)). Then for $\iota \in \mathrm{Aut}_E(F)$, we see $(g^{-1}\iota g)|_E = (g^{-1}g)|_E = \mathrm{id}_E$, so $g^{-1}\iota g \in \mathrm{Aut}_E(F)$. Therefore, $\mathrm{Aut}_E(F) \trianglelefteq \mathrm{Aut}_k(F)$.

For the necessity, suppose $\mathrm{Aut}_E(F) \trianglelefteq \mathrm{Aut}_k(F)$. Note that the stabilizers $\mathrm{Stab}(\iota) = \mathrm{Aut}_{\iota(E)}(F)$ are conjugate of each other, $\mathrm{Aut}_k(F)$ being normal implies $\mathrm{Aut}_{\iota(E)}(F) = \mathrm{Aut}_E(F)$ for all ι, thus $E = \iota(E)$ since the Galois correspondence is a bijection. Again by Theorem 6.3 (6), E/k is Galois.

Furthermore, in this case, define the homomorphism $\varphi : \mathrm{Aut}_k(F) \to \mathrm{Aut}_k(E)$ by the restriction on E. φ is clearly surjective, and $\ker \varphi = \mathrm{Aut}_E(F)$. Hence by first isomorphism theorem, $\mathrm{Aut}_E(F) \trianglelefteq \mathrm{Aut}_k(F)$. ■

Proposition 6.25 (Composite Galois extensions)

Suppose $k \subseteq F$ is a Galois extension and $k \subseteq K$ is any finite extension. Then $K \subseteq KF$ is a Galois extension, and $Gal(KF/K) \cong Gal(F/(F \cap K))$. ♠

6.6 Applications of Galois Theory

6.6.1 Geometric Impossibilities

Constructions by straightedge and compass follows the following rules:

- If points A, B are construction, we can draw a line joining them (straightedge),
- If points A, B are constructed, we can draw the circle with center at A and containing B (compass), and
- We can mark any points of intersection of distinct lines, line and circle, or circle.

Given a point A and a line l, we may construct a line $l' \perp l$ passing through A. We can then construct a line $l'' \parallel l$ passing through A by repeat the above construction on l'.

Definition 6.15 (Constructible numbers)

*A real number r is **constructible** if if the point $(r, 0)$ is constructible with straightedge and compass (assuming $O = (0, 0)$ and $P = (1, 0)$); we denote the set of constructible real numbers by $\mathcal{C}_{\mathbb{R}} \subseteq \mathbb{R}$.*

*A complex number $z = x + iy$ is **constructible** if the point (x, y) is constructible by straightedge and compass; we denote the set by $\mathcal{C}_{\mathbb{C}} \subseteq \mathbb{C}$.*

Proposition 6.26

A complex number $z = x + iy \in \mathcal{C}_{\mathbb{C}}$ if and only if $x, y \in \mathcal{C}_{\mathbb{R}}$.

Proposition 6.27

The subset $\mathcal{C}_{\mathbb{R}} \subseteq \mathbb{R}$ is a subfield of $\mathbb{R}$, $\mathcal{C}_{\mathbb{C}}$ is a subfield of $\mathbb{C}$, and in fact $\mathcal{C}_{\mathbb{C}} = \mathcal{C}_{\mathbb{R}}(i)$.

Proof The set of constructible numbers are nonempty because $0, 1 \in \mathcal{C}_{\mathbb{R}}$. Suppose $p < q \in \mathcal{C}_{\mathbb{R}}$, it is not hard to show $q - p \in \mathcal{C}_{\mathbb{R}}$. Let l be the line passing through $P = (p, 0)$ and $Q = (q, 0)$. Construct a line $l' \parallel l$ through $(1, 0)$, then the intersection of l' with y-axis is given by $(p/q, 0)$. Therefore, $p/q \in \mathcal{C}_{\mathbb{R}}$. Hence $\mathcal{C}_{\mathbb{R}}$ is a field. $\mathcal{C}_{\mathbb{C}} = \mathcal{C}_{\mathbb{R}}(i)$ follows from Proposition 6.26. ■

Remark In particular, we can consider the constructible numbers as $\mathbb{Q}$-extensions: $\mathbb{Q} \subseteq \mathcal{C}_{\mathbb{R}} \subseteq \mathcal{C}_{\mathbb{C}}$.

Theorem 6.6

Let $\gamma \in \mathbb{R}$, then $\gamma \in \mathcal{C}_{\mathbb{R}}$ if and only if there exists real numbers $\delta_1, \cdots, \delta_k$ such that $\gamma \in \mathbb{Q}(\delta_1, \cdots, \delta_k)$, and $[\mathbb{Q}(\delta_1, \cdots, \delta_j) : \mathbb{Q}(\delta_1, \cdots, \delta_{j-1})] = 2$ for all j.

Proof ***Sketch***: For sufficiency, we prove the intersections of two lines, two circles, and a line and a circle can be viewed as a extension of degree ≤ 2. (i) Two non-parallel lines in F has intersection in F. (ii) Given a line and a circle in F, if they have an intersection point δ, then $\delta \in F(\sqrt{\delta})$ and $[F(\sqrt{\delta}) : F] = 2$. (iii) The intersection of two circles can be reduced to the above case. We therefore conclude the statement by viewing the construction of γ as stages of the construction of the intersection.

For necessity, note that the root of quadratic function can be constructed as the y-intercept of circle centered at some $P = (p, 0)$ through some $Q = (q, 0)$, then we may construct γ through constructing δ_i's. ■

Remark Since $\mathcal{C}_{\mathbb{C}} = \mathcal{C}_{\mathbb{R}}(i)$, the same statement holds for constructible complex numbers, including i in the list of δ_j (or simply allowing the δ_j to be complex numbers).

Corollary 6.5

Let $\gamma \in \mathcal{C}_{\mathbb{C}}$ be a constructible number, then $[\mathbb{Q}(\gamma) : \mathbb{Q}]$ is a power of 2.

6.6.2 Cyclomatic Polynomials and Fields

Definition 6.16 (Roots of unity, Cyclomatic Polynomials)

*Define the complex numbers $\zeta_n := e^{2\pi i/n}$, then $\mu_n := \{1, \zeta_n, \cdots, \zeta_n^{n-1}\}$ are roots of $x^n - 1$, we call these elements the **n-th root of unity**. We say ζ_n^m is **primitive** if it is the generator of μ_n.*

*The **cyclotomic polynomial** is defined to be*

$$\Phi_n(x) = \prod_{\zeta_n^m \text{ primitive}} (x - \zeta) = \prod_{\substack{1 \le m \le n \\ \gcd(m,n)=1}} (x - \zeta_n^m),$$

*and its degree $\phi(n) = |\{1 \le m < n \mid \gcd(n, m) = 1\}|$ is called the **Euler's totient function**.*

Example 6.6 Suppose p is a prime, then $\Phi_p(x) = (x^p - 1)/(x - 1) = x^{p-1} + \cdots + x + 1$. It is irreducible since $\Phi_p(x + 1) = x^{p-1} + \binom{p}{1} x^{p-2} + \cdots + \binom{p}{p-1}$ is irreducible by Eisenstein's criterion.

Proposition 6.28

(a) For all positive integers n, $x^n - 1 = \prod_{1 \le d \mid n} \Phi_d(x)$.

(b) The cyclotomic polynomials $\Phi_n(x)$ have integer coefficients, i.e., $\Phi_n(x) \in \mathbb{Z}[x]$.

Proof ***Sketch***: (a) $x^n - 1$ and $\prod \Phi_d(x)$ have the same roots, namely $\{1, \cdots, \zeta_n, \cdots, \zeta_n^{n-1}\}$, and they are both separable, we then conclude the equality.

(b) Proceed by strong induction on n. Let $f(x) := \prod_{1 \le d < n, d \mid n} \Phi_d(x)$, then $x^n - 1 = f(x)\Phi_n(x)$ by (a). Euclidean division over $\mathbb{Z}[x]$ gives $x^n - 1 = f(x)q(x) + r(x)$, then $f(x)(q(x) - \Phi_n(x)) = r(x)$, forcing $r(x) = 0$ and thus $\Phi_n(x) = q(x) \in \mathbb{Z}[x]$. ■

Proposition 6.29

For all $n > 0$, $\Phi_n(x) \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$.

Proof Proof by contradiction, assume $\Phi_m(x)$ is reducible in $\mathbb{Z}[x]$. Then $\Phi_n(x) = f(x)g(x)$ for some irreducible $f(x)$, then it is the minimal polynomial of some ζ_n^m. Choose $p \nmid n$ such that ζ_n^{mp} is not a root of f. Then $\Phi_n(\zeta_n^{mp}) = 0$ implies that $g(\zeta_n^{mp}) = 0$.

Consider the polynomials in modulo p, i.e., $\mathbb{F}_p[x]$. Then ζ_n^m is a root of $g(x^p) = g(x)^p$, so $f(x) \mid g(x)$ in $\mathbb{F}_p[x]$, thus $f(x)^2 \mid \Phi_n(x)$, namely $\Phi_n(x)$ is inseparable. Note that $\Phi_n(x)' = nx^{n-1} \not\equiv 0$, the cyclotomic polynomial is separable, contradiction. Hence $\Phi_n(x)$ is irreducible. ■

Definition 6.17 (Cyclotomic field)

*The splitting field $\mathbb{Q}(\xi_n)$ for the polynomial $x^n - 1$ over $\mathbb{Q}$ is the n-**th cyclotomic field**.*

Proposition 6.30

$\mathbb{Q}(\xi_n)/\mathbb{Q}$ is a Galois extension, with the Galois group Gal$(\mathbb{Q}(\xi_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Proof The extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois because it is the splitting field of $\Phi_n(x)$. Define $\sigma : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ by $\sigma(m + n\mathbb{Z}) : \zeta_n \mapsto \zeta_n^m$, then σ is an injective homomorphism. By the order consideration, note that $|\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$, σ is an isomorphism. Hence $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. ■

6.6.3 Constructibility of n-gons

Proposition 6.31 (Galois extension of degree p^r)

Let F/k be a Galois extension, and assume $[F : k] = p^r$ for some prime p and $r \geq 0$.Then there exist intermediate fields

$$k = E_0 \subseteq E_1 \subseteq E_2 \subseteq \ldots \subseteq E_r = F$$

such that $[E_i : E_{i-1}] = p$ for $i = 1, \ldots, r$.

Theorem 6.7 (Constructibility of n-gons)

The regular n-gon is constructible by straightedge and compass if and only if $\phi(n)$ is a power of 2.

Chapter 7 Homological Algebra

Introduction

- *Additive and abelian category*
- *Image and coimage*
- *Exact sequence, homology*
- *Kernel and cokernel*
- *Functors*
- *Category of cochain complexes*

7.1 Categorical Preliminaries

7.1.1 Additive Category

Definition 7.1 (Additive category)

*A category A is **additive** if:*

*(1) A has a **zero-object**, i.e., an object that is both initial and terminal,*

(2) A has both finite products and finite coproducts, and

*(3) each set of morphisms $\hom_A(A, B)$ is endowed with an abelian group structure, in such way that the composition maps are **bilinear**, i.e., $f \circ (g + g') = f \circ g + f \circ g'$ and $(f + f') \circ g = f \circ g + f' \circ g$.*

*The **zero-morphism** $0 : A \to B$ is defined by the composition of $A \to 0$ and $0 \to B$.* ♣

Remark With the notion of zero-morphism, two morphisms f, g are equal if and only if $f - g = 0$. In addition, any composition with zero-morphism yields zero-morphism, i.e., $0 \circ f = 0 = f \circ 0$.

Definition 7.2 (Kernel, Cokernel)

*Let $\varphi : A \to B$ be a morphism in an additive category A. A morphism $\iota : K \to A$ is a **kernel** of φ if $\varphi \circ \iota = 0$, and for all morphism $\alpha : Z \to A$ such that $\varphi \circ \alpha = 0$, there exists a unique $\tilde{\alpha} : Z \to K$ making the diagram commute:*

$$\begin{tikzcd}
Z \arrow[r, "\alpha"] \arrow[dr, dashed, "\tilde{\alpha}"'] & A \arrow[r, "\varphi"] & B \\
& K \arrow[u, "\iota"'] &
\end{tikzcd}$$

*A morphism $\pi : B \to C$ is a **cokernel** of φ if $\pi \circ \varphi = 0$, and for all $\beta : B \to Z$ such that $\beta \circ \varphi = 0$, there exists a unique $\tilde{\beta} : C \to Z$ making the diagram commute:*

$$\begin{tikzcd}
A \arrow[r, "\varphi"] & B \arrow[r, "\beta"] \arrow[d, "\pi"'] & Z \\
& C \arrow[ur, dashed, "\tilde{\beta}"'] &
\end{tikzcd}$$

♣

Proposition 7.1 (Characterization of mono-/epi-morphism via (co)kernels I)

A morphism $\varphi : A \to B$ in an additive category is a monomorphism if and only if for all $\alpha : Z \to A$, $\varphi \circ \alpha = 0 \Rightarrow \alpha = 0$. It is an epimorphism if and only if for all $\beta : B \to Z$, $\beta \circ \varphi = 0 \Rightarrow \beta = 0$. ♠

Proof The monomorphism part follows from the fact that $\varphi \circ \alpha = \varphi \circ \alpha' \Rightarrow \alpha = \alpha'$ is equivalent to $\varphi \circ (\alpha - \alpha') = 0 \Rightarrow \alpha - \alpha' = 0$. The epimorphism part is analogous. ■

Proposition 7.2 ((Co)kernels are (epi-/)mono-morphisms)

In any additive category, kernels are monomorphisms and cokernel are epimorphisms. ♠

Proof Suppose $\ker \varphi \circ \tilde{\alpha} = 0$. Note that $Z \to A \to B = 0$, then $0 : Z \to A$ factors through K by $0 = \ker \varphi \circ \tilde{\alpha} = \ker \varphi \circ 0$ by the definition of kernel, it follows that $\tilde{\alpha} = 0$ since the factorization is unique.

$$\begin{tikzcd}
Z \arrow[r, "0"] \arrow[dr, shift left, "\tilde{\alpha}"] \arrow[dr, dashed, shift right, "0"'] & A \arrow[r, "\varphi"] & B \\
& K \arrow[u, "\ker \varphi"'] &
\end{tikzcd}$$

The cokernel part is analogous. ■

Proposition 7.3 (Characterization of mono-/epi-morphism via (co)kernels I)

Let $\varphi : A \to B$ be a morphism in an additive category. If φ has a kernel, then φ is a monomorphism if and only if $0 \to A$ is its kernel. If φ has a cokernel, then φ is an epimorphism if and only if $A \to 0$ is its cokernel. ♠

Proof For the necessity, suppose $0_A : 0 \to A$ is the kernel of φ. Then if $\varphi \circ \alpha = 0$, α factors through 0_A, we thus conclude that $\alpha = 0$. Hence φ is a monomorphism.

Conversely, for the sufficiency, suppose φ is a monomorphism. If $\varphi \circ \alpha = 0$, then $\alpha = 0$ by Proposition 7.1. It follows that $\alpha = 0$ factors through $Z \to 0 \to A$, namely $0 \to A$ is a kernel.

The epimorphism part is analogous. ■

7.1.2 Abelian Category

Definition 7.3 (Abelian category)

An additive category $\mathcal{A}$ is abelian if:

(1) kernels and cokernels exist in $\mathcal{A}$, and

(2) every monomorphism is a kernel of some morphism, and every epimorphism is a cokernel of some morphism. ♣

Proposition 7.4

In an abelian category $\mathcal{A}$, every kernel is the kernel of its cokernel; every cokernel is the cokernel of its kernel.

Remark For the cokernel part, let π to be the cokernel of φ and ι to be the kernel of π, we want to prove $\pi = \text{coker } \iota$. Consider

$$\begin{tikzcd}
& & L \\
Z \arrow[r, "\varphi"] \arrow[d, dashed] & A \arrow[r, "\pi=\text{coker }\varphi"'] \arrow[ru, "\beta"] & B \arrow[u, dashed] \\
K \arrow[ru, "\iota=\ker \pi"'] & &
\end{tikzcd}$$

it suffices to prove that for all β s.t. $\beta \circ \iota = 0$, β factor through π.

Proposition 7.5

Let $\varphi : A \to B$ be a morphism in an abelian category $\mathcal{A}$, and assume that φ is both a monomorphism and an epimorphism. Then φ is an isomorphism.

Remark We obtain a left inverse of φ by viewing φ as the kernel of its cokernel $B \to 0$, and a right inverse is obtained by viewing φ as the cokernel of its kernel $0 \to A$.

$$\begin{tikzcd}
& & B \arrow[d, "\text{id}"] \arrow[ld, dashed] & \\
0 \arrow[r] & A \arrow[r, "\varphi"] \arrow[d, "\text{id}"'] & B \arrow[r] \arrow[ld, dashed] & 0 \\
& A & &
\end{tikzcd}$$

Proposition 7.6

In an abelian category, finite products and coproducts coincide.

7.1.3 Images and Canonical Decomposition of Morphisms

Proposition 7.7 (ker(coker φ))

Let $\varphi : A \to B$ be a morphism in an abelian category, and let $\iota : K \to B$ be the kernel of the cokernel of φ. Then

(a) ι is a monomorphism;

(b) φ factors through ι; and

(c) ι is initial with these properties.

Proof (a) follows from Proposition 7.1, and (b) follows from $\text{coker } \varphi \circ \varphi = 0$ and the definition of kernel.

(c) Let $\psi : L \to B$ satisfies the above properties, consider its cokernel $B \to \mathrm{Cok}_\psi$.

Step 1: coker ψ factors through coker φ.

Since coker $\psi \circ \psi = 0$ and φ factors through ψ, then coker $\psi \circ \varphi = 0$, followed by coker ψ factors through coker φ by the definition of cokernel.

Step 2: ι factors through ψ.

Note that coker $\psi \circ \iota = 0$ since coker $\varphi \circ \iota = 0$ and coker φ factors through coker ψ. It follows that ι factors through ψ by the definition of kernel. ■

$$\begin{tikzcd}
 & L \arrow[dr, "\psi"] & & \\
A \arrow[ur] \arrow[r] \arrow[rr, bend right, "\varphi"'] & K \arrow[u, dashed, "?"] \arrow[r, "\iota"] & B \arrow[r, "\text{coker } \varphi"] \arrow[dr, "\text{coker } \psi"'] & \mathrm{Cok}_\varphi \arrow[d, dashed] \\
 & & & \mathrm{Cok}_\psi
\end{tikzcd}$$

Remark This proposition motivates the general definition of image: every monomorphism through which φ factors must factor uniquely through im φ.

Definition 7.4 (Image, Coimage)

*Let $\varphi : A \to B$ be an abelian category. The **image** of φ is the object im $\varphi = \ker($coker $\varphi)$. The **coimage** of φ is the object coim $\varphi :=$ coker$(\ker \varphi)$ as the dual definition of image.*

Proposition 7.8 (Factorization through (co)image)

Let $\varphi : A \to B$ be a morphism in an abelian category, and let im $\varphi : K \to B$, coim $\varphi : A \to C$ be its image and coimage, respectively. Then the induced morphisms $A \to K$ and $C \to B$ are, respectively, an epimorphism and a monomorphism.

Proof Let φ factors through im φ into $\bar{\varphi} : A \to K$, and let $\bar{\varphi}$ factors through im $\bar{\varphi}$.

$$\begin{tikzcd}
A \arrow[rr, "\bar{\varphi}" description] \arrow[rrr, bend left, "\varphi"] \arrow[dr] & & K \arrow[r, tail, "\text{im } \varphi"'] & B \\
 & K' \arrow[ur, tail, "\text{im } \bar{\varphi}"] \arrow[urr, tail, dotted] & &
\end{tikzcd}$$

Note that $K' \to B$ is a monomorphism through which φ factors, and $K' \to B$ is preceding the initial morphism im φ, then im φ is an isomorphism. In particular, the cokernel coker im $\bar{\varphi}$ = coker $\bar{\varphi} = 0$, followed by $\bar{\varphi}$ is an epimorphism. ■

Theorem 7.1 (Canonical decomposition in abelian categories)

Every morphism $\varphi : A \to B$ in an abelian category $\mathcal{A}$ may be decomposed as

$$\varphi : \quad A \xrightarrow[\textit{coim}\,\varphi]{} C \xrightarrow{\sim} K \xrightarrow[\textit{im}\,\varphi]{} B$$

where $A \to C$ *is coker* $(\ker\varphi) =$ *coim* φ *and* $K \to B$ *is* $\ker($*coker* $\varphi) =$ *im* φ*. The induced morphism* $\tilde{\varphi} : C \to K$ *is uniquely determined and is an isomorphism.* ♡

Proof There exists a unique homomorphism $\psi : K \to C$ making the diagram commute by the universal property im φ.

$$\begin{tikzcd}
 & K \arrow[rd, bend left, tail, "\operatorname{im}\varphi"] \arrow[dd, dashed] & \\
A \arrow[ru, bend left, two heads, "\bar{\varphi}"] \arrow[rr, "\varphi"] \arrow[rd, bend right, two heads, "\operatorname{coim}\varphi"'] & & B \\
 & C \arrow[ru, bend right, tail, two heads, "\underline{\varphi}"'] &
\end{tikzcd}$$

Since $\psi \circ \bar{\varphi}$ is an epimorphism, so does ψ; similarly, since $\underline{\varphi} \circ \psi$ is a monomorphism, so does ψ. Therefore ψ is an isomorphism, taking $\varphi^{-1} : C \to K$ suffices. ■

7.2 Functors

Definition 7.5 (Functor)

Let $\mathcal{C}, \mathcal{D}$ be two categories. A ***(covariant) functor*** $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ *consists of*

(1) an assignment $(A \in \mathcal{C}) \to (F(A) \in \mathcal{D})$,

(2) a function $\mathcal{F}_{A,B} : \hom_{\mathcal{C}}(A, B) \to \hom_{\mathcal{D}}(\mathcal{F}(A), \mathcal{F}(B))$ for every pair of objects $A, B \in \mathcal{C}$ (we may write $\mathcal{F} : \mathcal{F}_{A,B}$ for simplicity), where the function $\mathcal{F}$

(i) preserves identities: $\mathcal{F}(id_A) = id_{F(A)}$ for all $A \in \mathcal{C}$, and

(ii) preserves composition: $\mathcal{F}(\beta \circ \alpha) = \mathcal{F}(\beta) \circ \mathcal{F}(\alpha)$ for all $A, B \in \mathcal{C}$, $\alpha : A \to B$, and $\beta : B \to C$.

A ***contravariant functor*** $\mathcal{G} : \mathcal{C} \to \mathcal{D}$ *is a covariant functor $\mathcal{C}^{op} \to \mathcal{D}$.* ♣

Remark For a contravariant functor $\mathcal{G} : \mathcal{C} \to \mathcal{D}$, (ii) is equivalent to $\mathcal{G}(\beta \circ_{\mathcal{C}} \alpha) = \mathcal{G}(\alpha) \circ_{\mathcal{D}} \mathcal{G}(\beta)$.

Example 7.1 Example of basic functors include:

- ***Forgetful functor***: $U : \textsc{Grp} \to \textsc{Set}$ defined by (1) U assigns each group to its underlying set, and (2) U map each group homomorphism to its underlying set-function.
- ***Free group***: $F : \textsc{Set} \to \textsc{Grp}$ defined by (1) $U : X \mapsto F(X)$ where $F(X)$ is the free group on the set X, and (2) U maps $\alpha : A \to B$ to the group homomorphism $F(A) \to F(B)$ induced by $\tilde{\alpha} : A \to B \subseteq F(B)$ by the universal property of free group.
- ***Group of units***: $(-)^{\times} : \textsc{Ring} \to \textsc{Grp}$ defined by (1) $(-)^{\times} : R \to R^{\times}$ assigning each ring to its group of units, and (2) maps each $\alpha : A \to B$ to the group homomorphism $\alpha|_{R^{\times}}$, i.e., the restriction of α on the group of units.

Example 7.2 For a category $\mathcal{C}$ and an object $X \in \mathcal{C}$, the **covariant Yoneda** functor $\mathcal{F}^X = \hom_{\mathcal{C}}(X, -) : \mathcal{C} \to \textsc{Set}$ is defined as:

(1) For each $A \in \mathcal{C}$, assign $\mathcal{F} : A \mapsto \hom_{\mathcal{C}}(X, A)$.

(2) For each $\alpha \in \hom_{\mathcal{C}}(A, B)$, map $\mathcal{F} : \alpha \mapsto \alpha^*$, where $\alpha^* : \hom_{\mathcal{C}}(X, A) \to \hom_{\mathcal{C}}(X, B)$ is defined by $\alpha^*(f) = \alpha \circ f$.

Analogously, we may define the ***contravariant Yoneda*** $\mathcal{F}_X =: \mathcal{C}^{op} \to \textsc{Set}$ assigning $A \mapsto \hom_{\mathcal{C}}(A, X)$.

Example 7.3 The ***Galois groups functor*** $\mathcal{F} = \mathrm{Gal}(-/k) : (\textsc{GalExt}_k)^{op} \to \textsc{Grp}$ is defined as

(1) For each $E \in (\textsc{GalExt}_k)^{op}$, assign $\mathcal{F} : E \mapsto \mathrm{Gal}(E/k)$.

(2) For each $\alpha \in \hom_{(\textsc{GalExt}_k)^{op}}(F, E) = \hom_{\textsc{GalExt}_k}(E, F)$, namely a (Galois) extension F/E, define $\mathcal{F}(\alpha)$ by the canonical map $\mathrm{Gal}(F/k) \to \mathrm{Gal}(E/k)$ obtained by restriction.

7.3 Complexes and Homology

7.3.1 Exactness in Abelian Category

Definition 7.6 (Exactness)

Let $\mathcal{A}$ be an abelian category. Given a sequence of objects and morphisms in $\mathcal{A}$,

$$\cdots \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \longrightarrow \cdots$$

*the sequence is **exact** at B if*

(1) $\psi \circ \varphi = 0$

(2) *coker*$(\varphi) \circ \ker(\psi) = 0$ ♣

Proposition 7.9 (Equivalent definition of exactness)

A sequence $\cdots A \xrightarrow{\varphi} B \xrightarrow{\psi} C \longrightarrow \cdots$ is exact at B if and only if im$(\varphi) = \ker(\psi)$. ♠

Remark That is, the above sequence is exact at B if and only if ψ and coker(φ) (both of which are morphisms with B as source) have the same kernel, if and only if φ and $\ker(\psi)$ (both of which are morphisms with B as target) have the same cokernel.

Proposition 7.10 (Exactness and mono-/epi-morphisms)

Let a sequence be given as above that is exact B. Then ψ is a monomorphism if and only if $\varphi = 0$, and φ is an epimorphism if and only if $\psi = 0$. ♠

Proposition 7.11 (Exact sequences and $\hom_{\mathcal{A}}(Z, -)$)

Let $\varphi \colon A \to B$ be a morphism in an additive category $\mathcal{A}$. Then $\iota \colon K \to A$ is a kernel for φ if and only if for all objects Z the induced sequence

$$0 \longrightarrow \hom_{\mathscr{A}}(Z, K) \xrightarrow{\iota_*} \hom_{\mathscr{A}}(Z, A) \xrightarrow{\varphi_*} \hom_{\mathscr{A}}(Z, B)$$

is exact, where $\iota_*(f) := \iota \circ f$ and $\varphi_*(g) := \varphi \circ g$. The result is analogous for cokernels. ♠

7.3.2 Complex and Homology

Proposition 7.12

In an abelian category, consider the sequence $A \xrightarrow{f} B \xrightarrow{g} C$. Then $g \circ f = 0$ if and only if im f factors through $\ker g$.

Proof For the sufficiency, if $g \circ f = 0$, then f factors through the monomorphism $\ker g$, so does im f by the universal property of image. For the necessity, if im f factors through $\ker g$, so does f, namely $f = \ker g \circ \tilde{f}$ for some $\tilde{f}$, then $g \circ f = g \circ \ker g \circ \tilde{f} = 0$. ■

Definition 7.7 (Complex)

*A **cochain complex** $M^\bullet = (M^\bullet, \mathrm{d}^\bullet)$ in an abelian category $\mathcal{A}$ is a sequence of morphisms*

$$\cdots \xrightarrow{d^{i-2}} M^{i-1} \xrightarrow{d^{i-1}} M^i \xrightarrow{d^i} M^{i+1} \xrightarrow{d^{i+1}} \cdots$$

*such that $\mathrm{d}^i \circ \mathrm{d}^{i-1} = 0$ for all $i \in \mathbb{Z}$. We call $\mathrm{d}^\bullet$ the **differentials** of the complex. We say $M^\bullet$ is **exact at i** if* im $\mathrm{d}^{i-1} = \ker \mathrm{d}^i$*, and we call $M^\bullet$ is **exact** if it is exact at all $i \in \mathbb{Z}$.*

Remark The motivation of *cohomology groups* of a cochain complex $(M^\bullet, d^\bullet)$ is a "measure its deviation of exactness": $H^i(M^\bullet) := \ker d^i/\text{im } d^{i-1}$.

In the general abelian category, note that im d^{i-1} factors through $\ker d^i$,

$$\begin{tikzcd}
M^{i-1} \arrow[r, "d^{i-1}"] \arrow[d] & M^i \arrow[r, "d^i"] & M^{i+1} \\
I \arrow[ur, tail, "\text{im } d^{i-1}"] \arrow[r, tail, dashed, "\sigma"'] & K \arrow[u, tail, "\ker d^i"'] &
\end{tikzcd}$$

this give rise to a unique monomorphism $\sigma : I \to K$. We may identity the ***i*-th cohomology** $H^i(M^\bullet) := \text{coker } \sigma$ (and we use quotient notation as a shorthand).

7.3.3 Category of Cochain Complexes

Definition 7.8 (Category of Cochain Complexes)

Let $\mathcal{A}$ be an abelian category, we define the category of cochain complexes $\mathcal{C}(\mathcal{A})$ by

- *The objects are cochain complexes $(M^\bullet, \mathrm{d}_M^\bullet)$ in $\mathcal{A}$*
- *The morphisms $\alpha : (M^\bullet, \mathrm{d}_M^\bullet) \to (N^\bullet, \mathrm{d}_N^\bullet)$ are given by families of morphisms $(\alpha^i : M^i \to N^i)_{i\in\mathbb{Z}}$ such that all diagrams of the following form commute:*

$$\begin{tikzcd}
\cdots \arrow[r] & M^{i-1} \arrow[r, "d_M^{i-1}"] \arrow[d, "\alpha^{i-1}"'] & M^i \arrow[r, "d_M^i"] \arrow[d, "\alpha^i"'] & M^{i+1} \arrow[r] \arrow[d, "\alpha^{i+1}"'] & \cdots \\
\cdots \arrow[r] & N^{i-1} \arrow[r, "d_N^{i-1}"'] & N^i \arrow[r, "d_N^i"'] & N^{i+1} \arrow[r] & \cdots
\end{tikzcd}$$

Proposition 7.13

If $\mathcal{A}$ is an abelian category, then $\mathcal{C}(A)$ is also an abelian category.

Definition 7.9 (Additive functor)

*Let $F : \mathcal{C} \to \mathcal{D}$ be a functor between additive categories. We call F **additive** if for all $A, B \in \mathcal{C}$, the induced map $F_{A,B} : \hom_{\mathcal{C}}(A, B) \to \hom_{\mathcal{D}}(F(A), F(B))$ is a group homomorphism.*

Proposition 7.14 (Homology as a functor)

For any fixed $i \in \mathbb{Z}$, the assignment $(M^\bullet, d^\bullet) \mapsto H^i(M^\bullet, d^\bullet)$ defines an additive covariant functor $\mathcal{C}(\mathcal{A}) \to \mathcal{A}$.

Remark We can also view cohomology as a functor $\mathcal{C}(\mathcal{A}) \to \mathcal{C}(\mathcal{A})$, by placing each cohomology object $H^i(M^\bullet)$ in degree i, connected by zero-morphisms, obtaining a complex $H^\bullet(M^\bullet)$.

Proposition 7.15 (Connecting homomorphism in degree 0)

Consider the short exact sequences $(L^\bullet, \lambda)$, $(M^\bullet, \mu)$, $(N^\bullet, \nu)$. Assume there exists a short exact sequence in $\mathcal{C}(\mathcal{A})$ given by $0 \longrightarrow L^\bullet \longrightarrow M^\bullet \longrightarrow N^\bullet \longrightarrow 0$. Then there exists an exact sequence in $\mathcal{A}$ as follows

$$\begin{tikzcd}
0 \arrow[r] & H^0(L^\bullet) \arrow[r] & H^0(M^\bullet) \arrow[r] & H^0(N^\bullet) \arrow[dll, "\delta"] & \\
 & H^1(L^\bullet) \arrow[r] & H^1(M^\bullet) \arrow[r] & H^1(N^\bullet) \arrow[r] & 0
\end{tikzcd}$$

Proof Sketch: By the **Freyd-Mitchell embedding theorem**, any abelian category can be identified with a full subcategory of R-Mod for some ring R. Then we may apply the snake lemma (Proposition 4.14).