Algebra Lecture Notes

Liming Pang

This lecture notes is for the one-semester undergraduate Algebra course that I taught at New York University.

Part of the content in the lecture notes is based on the textbook that we use in this course (Michael Artin, Algebra, 2nd Edition, Pearson, 2010)

Contents

In this course, we are going to learn something new: Abstract Algebra. We are going to study the two abstract concepts: groups and rings. They are defined in an abstract and theoretical fashion, but their applications can be found in many different occasions. Similar to the course of Analysis, Algebra requires rigorous proofs, and it is one of the most important tools and languages for modern mathematics.

Here are some concrete suggestions:

1. Writing proofs in mathematics is a serious task. Every step should be logically correct. One small mistake may make the entire argument invalid.

2. When meeting with a new definition, think about the motivations and keep in mind some examples. Examples may help in understanding concepts and coming up with proofs. However, when formal proofs are written down, you should stick to the abstract definitions. An argument by showing an example is not a sufficient proof logically.

3. When learning a theorem, do not just memorise the result. Understanding the reason why it is true is more important. You should make sure that you can follow all the details of proofs. Trying to understand proofs formulated by others can also help in improving your ability of providing proofs.

4. In order to obtain a better understanding of the course material, you will need to do practice problems. The homework provides a minimum amount of exercises that you need. Besides homework, you should also spend some time on the exercises in the textbook. For any homework problem or other exercise that you have no idea how to solve, at least try to think about it for an hour before asking others for hints or help. It is the thinking process that makes the progress. By concentrating and thinking hard, you will need to recall everything you have learned, which is a good opportunity for review. And this kind of active thinking can also help you relate different topics together to gain deeper understanding of the concepts that you have learned.

1 Elementary Set Theory

1.1 Functions

Definition 1.1.1. Given two sets X and Y, a **function** (or a **map**) $f : X \longrightarrow Y$ (from X to Y) is a subset S_f of the set $X \times Y$ such that for any $x \in X$, there exists a unique $y \in Y$ such that $(x, y) \in S_f$. If $f : X \longrightarrow Y$ is a function and $(x, y) \in S_f$, we usually write $y = f(x)$. X is called the **domain** of f, Y is called the **codomain** of f. The set $\{y \in Y | y = f(x) \text{ for some } x \in X\}$ is called the **range** or **image** of f. If $y \in Y$, the set $f^{-1}(y) = \{x \in X | y = f(x)\}$ is called the **preimage** of y.

Definition 1.1.2. Given two functions $f : X \longrightarrow Y$ and $g : Y \longrightarrow Z$, their **composition function** $g \circ f$ is the function:

$S_{g \circ f} = \{(x, z) \in X \times Z | \exists y \in Y \text{ such that } (x, y) \in S_f \text{ and } (y, z) \in S_g\}$.

Note the above definition indicates $y = f(x)$ and $z = g(y)$, so we can write $z = g \circ f(x) = g(f(x))$.

Definition 1.1.3. A function $f : X \longrightarrow Y$ is **injective** if $f(x_1) = f(x_2)$ in Y implies $x_1 = x_2$ in X. Equivalently, f is injective if $x_1 \neq x_2$ in X implies $f(x_1) \neq f(x_2)$ in Y. When f is injective, we also say it is **one-to-one**.

Definition 1.1.4. A function $f : X \longrightarrow Y$ is **surjective** if for any $y \in Y$, there exists $x \in X$ such that $y = f(x)$. In other words, f is surjective if the range of f equals to Y. When f is surjective, we also say it is **onto**.

Definition 1.1.5. A function is **bijective** if it is both injective and surjective.

Example 1.1.6. *$f : \mathbb{Z} \longrightarrow \mathbb{N}$ defined by $f(x) = x^2$ is not injective, since $f(n) = f(-n)$ for any $n \in \mathbb{Z}$. It is not surjective since $y \in \mathbb{N}$ has no preimage if it is not a perfect square.*

Example 1.1.7. *$f : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $f(x) = 2x$ is injective, since $f(x_1) = f(x_2)$ means $2x_1 = 2x_2$, which implies $x_1 = x_2$. It is not surjective since the range is the set of even numbers, not the entire set of integers.*

Example 1.1.8. *$f : \mathbb{R} \longrightarrow \mathbb{R}$ defined by $f(x) = 2x$ is injective, since $f(x_1) = f(x_2)$ means $2x_1 = 2x_2$, which implies $x_1 = x_2$. It is surjective since for any $y \in \mathbb{R}$, $y = f(\frac{y}{2})$. We conclude f is bijective.*

Definition 1.1.9. If X is a set, define the **identity function** on X to be

$$X \xrightarrow{id_X} X$$

$$x \mapsto x$$

Definition 1.1.10. $g : Y \longrightarrow X$ is the **inverse function** of $f : X \longrightarrow Y$ if $f \circ g = id_Y$ and $g \circ f = id_X$. If f has inverse function, we say f is **invertible**.

Exercise 1.1.11. *Prove the inverse function of $f : X \longrightarrow Y$ is unique if it exists.*

It turns out that we can make use of the inverse functions to check if a given function is bijective.

Lemma 1.1.12. *If $f : X \longrightarrow Y$ and $g : Y \longrightarrow X$ are functions, and $g \circ f = id_X$, then f is injective and g is surjective.*

Proof. If $f(x_1) = f(x_2)$, $g \circ f(x_1) = g \circ f(x_2)$. By assumption, this means $id_X(x_1) = id_X(x_2)$, i.e. $x_1 = x_2$, so f is injective.

For any $x \in X$, $x = id_X(x) = g \circ f(x) = g(f(x))$, so g is surjective. □

Proposition 1.1.13. *$f : X \longrightarrow Y$ is invertible if and only if f is bijective.*

Proof. If $f : X \longrightarrow Y$ has inverse function $g : Y \longrightarrow X$, then by the above lemma,

$$\begin{cases} f \circ g = id_Y \Longrightarrow f \text{ is surjective} \\ g \circ f = id_X \Longrightarrow f \text{ is injective} \end{cases}$$

we conclude f is bijective.

Conversely, if f is bijective, for each $y \in Y$, there is a unique $x \in X$ (surjectivity implies existence, and injectivity implies the uniqueness) such that $f(x) = y$, and we define the function $g(y) = x$. g is the inverse function of f since $g \circ f(x) = g(y) = x$ and $f \circ g(y) = f(x) = y$. □

Remark 1.1.14. The inverse function of f, if exists, is often denoted by f^{-1}.

Example 1.1.15. *$f : \mathbb{R} \longrightarrow \mathbb{R}$ defined by $f(x) = 2x$ is bijective since it has inverse function $f^{-1}(x) = \frac{x}{2}$.*

1.2 Mathematical Induction

One powerful tool for proofs is the mathematical induction. It is applied when we would like to prove some statement $S(n)$ that is true for the set $\{n \in \mathbb{N} | n \geq a\}$, where $a \in \mathbb{N}$ is a constant.

There are two steps for **mathematical induction**.

Step 1. Prove $S(a)$ is true.

Step 2. Based on the hypothesis that $S(k)$ $(k \geq a)$ is true, prove $S(k+1)$ is true.

Example 1.2.1. *Show that* 8 *divides* $3^{2n} - 1$ *for all* $n \in \mathbb{N}$.

1. *When* $n = 0$, $3^{2\times 0} - 1 = 0$, *which is divisible by* 8.
2. *Assume* $3^{2k} - 1$ *is divisible by* 8. *Then for* $n = k + 1$,

$$3^{2(k+1)} - 1 = 9 \times 3^{2k} - 1 = 8 \times 3^{2k} + (3^{2k} - 1)$$

which is divisible by 8.

We therefore conclude the statement is true for all natural numbers.

Sometimes, mathematical induction is not strong enough to prove some statements of the form $S(n)$. We may try to use the **strong induction** instead, which is described as below:

Step 1. Show that $S(a), S(a+1), ..., S(b)$ are true for some choice of $b \geq a$

Step 2. Based on the hypothesis that $S(n)$ is true for all $a \leq n \leq k$ $(k \geq b)$, show that $S(k+1)$ is true.

Example 1.2.2. *The Fibonacci Numbers* F_n $(n \geq 0)$ *are defined by:*

$$\begin{cases} F_0 = 0 \\ F_1 = 1 \\ F_n = F_{n-1} + F_{n-2} \end{cases}$$

Show that if $\phi = \frac{1+\sqrt{5}}{2}$, *then* $F_n \geq \phi^{n-2}$ *for all* $n \geq 2$. *Note that* ϕ *is the Golden Ratio which satisfies* $\phi^2 = \phi + 1$.

1. *When* $n = 2$, $F_2 = F_1 + F_0 = 1$ *and* $\phi^{2-2} = 1$, *so* $F_2 \geq \phi^{2-2}$ *is true. When* $n = 3$, $F_3 = F_2 + F_1 = 2$, $\phi^{3-2} = \frac{1+\sqrt{5}}{2} < 2$, *so* $F_3 \geq \phi^{3-1}$ *is true.*

2. Suppose $F_n \geq \phi^{n-2}$ is true for all $2 \leq n \leq k$, $(k \geq 3)$. Then for $n = k + 1$:

$$F_{k+1} = F_k + F_{k-1} \geq \phi^{k-2} + \phi^{k-3} = \phi^{k-3}(\phi + 1) = \phi^{k-3}\phi^2 = \phi^{(k+1)-2}$$

We therefore conclude the statement is true for all $n \geq 2$.

1.3 Equivalence Relations

Definition 1.3.1. A **relation** on a set S is a subset $R \subseteq S \times S$, that is, a subset of the ordered pairs of elements in S.

Definition 1.3.2. A relation R on S is called an **equivalence relation** if it satisfies:

1. (Reflexive) $x \in S \Longrightarrow (x, x) \in R$
2. (Symmetric) $(x, y) \in R \Longrightarrow (y, x) \in R$
3. (transitive) $(x, y) \in R, (y, z) \in R \Longrightarrow (x, z) \in R$

Notation 1.3.3. *When a relation is an equivalent relation, we usually write $x \sim_R y$ if $(x, y) \in R$. If the relation R is clear from context, we can omit the letter R and just write $x \sim y$.*

Example 1.3.4. *On the set of integers $\mathbb{Z}$, define $x \sim y$ if $x - y \in 2\mathbb{Z}$. This is an equivalence relation:*

1. *$\forall k \in \mathbb{Z}$, $k - k = 0 \in 2\mathbb{Z}$, so $k \sim k$.*
2. *If $k \sim l$, $k - l \in 2\mathbb{Z}$, $l - k \in 2\mathbb{Z}$, so $l \sim k$.*
3. *If $k \sim l$ and $l \sim m$, $k - l \in 2\mathbb{Z}$ and $l - m \in 2\mathbb{Z}$, then $k - m = (k - l) + (l - m) \in 2\mathbb{Z}$, so $k \sim m$.*

Example 1.3.5. *$X = \{f : [0, 1] \longrightarrow \mathbb{R} | f$ is integrable$\}$. Define $f_1 \sim f_2$ if*

$$\int_0^1 |f_1 - f_2| \, dx = 0$$

This is an equivalence relation:

1. *$\forall f \in X$, $\int_0^1 |f - f| \, dx = \int_0^1 0 \, dx = 0$, so $f \sim f$*

2. *If* $f_1 \sim f_2$, $\int_0^1 |f_1 - f_2|\, dx = 0$, *then* $\int_0^1 |f_2 - f_1|\, dx = 0$, *so* $f_2 \sim f_1$.

3. *If* $f_1 \sim f_2$ *and* $f_2 \sim f_3$, $\int_0^1 |f_1 - f_2|\, dx = 0$ *and* $\int_0^1 |f_2 - f_3|\, dx = 0$, *then* $0 \leq \int_0^1 |f_1 - f_3|\, dx \leq \int_0^1 |f_1 - f_2|\, dx + \int_0^1 |f_2 - f_3|\, dx = 0$, *this implies* $\int_0^1 |f_1 - f_3|\, dx = 0$, *so* $f_1 \sim f_3$.

Definition 1.3.6. Given an equivalence relation on a set S, define the **equivalence class** of $a \in S$ to be the subset

$$[a] = \{b \in S | a \sim b\}$$

Proposition 1.3.7. *Given an equivalence relation on a set* S, *for any* $a, b \in S$, *either* $[a] = [b]$ *or* $[a] \cap [b] = \emptyset$

Proof. Suppose $[a] \cap [b] \neq \emptyset$. Then $\exists x \in [a] \cap [b]$, which implies $a \sim x$ and $b \sim x$.

For any $y \in [a]$, $a \sim y$, and the relation is an equivalence relations, so

$$y \sim a \sim x \sim b$$

we get $y \in [b]$, so $[a] \subseteq [b]$. Similarly, we can also prove $[b] \subseteq [a]$, so $[a] = [b]$. □

Definition 1.3.8. A **partition** of a set S is a subdivision of S into non-overlapping and nonempty subsets S_i:

$$S = \sqcup_{i \in I} S_i$$

where I is some index.

Example 1.3.9. *We can make a partition of* $\mathbb{Z}$ *into the set of odd numbers and the set of even numbers.*

Proposition 1.3.10. *The equivalence classes of an equivalence relation on* S *give a partition of* S, *and conversely, a partition of* S *defines an equivalence relation on* S.

Proof. We have just proved that different equivalence classes are disjoint, and their union will be S since for any $x \in S$, $x \in [x]$. S is the disjoint union of all the equivalence classes.

Conversely, if there is a partition on S, we can define $a \sim b$ if a lies in the same part of the partition as b, and it is not hard to check this is an equivalence relation.

□

Definition 1.3.11. S is a set with an equivalence relation defined on it. Let $\bar{S}$ be the set of all the equivalnece classes. $\bar{S}$ is called the **quotient space** of S by the equivalence relation. There is a map

$$S \xrightarrow{\pi} \bar{S}$$

$$x \mapsto [x]$$

called the **quotient map** or **projection map**.

Notation 1.3.12. *Sometimes we also denote an equivalence class $[x]$ by C_x or $\bar{x}$.*

Example 1.3.13. *Recall that we have defined an equivalence relation on $\mathbb{Z}$ that $x \sim y$ if $x-y \in 2\mathbb{Z}$, i.e., $x-y$ is even. There are two distinct equivalence classes, $\bar{0}$ and $\bar{1}$. $\bar{0}$ is the set of all even numbers and $\bar{1}$ is the set of all odd numbers.*

Example 1.3.14. *More generally, for any natural number $n \geq 2$, there is an equivalence relation $x \sim y$ if n divides $y - x$. The equivalence classes are called* ***congruence classes of integers modulo*** **n**. *It turns out that there is a natural group structure on this quotient space induced from that of the group of integers, and we will explore the details later when we discuss the concept of quotient groups.*

2 Groups and Functions between Groups

2.1 Groups

Definition 2.1.1. A **group** is a nonempty set G with a law of composition

$$G \times G \longrightarrow G$$

$$(g_1, g_2) \mapsto g_1 g_2$$

satisfying:

1. The composition is **associative**:

$$\forall g_1, g_2, g_3 \in G, (g_1 g_2) g_3 = g_1 (g_2 g_3)$$

2. G contains an **identity element** 1, such that

$$\forall g \in G, g1 = 1g = g$$

3. Every element in G has an **inverse**:

$$\forall g \in G, \exists g^{-1} \in G \Longrightarrow g g^{-1} = g^{-1} g = 1$$

Definition 2.1.2. If the law of composition for a group G is **commutative**, i.e.

$$\forall g_1, g_2 \in G, g_1 g_2 = g_2 g_1$$

then G is called an **abelian group**.

Remark 2.1.3.

1. Given a pair of elements $(g_1, g_2) \in G \times G$ in a group G, the element obtained by applying the law of composition to (g_1, g_2) is usually denoted as $g_1 g_2, g_1.g_2$ or $g_1 \circ g_2$. If the group is abelian, it can also be written as $g_1 + g_2$.

2. It is also common to use the letter e to denote the identity element. If the composition is written as $g_1 + g_2$ in an abelian group, then the identity element is usually denoted by 0.

3. The definition of a group consists of the information of both the underlying set and the law of composition. When a group is given, it is law of composition is already determined. There may be more than one group structures on a given set by assigning different laws of compositions.

Example 2.1.4. *The set of integers $\mathbb{Z}$ with the law of composition to be addition of numbers form a group, denoted as $\mathbb{Z}^+$. We can check this is indeed a group:*

1. *The addition of integers is associative:*

$$(n_1 + n_2) + n_3 = n_1 + (n_2 + n_3)$$

2. *The integer 0 is the identity element:*

$$\forall n \in \mathbb{Z}, n + 0 = 0 + n = n$$

3. *Every integer has an inverse:*

$$\forall n \in \mathbb{Z}, n + (-n) = (-n) + n = 0$$

Example 2.1.5. *The set of nonzero rational numbers with the law of composition to be multiplication of numbers form a group $\mathbb{Q}^\times$:*

1. *Multiplication of rational numbers is associative:*

$$(q_1 q_2)q_3 = q_1(q_2 q_3)$$

2. *The identity element is the rational number 1:*

$$\forall q \in \mathbb{Q}^\times, q.1 = 1.q = q$$

3. *Every nonzero rational number has multiplicative inverse:*

$$\forall q \in \mathbb{Q}^\times, q.\frac{1}{q} = \frac{1}{q}.q = 1$$

Example 2.1.6. *The set of all real $n \times n$ invertible matrices with the law of composition to be matrix multiplication form a group $GL_n(\mathbb{R})$, called the* ***general linear group****:*

1. *Matrix multiplication is associative:*

$$(AB)C = A(BC)$$

2. *The identity element is the identity $n \times n$ matrix I_n:*

$$\forall A \in GL_n(\mathbb{R}), AI_n = I_n A = A$$

3. *The inverse of $A \in GL_n(\mathbb{R})$ is its matrix inverse A^{-1}:*

$$AA^{-1} = A^{-1}A = I_n$$

Example 2.1.7. *Let $X_n = \{1, 2, 3, ..., n\}$ be a set of n elements. The set of all bijections of X_n to itself with the law of composition the composition of functions form a group S_n, called the* ***permutation group*** *of n letters:*

1. *Composition of functions is associative*

2. *The identity element is the identity function on X:*

$$\forall f \in S_n, f \circ id_X = id_X \circ f = f$$

3. *The inverse of $f \in S_n$ is its inverse function f^{-1}:*

$$f \circ f^{-1} = f^{-1} \circ f = id_X$$

We will introduce a more convenient notation for the elements of S_n in the next section. before that we will first explore some general properties for groups.

Proposition 2.1.8. *A group G admits the* ***Cancellation Law****:*

$$ac = bc \Longrightarrow a = b$$

Proof. Multiplying c^{-1} on both sides of $ac = bc$:

$$\begin{aligned} (ac)c^{-1} &= (bc)c^{-1} \\ a(cc^{-1}) &= b(cc^{-1}) \\ a1 &= b1 \\ a &= b \end{aligned}$$

□

Proposition 2.1.9. *The identity element in a group G is unique.*

Proof. Assume 1 and $1'$ are both identity elements of a group G. Then

$$1 = 1.1' = 1'$$

□

Definition 2.1.10. The **order** of a group G is the number of elements in its underlying set, and is denoted by $|G|$. If $|G| < \infty$, we say G is a **finite group**; otherwise we say it is an **infinite group**.

Notation 2.1.11. *g is an element in a group G. Then we write $g^0 = 1$, $g^1 = g$, and write g^{-1} for the inverse of g.*

If k is a positive integer, $g^k = \underbrace{g...g}_{k \text{ copies}}$ and $g^{-k} = \underbrace{g^{-1}...g^{-1}}_{k \text{ copies}}$

Definition 2.1.12. If G is a finite group, we can use a table of following form to represent its law of composition, which is called the **multiplication table** for G

	1	a	b	c	d	...
1	1	a	b	c	d	
a	a	a^2	ab	ac	ad	
b	b	ba	b^2	bc	bd	
c	c	ca	cb	c^2	cd	
d	d	da	db	dc	d^2	
...						

Example 2.1.13. *The Klein Four group K_4 is a group of 4 elements $\{1, a, b, c\}$ with the law of composition defined by its multiplication table*

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

2.2 Permutations

Let X be a set. The set of all bijections of X, $P(X) = \{f : X \to X | f \text{ is bijective}\}$ with the law of composition to be composition of functions form a group, called the **permutation group** on X:

1. Composition of functions is associative

2. The identity element is the identity function on X:

$$\forall f \in P(X), f \circ id_X = id_X \circ f = f$$

3. The inverse of $f \in P(X)$ is its inverse function f^{-1}:

$$f \circ f^{-1} = f^{-1} \circ f = id_X$$

When X is a set of n elements, we can rename the elements by the numbers $1, 2, ..., n$, and call its permutation group the permutation group of n letters, denoted by S_n.

A first question: what is the order of S_n? This is to ask how many bijective maps

$$\{1, 2, ..., n\} \longrightarrow \{1, 2, ..., n\}$$

The answer is found by applying the Multiplication Principle from Combinatorics: $f(1)$ has n choices, and then $f(2)$ has $n-1$ choices,...., so the total number of choices is $n! = 1 \times 2 \times ... \times n$. We conclude $|S_n| = n!$

We need to find a way to represent the elements in S_n, so we introduce the following convention.

Definition 2.2.1. A **cycle** $(a_1\ a_2\ ...\ a_k) \in S_n$, where $a_1, ..., a_k$ are distinct numbers between 1 and n, is the function sending a_1 to a_2, a_2 to a_3,..., a_k to a_1, while keeping the other numbers fixed.

When $n = 2$, $S_2 = \{id, (1\ 2)\}$ is a group of order 2, and the multipliction table is

	id	$(1\ 2)$
id	id	$(1\ 2)$
$(1\ 2)$	$(1\ 2)$	id

When $n = 3$, $S_3 = \{id, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$. This is a non-abelian group:

$$(1\ 2)(1\ 3) = (1\ 3\ 2) \neq (1\ 2\ 3) = (1\ 3)(1\ 2)$$

There are some interesting properties of S_3:

1. $(1\ 2)^2 = (1\ 3)^2 = (2\ 3)^2 = id$

2. $(1\ 2\ 3)^3 = (1\ 3\ 2)^3 = id$

3. $(1\ 3\ 2)(1\ 2\ 3) = (1\ 2\ 3)(1\ 3\ 2) = id$

4. $(1\ 2\ 3) = (1\ 3\ 2)^2, (1\ 3\ 2) = (1\ 2\ 3)^2$

If we write $x = (1\ 2), y = (1\ 2\ 3)$, then $(1\ 3) = xy^2$, $(2\ 3) = xy$, $(1\ 3\ 2) = y^2$. We thus obtain

$$S_3 = \{id, x, y, y^2, xy, xy^2\}$$

Definition 2.2.2. Two cycles $(a_1\ \ ...\ \ a_k)$ and $(b_1\ \ ...\ \ b_m)$ in S_n are disjoint if $a_1, ..., a_k, b_1, ..., b_m$ are all distinct numbers.

Example 2.2.3. $(1\ \ 2\ \ 3)$ *and* $(4\ \ 5)$ *are disjoint, while* $(1\ \ 2\ \ 4)$ *and* $(4\ \ 5)$ *are not.*

We are going to introduce some properties of S_n, while the proofs will be postponed.

Proposition 2.2.4. *Disjoint cycles commute with each other.*

Example 2.2.5. $(1\ \ 2\ \ 3)(4\ \ 5) = (4\ \ 5)(1\ \ 2\ \ 3)$

Proposition 2.2.6. *Each element in S_n can be written as a finite product of pairwise disjoint cycles, and the product is unique up to reordering of the cycles. (Since disjoint cycles commute with each other, change of the ordering will not change the resulting product)*

Example 2.2.7. *If $\sigma \in S_5$, $\sigma(1) = 2, \sigma(2) = 1, \sigma(3) = 4, \sigma(4) = 3, \sigma(5) = 5$, then we can write*

$$\sigma = (1\ \ 2)(3\ \ 4)$$

Example 2.2.8. *We can write any product of cycles into a product of disjoint cycles:*

For example, let $\sigma = (1\ \ 2\ \ 3)(3\ \ 4\ \ 5) \in S_5$. $(1\ \ 2\ \ 3)$ and $(3\ \ 4\ \ 5)$ are bijective functions, and the law of composition of elements in S_n is the composition of functions, so in order to compute $\sigma(1)$, we need to first find the image of 1 under $(3\ \ 4\ \ 5)$, and then evaluate the result under $(1\ \ 2\ \ 3)$. The detailed computations can be shown by the following diagram, which indicates we can write

$$\sigma = (1\ \ 2\ \ 3\ \ 4\ \ 5)$$

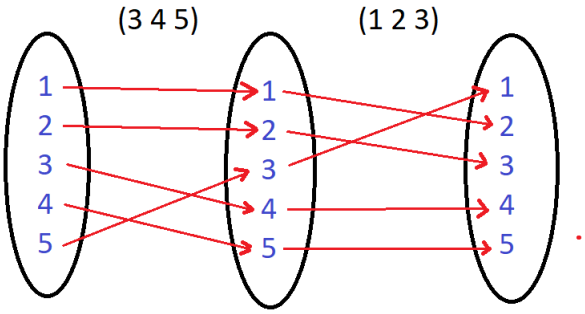


Figure 1: $(1\ \ 2\ \ 3)(3\ \ 4\ \ 5) = (1\ \ 2\ \ 3\ \ 4\ \ 5)$

Proposition 2.2.9. $(a_1\ \ a_2\ \ \ldots\ \ a_k)^{-1} = (a_k\ \ a_{k-1}\ \ \ldots\ \ a_1)$

Proof. It suffices to check $(a_1\ \ a_2\ \ \ldots\ \ a_k)(a_k\ \ a_{k-1}\ \ \ldots\ \ a_1) = id$ by evaluating on any $i \in \{1, 2, ..., n\}$ □

Exercise 2.2.10. *How many k-cycles are there in S_n?*

We will explore more about S_n when we are equipped with more tools in group theory.

2.3 Subgroups

Definition 2.3.1. A **subgroup** H of a group G is a subset of G satisfying:

1. Closure: $\forall a, b \in H \Longrightarrow ab \in H$
2. Identity: $1 \in H$
3. Inverse: $\forall a \in H \Longrightarrow a^{-1} \in H$

Example 2.3.2. *Given any group G, we can find two subgroups: G and $\{1\}$. Of course, when $G = \{1\}$, these two subgroups coincide.*

Proposition 2.3.3. *A nonempty subset H of a group G is a subgroup of G if and only if $\forall a, b \in H \Longrightarrow a^{-1}b \in H$*

Proof. If H is a subgroup of G, for any $a, b \in H$, we know $a^{-1} \in H$, then $a^{-1}b \in H$.

Conversely, if $\forall a, b \in H \Longrightarrow a^{-1}b \in H$, we need to verify the three axioms in the definition of subgroup. First, since H is nonempty, there exists $a \in H$, so $1 = a^{-1}a \in H$. Second, $\forall a \in H$, $a^{-1} = a^{-1}1 \in H$. Last, $\forall a \in H, b \in H$, we just showed $a^{-1} \in H$, so we see $ab = (a^{-1})^{-1}b \in H$ □

We can use the above proposition to test if a given subset is a subgroup.

Example 2.3.4. *$SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) | \det(A) = 1\}$ is a subgroup of $GL_n(\mathbb{R})$: $\forall A, B \in SL_n(\mathbb{R})$, we see*

$$\det(A^{-1}B) = \det(A)^{-1} \det(B) = 1$$

so $A^{-1}B \in SL_n(\mathbb{R})$.

Example 2.3.5. *If $m < n$ are positive integers, we can regard S_m as a subgroup of S_n, by viewing each element of S_m as a permutation that may permute $1, 2, ..., m$ while fixes $m + 1, m + 2, ..., n$.*

2.4 Subgroups of $\mathbb{Z}$

We now classify all the subgroups of the group of integers $\mathbb{Z}$ with addition.

If a is an integer, we write

$$a\mathbb{Z} = \{ak \in \mathbb{Z} | k \in \mathbb{Z}\}$$

which is the set of all multiples of a.

Theorem 2.4.1. *If H is a subgroup of $\mathbb{Z}$, then $H = a\mathbb{Z}$ for some $a \in \mathbb{N}$.*

Proof. Let H be a subgroup of $\mathbb{Z}$.

If $H = \{0\}$, then we can write $H = 0\mathbb{Z}$. If $H = \mathbb{Z}$, we can write $H = 1\mathbb{Z}$.

If $\{0\} \subsetneqq H \subsetneqq \mathbb{Z}$, then there exists m such that $m \in H \setminus \{0\}$. Since H is a subgroup of $\mathbb{Z}$, we get $-m \in H$. $m \neq 0$ indicates one of m and $-m$ is a positive integer, thus H contains at least one positive integer.

Define $a = \min\{m \in H | m > 0\}$. By the previous paragraph, we know $\{m \in H | m > 0\}$ is nonempty, so a exists. The assumption $H \neq \mathbb{Z}$ implies $a \neq 1$, since $1 \in \mathbb{Z}$ will imply $H = \mathbb{Z}$. Now we are going to show $H = a\mathbb{Z}$.

First, we will show $H \subseteq a\mathbb{Z}$: for any $n \in H$, suppose it is not in $a\mathbb{Z}$, i.e., n is not a multiple of a. Then there exists $q \in \mathbb{Z}$ and $r \in \mathbb{N}$ with $1 \leq r \leq a$ such that $n = aq + r$. This means

$$r = n - aq$$

Since $a \in H$, aq is a summation of copies of a or $-a$, we see $aq \in H$ and $-aq \in H$, so $r = n - aq \in H$. But this contradicts to the definition of a that a is the smallest positive integer in H. We conclude n is a multiple of $a\mathbb{Z}$, so $H \subseteq a\mathbb{Z}$.

Next, $a\mathbb{Z} \subseteq H$ since any multiple of a is in H by the fact H is a subgroup of $\mathbb{Z}$ and $a \in H$. So we have shown $H = a\mathbb{Z}$.

□

This theorem has interesting applications in number theory.

Given two integers a, b. Consider the set

$$S = a\mathbb{Z} + b\mathbb{Z} = \{ak + bm \in \mathbb{Z} | k, m \in \mathbb{Z}\}$$

Exercise 2.4.2. *Show that S is a subgroup of $\mathbb{Z}$.*

Once you verify that S is a subgroup of $\mathbb{Z}$, the previous theorem implies there exists $d \in \mathbb{N}$ such that $S = d\mathbb{Z}$. We call d the **greatest common divisor** of a and b.

Proposition 2.4.3. *If d is the greatest common divisor of a and b, then:*

1. *d divides a and d divides b.*
2. *There exists $r, s \in \mathbb{Z}$ such that $ar + bs = d$.*
3. *If c divides a and c divides b, then c divides d.*

Proof.

1. $a \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, so d divides a. Similarly, d divides b.
2. $d \in d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, so there exists $r, s \in \mathbb{Z}$ such that $d = ar + bs$.
3. By (2), $d = ar + bs$ for some $r, s \in \mathbb{Z}$. If c divides a, b, then c divides ar, bs, we see c divides $d = ar + bs$.

□

Definition 2.4.4. Two nonzero integers a, b are called **relatively prime** if their greatest common divisor is 1, i.e., $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$.

Corollary 2.4.5. *a and b are relatively prime if and only if there exists $r, s \in \mathbb{Z}$ such that $ar + bs = 1$.*

Proof. If a, b are relatively prime, by the definition, the greatest common divisor of a, b is 1, so the previous theorem implies there exists $r, s \in \mathbb{Z}$ such that $ar + bs = 1$.

Conversely, if there exists $r, s \in \mathbb{Z}$ such that $ar + bs = 1$, assume the common divisor of a, b is d, we see d divides $ar + bs = 1$, so $d = 1$. □

Corollary 2.4.6. *p is a prime number and $a, b \in \mathbb{Z}$. If p divides ab, then p divides a or p divides b.*

Proof. Assume p does not divide a. Since p is a prime, the only natural number that divides both a and p is 1. This indicates there exists $r, s \in \mathbb{Z}$ such that

$$ar + ps = 1$$

But multiplying b on both sides of the equation:

$$abr + psb = b$$

We know p divides ab, so p divides abr. Also p divides psb, we get p divides $b = abr + psb$. □

2.5 Cyclic Groups and Cyclic Subgroups

Definition 2.5.1. G is a group. $x \in G$. The **cyclic subgroup** of G generated by x is the set of all powers of x:

$$< x >= \{x^k \in G | k \in \mathbb{Z}\}$$

Proposition 2.5.2. *G is a group. $x \in G$. Let $S = \{k \in \mathbb{Z} | x^k = 1\}$, then S is a subgroup of $\mathbb{Z}$.*

Proof. If $k, l \in S$, then $x^k = x^l = 1$. $x^{-k} = (x^k)^{-1} = 1$, so $x^{-k_1+k_2} = x^{-k}x^l = 1$, we see $-k + l \in S$, and conclude S is a subgroup of $\mathbb{Z}$. □

Corollary 2.5.3. *G is a group. $x \in G$. Let $S = \{k \in \mathbb{Z} | x^k = 1\}$, if $S \neq \{0\}$, then there exists positive integer $|x|$ such that $S = |x|\mathbb{Z}$. Furthermore, $x^l = x^m$ if and only if $|x|$ divides $l - k$, so as a set, $< x >= \{1, x, ..., x^{|x|-1}\}$.*

Definition 2.5.4. H is a subgroup of G. Define the **order** of H to be the number of elements in H, denoted by $|H|$.

Definition 2.5.5. x is an element in a group G. If $| < x > |$ is infinite, we say x has **infinite order**. If $| < x > |$ is finite, define the **order** of the element x to be $|x| = | < x > |$, i.e., the order of the cyclic subgroup it generates.

Proposition 2.5.6. *G is a group, and $x \in G$ is an element of order n. Then $x^k = 1 \iff k$ is a multiple of n.*

Proof. It follows directly from Corollary 2.5.3. □

Definition 2.5.7. G is a group. If there exists $x \in G$ such that $G =< x >$, we say G is a **cyclic group** generated by x, and x is called a **generator** of the cyclic group G.

Example 2.5.8. *$\mathbb{Z}$ is an infinite cyclic group generated by $1 \in \mathbb{Z}$. It can also be generated by $-1 \in \mathbb{Z}$. Each subgroup of $\mathbb{Z}$, $a\mathbb{Z}$, is a cyclic subgroup generated by $a \in \mathbb{N}$.*

Theorem 2.5.9. *If $G =< x >$ is a cyclic group, then every subgroup of G is a cyclic subgroup.*

Proof. Let H be a subgroup of $G =< x >$ such that $H \neq \{1\}$. Let

$$m = \min\{k \in \mathbb{N}^{>0} | x^k \in H\}$$

We will prove that H is the cyclic subgroup generated by x^m, i.e.,

$$H = \{x^{lm} \in G | l \in \mathbb{Z}\}$$

First, for any $l \in \mathbb{Z}$, $x^{lm} = (x^m)^l \in H$, so $\{x^{lm} \in G | l \in \mathbb{Z}\} \subseteq H$.

Second, suppose $x^s \in H$, we will show m divides s. Suppose m does not divide S, then there exists integers q, r with $1 \leq r \leq m$ and

$$s = qm + r$$

This implies $x^s = x^{qm+r} = x^{qm}.x^r$, i.e., $x^r = (x^{-qm}).x^s \in H$, but this contradicts to $m = \min\{k \in \mathbb{N}^{>0} | x^k \in H\}$, we conclude m divides s, hence $H \subseteq \{x^{lm} \in G | l \in \mathbb{Z}\}$. □

Exercise 2.5.10. *$G =< x >$ is a finite cyclic group. Prove $G =< x^k >$ if and only if k and $|x|$ are relatively prime.*

2.6 Homomorphisms and Normal Subgroups

Definition 2.6.1. G and G' are groups. A **homomorphism** $\phi : G \longrightarrow G'$ is a function satisfying $\forall a, b \in G, \phi(ab) = \phi(a)\phi(b)$. That is, the function is compatible with the group structures.

Example 2.6.2. *Determinant function is a homomorphism:*

$$GL_n(\mathbb{R}) \xrightarrow{\det} \mathbb{R}^\times$$

$$A \mapsto \det(A)$$

Example 2.6.3. *If G is a group, and $x \in G$, then there is a homomorphism:*

$$\mathbb{Z} \longrightarrow G$$

$$k \mapsto x^k$$

Proposition 2.6.4. *A homomorphism $\phi : G \longrightarrow G'$ maps identity to identity, and inverse to inverse:*

1. $\phi(1_G) = 1_{G'}$
2. $\forall g \in G, \phi(g)^{-1} = \phi(g^{-1})$

Proof. 1. $\phi(1_G) = \phi(1_G.1_G) = \phi(1_G)\phi(1_G)$, so $\phi(1_G) = 1_{G'}$

2. $\phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(1_G) = 1_{G'}$, so $\phi(g)^{-1} = \phi(g^{-1})$

□

Definition 2.6.5. $\phi : G \longrightarrow G'$ is a homomorphism. Define the **kernel** of ϕ to be

$$\ker \phi = \{g \in G | \phi(g) = 1_{G'}\}$$

Define the **image** of ϕ to be

$$\operatorname{Im} \phi = \{\phi(g) \in G' | g \in G\}$$

Proposition 2.6.6. *$\phi : G \longrightarrow G'$ is a homomorphism, then $\ker \phi$ is a subgroup of G and $\operatorname{Im} \phi$ is a subgroup of G'.*

Proof. If $a, b \in \ker \phi$, $\phi(a) = \phi(b) = 1_{G'}$.

$$\phi(a^{-1}b) = \phi(a)^{-1}\phi(b) = 1_{G'}$$

So $a^{-1}b \in \ker \phi$, $\ker \phi$ is a subgroup of G.

If $x, y \in \operatorname{Im} \phi$, then there exists $a, b \in G$ such that $x = \phi(a)$ and $y = \phi(b)$. Then $x^{-1}y = \phi(a)^{-1}\phi(b) = \phi(a^{-1}b) \in \operatorname{Im} \phi$. So $\operatorname{Im} \phi$ is a subgroup of G'. □

Proposition 2.6.7. *$\phi : G \longrightarrow G'$ is a homomorphism, then ϕ is injective if and only if $\ker \phi = \{1_G\}$.*

Proof. If ϕ is injective, then $\ker \phi = \phi^{-1}(1_{G'})$ consists of at most one element, and we know $1_G \in \ker \phi$, we get $\ker \phi = \{1_G\}$.

Conversely, if $\ker \phi = \{1_G\}$, for any $a, b \in G$ such that $\phi(a) = \phi(b)$, we have $\phi(a^{-1}b) \in \ker \phi = \{1_G\}$ so $a^{-1}b = 1_G$, $a = b$, hence ϕ is injective. □

Example 2.6.8. $\det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^\times$ *is a homomorphism, and*

$$\ker \det = \{A \in GL_n(\mathbb{R}) | \det A = 1\} = SL_n(\mathbb{R})$$

An important observation regarding the kernel of a homomorphism $\phi : G \longrightarrow G'$ is that if $g \in \ker \phi$, then for any $x \in G$, $xgx^{-1} \in \ker \phi$:

$$\phi(xgx^{-1}) = \phi(x)\phi(g)\phi(x)^{-1} = \phi(x).1_{G'}.\phi(x)^{-1} = 1_{G'}$$

This observation leads to the following concept:

Definition 2.6.9. G is a group. The **conjugation** of $x \in G$ by $g \in G$ is the element $gxg^{-1} \in G$. We say x and gxg^{-1} are conjugate elements.

Definition 2.6.10. A subgroup N of G is called a **normal subgroup** if $\forall n \in N, \forall g \in G, gng^{-1} \in N$.

Exercise 2.6.11. *N is a subgroup of G. Prove the following are equivalent:*

1. *N is a normal subgroup of G.*
2. *$\forall g \in G$, $gNg^{-1} \subseteq N$.*
3. *$\forall g \in G$, $gNg^{-1} = N$.*

Example 2.6.12. *If G is an abelian group, then any subgroup of G is a normal subgroup of G.*

This definition describes our previous observation of kernels:

Proposition 2.6.13. *The kernel of a homomorphism is a normal subgroup of the domain group.*

Example 2.6.14. *We have shown that $SL_n(\mathbb{R}) = \ker \det$, so by the above proposition, $SL_n(\mathbb{R})$ is a normal subgroup of $GL_n(\mathbb{R})$.*

Definition 2.6.15. The **centre** of a group G is the subset

$$Z(G) = \{g \in G | gx = xg \text{ for any } x \in G\}$$

Exercise 2.6.16. *Prove G is abelian if and only if $Z(G) = G$.*

Exercise 2.6.17. *Prove the centre of G, $Z(G)$, is a normal subgroup of G.*

Definition 2.6.18. If G is a group whose only normal subgroups are $\{1\}$ and G, we say G is a **simple group**.

Corollary 2.6.19. *If G is a simple group, then either G is abelian or G has trivial centre.*

2.7 Isomorphisms and Automorphisms

Definition 2.7.1. An **isomorphism** is a bijective homomorphism.

Example 2.7.2. *If $G =< x >$ in an infinite cyclic group, then*

$$\phi : \mathbb{Z} \longrightarrow G$$

$$k \mapsto x^k$$

is an isomorphism.

Proposition 2.7.3. *If $\phi : G \longrightarrow G'$ is an isomorphism, then ϕ^{-1} is also an isomorphims.*

Proof. We need to show the inverse function $\phi^{-1} : G' \longrightarrow G$ is also a homomorphism.

For any $x, y \in G'$, let $a = \phi^{-1}(x)$ and $b = \phi^{-1}(y)$. This means $x = \phi(a)$ and $y = \phi(b)$. Since ϕ is a homomorphism, $xy = \phi(a)\phi(b) = \phi(ab)$, we get

$$\phi^{-1}(xy) = ab = \phi^{-1}(x)\phi^{-1}(y)$$

□

Definition 2.7.4. Two groups G and G' are called **isomorphic** if there exists an isomorphism $\phi : G \longrightarrow G'$, and we write $G \cong G'$.

Intuitively, two groups are isomorphic means they have the same algebraic structures, that is, they will share all the algebraic properties. We can interpret an isomorphism as "a change of name" for the elements in the group.

Definition 2.7.5. All the groups isomorphic to a given group G form the **isomorphic class** of G. When we classify groups we will classify them up to isomorphism classes.

Definition 2.7.6. An isomorphism $\phi : G \longrightarrow G$ of a group to itself is called an **automorphism** of G.

Example 2.7.7.

$$\phi : \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$k \mapsto -k$$

Example 2.7.8. *G is a group. $g \in G$. Then there is an automorphism of G given by conjugation:*

$$\phi_g : G \longrightarrow G$$
$$x \mapsto gxg^{-1}$$

Exercise 2.7.9. *Verify ϕ_g in the above example is an automorphism.*

Definition 2.7.10. The set of all automorphisms of G with the law of composition to be composition of functions form a group, called the **group of automorphisms** of G, denoted by $Aut(G)$.

Example 2.7.11. *We will prove in homework that $Aut(\mathbb{Z})$ is isomorphic to a cyclic group of order 2.*

Definition 2.7.12. The **inner automorphism group** of a group G is the subgroup

$$Inn(G) = \{\phi_g \in Aut(G) | g \in G\}$$

where ϕ_g is defined in Example 2.7.8 .

Exercise 2.7.13. *Verify $Inn(G)$ is a subgroup of $Aut(G)$.*

Exercise 2.7.14. *Prove $f : G \longrightarrow Aut(G)$ defined by $f(g) = \phi_g$ defines a group homomorphism, and the kernel of f is $Z(G)$.*

3 Quotients and Products of Groups

3.1 Cosets

Definition 3.1.1. H is a subgroup of G, and $x \in G$. The subset

$$xH = \{xh \in G | h \in H\}$$

is called a **left coset**, and the subset

$$Hx = \{hx \in G | h \in H\}$$

is called a **right coset**.

Given a subgroup H of a group G, we can define an equivalence relation on G: $x \sim y$ if $\exists h \in H$ such that $y = xh$. We can check this is an equivalence relation:

1. $\forall x \in G$, $x = x.1$ and $1 \in H$, so $x \sim x$.
2. If $x \sim y$, $y = xh$ for some $h \in H$, then $x = yh^{-1}$, $h^{-1} \in H$, so $y \sim x$.
3. If $x \sim y$ and $y \sim z$, then $y = xh_1$ and $z = yh_2$ for some $h_1, h_2 \in H$. $z = yh_2 = xh_1h_2$ with $h_1h_2 \in H$, so $x \sim z$.

Each equivalence class is of the form

$$[x] = \{g \in G | x \sim g\} = \{g \in G | g = xh \text{ for some } h \in H\} = xH$$

We see each equivalence class is indeed a left coset, so left cosets form a partition of G. In particular, this implies

Corollary 3.1.2. *Two left cosets xH and yH are either equal or disjoint.*

If we replace left cosets by right cosets and make the corresponding modifications in the above discussion, we will obtain similar results for right cosets as well.

Example 3.1.3. *$2\mathbb{Z}$ is a subgroup in $\mathbb{Z}$. There are two distinct left cosets: $0 + 2\mathbb{Z}$ and $1 + 2\mathbb{Z}$.*

Proposition 3.1.4. *H is a subgroup of a group G. $a, b \in G$. The following are equivalent:*

1. $\exists h \in H$ *such that* $b = ah$

2. $a^{-1}b \in H$

3. $b \in aH$

4. $aH = bH$

Exercise 3.1.5. *Prove the above proposition.*

Definition 3.1.6. H is a subgroup of G. Define the **index** of H in G to be the number of left (or right) cosets, and it is denoted by $[G : H]$.

Example 3.1.7. $[\mathbb{Z} : 2\mathbb{Z}] = 2$ *since there are two distinct left cosets.*

Theorem 3.1.8 (Lagrange's Theorem)**.** *H is a subgroup of a finite group G. Then*

$$[G : H] = \frac{|G|}{|H|}$$

In particular, we see the order of a subgroup divides the order of a group.

Proof. Since all the left cosets form a partition of G, we only need to show all the cosets have $|H|$ elements, and by the definition of index, there are $[G : H]$ left cosets in total, so we finish the proof.

Given $x \in G$, define a function

$$f : H \longrightarrow xH$$

$$h \mapsto xh$$

It is easy to see f is bijective, which implies $|xH| = |H|$. □

Example 3.1.9. $|S_3| = 6$, *and* $| < (1\ 2) > | = |\{id, (1\ 2)\}| = 2$, *so by Lagrange' Theorem, there are* $\frac{6}{2} = 3$ *left cosets. Indeed they are:*

$id < (1\ 2) >= \{id, (1\ 2)\}$

$(1\ 3) < (1\ 2) >=< (1\ 3), (1\ 3)(1\ 2) >= \{(1\ 3), (1\ 2\ 3)\}$

$(2\ 3) < (1\ 2) >= \{(2\ 3), (2\ 3)(1\ 2)\} = \{(2\ 3), (1\ 3\ 2)\}$

Corollary 3.1.10. *The order of an element in a group divides the order of the group.*

Proof. $x \in G$. Let $< x >$ be the cyclic subgroup generated by x. By Lagrange's Theorem, $|x| = | < x > |$ divides $|G|$. □

Corollary 3.1.11. *G is a finite group and $x \in G$, then $x^{|G|} = 1$.*

Proof. This follows from the colollary above. □

Corollary 3.1.12. *A group of prime order is cyclic.*

Proof. If $|G| = p$ is a prime, take any $x \neq 1$ in G. Then $|x|$ divides p and $|x| \neq 1$, we get $|x| = p = |G|$. This means $< x >= G$, so G is cyclic. □

Proposition 3.1.13. *H is a subgroup of G and K is a subgroup of H, then $[G : K] = [G : H][H : K]$*

Proof. When G is a finite group, this is just a corollary of the Lagrange's Theorem:

$$[G : K] = \frac{|G|}{|K|} = \frac{|G|}{|H|}\frac{|H|}{|K|} = [G : H][H : K]$$

More generally, we cannot assume $|G|$ is finite, so we need to argue by counting.

Assume $[G : H] = m$ and $[H : K] = n$. Choose a representative for each left coset of H in G:

$$g_1H, g_2H, ..., g_mH$$

and choose a representative for each left coset of K in H:

$$h_1K, h_2K, ..., h_nK$$

Then we will prove all the distinct left cosets of K in G are g_ih_jK, $1 \leq i \leq m$ and $1 \leq j \leq n$. This will indicate there are in total mn cosets of K in G, so $[G : K] = mn = [G : H][H : K]$.

First, if $i_1 \neq i_2$, then $g_{i_1}h_{j_1}K \subset g_{i_1}H$ and $g_{i_2}h_{j_2}K \subset g_{i_2}H$, and $g_{i_1}H \cap g_{i_2}H = \emptyset$, so $g_{i_1}h_{j_1}K \cap g_{i_2}h_{j_2}K = \emptyset$.

Next, if $i_1 = i_2$ but $j_1 \neq j_2$, then $h_{j_1}K \cap h_{j_2}K = \emptyset$, so $g_{i_1}h_{j_1}K \cap g_{i_1}h_{j_2}K = \emptyset$.

We therefore see that all the g_ih_jK are disjoint. We still need to show their union is G.

$\forall x \in G$, $\exists 1 \leq i \leq m$ such that $x \in g_iH$. We can find $h \in H$ such that $x = g_ih$, and there is $1 \leq j \leq n$ such that $h \in h_jK$, so we can find $k \in K$ such that $h = h_jk$, $x = g_ih = g_ih_jk \in g_ih_jK$. We conclude $G = \sqcup_{1 \leq i \leq m, 1 \leq j \leq n} g_ih_jK$.

□

3.2 Quotient Groups

Similar to left cosets, the right cosets of H in G also give a partition of G. But in general, left cosets and right cosets may lead to different partitions, since it may happen that $gH \neq Hg$ for some $g \in G$. We would like to see when left cosets and right cosets coincide with each other. The observation is:

$\forall x \in G, xH = Hx \iff \forall x \in G, xHx^{-1} = H \iff H$ is a normal subgroup of G

So we see that we don't distinguish left and right cosets if and only if H is a normal subgroup in G.

If N is a normal subgroup in G, denote the set of cosets by G/N, and it has a group structure:

$$G/N \times G/N \longrightarrow G/N$$

$$(g_1N, g_2N) \mapsto (g_1N)(g_2N) = g_1g_2N$$

We call this group G/N the **quotient group**, and we define

$$\pi : G \longrightarrow G/N$$

$$g \mapsto gN$$

to be the **quotient map**.

Proposition 3.2.1. *The quotient map $\pi : G \longrightarrow G/N$ is a surjective homomorphism.*

Proof. For any $gN \in G/N$, $gN = \pi(g)$, so it is surjective. It is a homomorphism since

$$\pi(g_1g_2) = g_1g_2N = (g_1N)(g_2N) = \pi(g_1)\pi(g_2)$$

□

We now have a clearer description of the relation between normal subgroups and group homomorphisms: The kernel of a homomorphism is a normal subgroup, and each normal subgroup is the kernel of a surjective homomorphism.

3.3 Integers modulo n

For each integer $n \geq 2$, $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$, and $\mathbb{Z}$ is abelian, so $n\mathbb{Z}$ is a normal subgroup in $\mathbb{Z}$. We thus have the quotient group

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, ..., (n-1) + n\mathbb{Z}\}$$

We usually write $k + n\mathbb{Z}$ as $\overline{k}$ or $[k]$. The group composition for this map, usually called addition, is given by

$$\overline{k_1} + \overline{k_2} = \overline{k_1 + k_2}$$

The identity element is $\overline{0}$. The inverse element of $\overline{k}$ is $\overline{-k} = \overline{n-k}$. This is a cyclic group of order n, and $\overline{1}$ is a generator. Also, $\overline{k_1} = \overline{k_2}$ if and only if n divides $k_1 - k_2$.

The corresponding quotient map

$$\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

$$k \mapsto \bar{k}$$

is called the **integer modulo n** map. If $\overline{k_1} = \overline{k_2}$, we say k_1 and k_2 are **congruent modulo n**, and we can write

$$k_1 \equiv k_2 \bmod n$$

Besides the addition, there is another operation that can be defined on $\mathbb{Z}/n\mathbb{Z}$, which is called multiplication, and defined by

$$\bar{k}_1\bar{k}_2 = \overline{k_1 k_2}$$

Lemma 3.3.1. *The multiplication on $\mathbb{Z}/n\mathbb{Z}$ is well-defined.*

Proof. If $\overline{a} = \overline{a'}$ and $\overline{b} = \overline{b'}$, then n divides $a' - a$ and $b' - b$, so there exists $l_1, l_2 \in \mathbb{Z}$ such tat

$$\begin{cases} a' - a = nl_1 \\ b' - b = nl_2 \end{cases}$$

We get

$$\begin{aligned} a'b' - ab &= (a + nl_1)(b + nl_2) - ab \\ &= ab + nl_1 b + nl_2 a + n^2 l_1 l_2 - ab \\ &= n(l_1 b + l_2 a + nl_1 l_2) \end{aligned}$$

So n divides $a'b' - ab$, $\overline{a}\overline{b} = \overline{a}'\overline{b}'$

□

Remark 3.3.2. The multiplication cannot make $\mathbb{Z}/n\mathbb{Z}$ into a group, since some elements are not multiplicatively invertible. For example, $\overline{0}$ has no multiplicative inverse. $\mathbb{Z}/n\mathbb{Z}$ together with addition and multiplication forms an algebraic structure called a ring, which we shall study later.

Definition 3.3.3. An element $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ is a **unit** if there exists $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$ such that $\overline{a}\overline{b} = \overline{1}$.

Proposition 3.3.4. *$\overline{a} \in \mathbb{Z}/n\mathbb{Z}$. The following are equivalent:*

1. *$\overline{a}$ is a unit.*
2. *n and a are relatively prime.*
3. *$\overline{a}$ is a generator for $\mathbb{Z}/n\mathbb{Z}$.*
4. *$f : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ defined by $f(\overline{k}) = \overline{ak}$ is an automorphims.*

Proof. (1) $\Longrightarrow$ (4): If $\overline{a}$ is a unit, then there exists $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$ such that $\overline{ab} = \overline{1}$. This implies the inverse function of $f(\overline{k}) = \overline{ak}$ is $g(\overline{k}) = \overline{bk}$, so f is invertible, and f is a homomorphism since $f(\overline{k+l}) = \overline{a(k+l)} = \overline{ak} + \overline{al} = f(\overline{k}) + f(\overline{l})$.

(4) $\Longrightarrow$ (3): If $f(\overline{k}) = \overline{ak}$ is an automorphism, then for any $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$, there is $\overline{l} \in \mathbb{Z}/n\mathbb{Z}$ such that $\overline{m} = f(\overline{l}) = \overline{al} = \underbrace{\overline{a + a + ... + a}}_{l \text{ copies}} = \underbrace{\overline{a} + ... + \overline{a}}_{l \text{ copies}}$.
We conclude $\overline{a}$ generates $\mathbb{Z}/n\mathbb{Z}$.

(3) $\Longrightarrow$ (2): If $\overline{a}$ is a generator of $\mathbb{Z}/n\mathbb{Z}$, then for $\overline{1} \in \mathbb{Z}/n\mathbb{Z}$, there is natural number l such that $\overline{1} = \underbrace{\overline{a} + ... + \overline{a}}_{l \text{ copies}} = \overline{al}$. This implies there is $b \in \mathbb{Z}$ such that $1 - al = nb$, i.e. $al + nb = 1$, so a and n are relatively prime.

(2) $\Longrightarrow$ (1): If n and a are relatively prime, then we can find $k, b \in \mathbb{Z}$ such that $nk + ab = 1$, which implies $\overline{ab} = \overline{1}$, so $\overline{a}$ is a unit.

□

Definition 3.3.5. The set of all units in $\mathbb{Z}/n\mathbb{Z}$ form a group with composition $\overline{a}\overline{b} = \overline{ab}$, and denote it by $(\mathbb{Z}/n\mathbb{Z})^\times$, called the **group of units**.

Lemma 3.3.6. *The above definition indeed defines a group.*

Proof. We have shown before $\overline{a}\overline{b} = \overline{ab}$ is well-defined on $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$. But we still need to show $\overline{ab}$ is a unit given $\overline{a}$ and $\overline{b}$ are units. This is because $\overline{a}$, $\overline{b}$ are units imply there exists $\overline{k}$, $\overline{l}$ such that $\overline{ak} = \overline{bl} = \overline{1}$. Then

$$\overline{ab}.\overline{kl} = \overline{abkl} = \overline{akbl} = \overline{1}$$

So $\overline{ab}$ is also a unit.

Next we can verify the three axioms for groups.
Associativity: $(\overline{a}\overline{b})\overline{c} = \overline{ab}\overline{c} = \overline{abc} = \overline{a}\overline{bc} = \overline{a}(\overline{b}\overline{c})$
Identity: $\overline{1}$ is the identity.
Inverse exists by the definition of units. □

Definition 3.3.7. The **Euler's phi function** defined on positive integers is

$\phi(n) =$ the number of element in $\{k \in \mathbb{N} | 1 \leq k \leq n$ and k, n are relatively prime$\}$

Lemma 3.3.8. $|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$

Proof. Each unit $\overline{a}$ has a unique representative on the set $\{1, 2, ..., n\}$, and $\overline{a}$ is a unit if and only if a, n are relatively prime, so the lemma follows. □

Theorem 3.3.9. *(Fermat's Little Theorem) If a, n are relatively prime, then*

$$a^{\phi(n)} \equiv 1 \ mod \ n$$

Proof. a, n are relatively prime $\Longrightarrow \overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, and $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$, so $\overline{a}^{\phi(n)} = \overline{1}$, i.e., $\overline{a^{\phi(n)}} = \overline{1}$, $a^{\phi(n)} \equiv 1 \bmod n$. □

Corollary 3.3.10. *If p is a prime, a is not divisible by p, then*

$$a^{p-1} \equiv 1 \ mod \ n$$

There is another interesting interpretation of $(\mathbb{Z}/n\mathbb{Z})^\times$:

Theorem 3.3.11. $Aut(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

Proof. First, if $f \in Aut(\mathbb{Z}/n\mathbb{Z})$, then we see

$$f(\overline{k}) = f(\underbrace{\overline{1} + ... + \overline{1}}_{k \text{ copies}}) = \underbrace{f(\overline{1}) + ... + f(\overline{1})}_{k \text{ copies}}$$

Let $\overline{a} = f(\overline{1})$, we see

$$f(\overline{k}) = \underbrace{\overline{a} + ... + \overline{a}}_{k \text{ copies}} = \overline{ak}$$

We thus see all the automorphisms $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ are of the form

$$f(\overline{k}) = \overline{ak}$$

for some $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$. We have proved in Proposition 4.6.18 that it is an automorphism if and only if $\overline{a} = f(\overline{1})$ is a unit.

So the following map

$$\Phi : Aut(\mathbb{Z}/n\mathbb{Z}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$

$$f \mapsto f(\overline{1})$$

is bijective. We need to verify Φ is a homomorphism: for any $f_1, f_2 \in Aut(\mathbb{Z}/n\mathbb{Z})$, let $\overline{b} = f_2(\overline{1})$, then

$$\Phi(f_1 \circ f_2) = f_1(f_2(\overline{1})) = f_1(\overline{b}) = \underbrace{f_1(\overline{1}) + ... + f_1(\overline{1})}_{b \text{ copies}} = \overline{b} f_1(\overline{1}) = f_1(\overline{1}) f_2(\overline{1}) = \Phi(f_1)\Phi(f_2)$$

□

Remark 3.3.12. The inverse function of Φ is

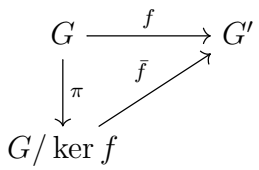
$$\Phi^{-1} : (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow Aut(\mathbb{Z}/n\mathbb{Z})$$

$$\overline{a} \mapsto f_{\overline{a}}$$

where $f_{\overline{a}}(\overline{k}) = \overline{ak}$

3.4 First Isomorphism Theorem

Theorem 3.4.1. *$f : G \longrightarrow G'$ is a surjective homomorphism, $\pi : G \longrightarrow G/\ker f$ is the quotient map. Then there is a unique isomorphism $\bar{f} : G/\ker f \longrightarrow G'$ such that $f = \bar{f} \circ \pi$, i.e., the following diagram commutes:*



Proof. Denote $N = \ker f$. Define $\bar{f} : G/N \longrightarrow G'$ by $\bar{f}(gN) = f(g)$.

We need to first show $\bar{f}$ is well-defined. If $g_1N = g_2N$, then $g_1^{-1}g_2 \in N$, $f(g_1^{-1}g_2) = 1_{G'}$, $f(g_1)^{-1}f(g_2) = 1_{G'}$, so $f(g_1) = f(g_2)$. This means

$$\bar{f}(g_1N) = f(g_1) = f(g_2) = \bar{f}(g_2N)$$

So $\bar{f}$ is well-defined.

Next, we show $\bar{f}$ is a homomorphism: for any $xN, yN \in G/N$,

$$\bar{f}(xN.yN) = \bar{f}(xyN) = f(xy) = f(x)f(y) = \bar{f}(xN)\bar{f}(yN)$$

$\bar{f}$ is injective since for any $gN \in \ker \bar{f}$, $1_{G'} = \bar{f}(gN) = f(g)$, so $g \in N$, $gN = N$. We see $\ker \bar{f} = \{N\}$, so $\bar{f}$ is injective.

$\bar{f}$ is surjective: for any $g' \in G'$, since f is surjective, there is $g \in G$ such that $g' = f(g)$, so $g' = \bar{f}(gN)$, $\bar{f}$ is surjective.

$f = \bar{f} \circ \pi$: for any $g \in G$, $\bar{f} \circ \pi(g) = \bar{f}(gN) = f(g)$.

$\bar{f}$ is unique: If there is $F : G/N \longrightarrow G'$ such that $f = F \circ \pi$, then for any $gN \in G/N$, $F(gN) = F(\pi(g)) = f(g) = \bar{f}(\pi(g)) = \bar{f}(gN)$, so $F = \bar{f}$.

□

Corollary 3.4.2. *If G is a finite group, $f : G \longrightarrow G'$ is a homomorphism, then $|G| = |\ker f| \times |\operatorname{Im} f|$*

Proof. By First Isomorphism Theorem, $G/\ker f \cong \operatorname{Im} f$, so $|G/\ker f| = |\operatorname{Im} f|$. By Lagrange's Theorem, $\frac{|G|}{|\ker f|} = |G/\ker f| = |\operatorname{Im} f|$, so $|G| = |\ker f| \times |\operatorname{Im} f|$ □

Corollary 3.4.3. *If G and G' are two groups such that $|G|, |G'|$ are relatively prime, then the only homomorphism $G \longrightarrow G'$ is the trivial map that sends every element of G to $1_{G'}$.*

Proof. If $f : G \longrightarrow G'$ is a homomorphism, then $\operatorname{Im} f$ is a subgroup of G', so $|\operatorname{Im} f|$ divides $|G'|$. The previous corollary tells us that $|\operatorname{Im} f|$ divides $|G|$, but $|G|$ and $|G'|$ are relatively prime, we conclude $|\operatorname{Im} f| = 1$, so f is the trivial map. □

Example 3.4.4. $\det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^\times$ *is a homomorphism,* $\ker(\det) = SL_n(\mathbb{R})$*, and* $\det$ *is surjective, so by First Isomorphism Theorem:*

$$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^\times$$

Example 3.4.5. $f : \mathbb{R} \longrightarrow \mathbb{C}^\times$ *defined by* $f(r) = e^{2\pi ri}$ *is a group homomorphism.* $\ker f = \mathbb{Z}$, $\operatorname{Im}(f) = S^1 = \{z \in \mathbb{C} || z| = 1\}$. *So by the First Isomorphism Theorem,*

$$\mathbb{R}/\mathbb{Z} \cong S^1$$

3.5 Product Groups

Definition 3.5.1. G and G' are groups. Define their **product group** to be the set of all ordered pairs (g, g'), where $g \in G$ and $g' \in G'$, with law of composition $(g_1, g_1')(g_2, g_2') = (g_1 g_2, g_1' g_2')$. The product group is denoted by $G \times G'$.

There are injective maps of G and G' into $G \times G'$ by

$$i_1 : G \longrightarrow G \times G'$$

$$g \mapsto (g, 1_{G'})$$

and

$$i_2 : G' \longrightarrow G \times G'$$

$$g' \mapsto (1_G, g')$$

Also there are surjective projections:

$$G \times G' \longrightarrow G$$

$$(g, g') \mapsto g$$

and

$$G \times G' \longrightarrow G'$$

$$(g, g') \mapsto g'$$

Lemma 3.5.2. *The images of the inclusions, $i_1(G)$ and $i_2(G')$ are normal subgroups in $G \times G'$.*

Exercise 3.5.3. *Prove the Lemma.*

Given a group G and two subgroups H and K, we construct the product group $H \times K$, and there is a map:

$$f : H \times K \longrightarrow G$$

$$(h, k) \mapsto hk$$

We see the image of f is $HK = \{hk \in G | h \in H, k \in K\}$. Now we are going to study when the above function is an isomorphism, that is, when G is isomorphic to a direct product of two of its subgroups.

Theorem 3.5.4. *G is a group, H and K are its subgroups. Then*

$$f : H \times K \longrightarrow G$$

defined above is an isomorphism if and only if $H \cap K = \{1\}$, $HK = G$ and H, K are normal subgroups of G.

Proof. If $f : H \times K \longrightarrow G$ is an isomorphism, then normal subgroups map to normal subgroups. Since $H \times \{1\}$ and $\{1\} \times K$ are normal subgroups in $H \times K$, their images, H and K, are normal subgroups in G.

The image of f is HK, and f is an isomorphism, so $HK = G$.

Suppose $H \cap K \neq \{1\}$, then there exists $g \in H \cap K$, $g \neq 1$. But then $f(g, 1) = g = f(1, g)$, contradict to f is an isomorphism. We conclude $H \cap K = \{1\}$.

Conversely, if $H \cap K = \{1\}$, $HK = G$ and H, K are normal subgroups of G, then f is injective: if $f(h_1, k_1) = f(h_2, k_2)$, then $h_1k_1 = h_2k_2$, $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{1\}$, we get $h_1 = h_2$ and $k_1 = k_2$.

The assumption $HK = G$ implies f is surjective.

It remains to check f is a homomorphism. $f((h_1, k_1)(h_@, k_2)) = f(h_1h_2, k_1k_2) = h_1h_2k_1k_2$. It suffices to prove $hk = kh$ for any $h \in H$ and $k \in K$. $hk = kh$ if and only if $hkh^{-1}k^{-1} = 1$. Observe that $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1}$. K is a normal subgroup, so $hkh^{-1} \in K$, $hkh^{-1}k^{-1} \in K$. Similarly we can show $hkh^{-1}k^{-1} \in H$, and by the fact $H \cap K = \{1\}$, we conclude $hkh^{-1}k^{-1} = 1$, i.e., $hk = kh$.

□

Corollary 3.5.5. *r and s are relatively prime positive integers, then a cyclic group of order rs is isomorphic to the product of a cyclic group of order r and a cyclic group of order s.*

Proof. $G =< x >$ is a cyclic group of order rs. Consider $H =< x^s >$ and $K =< x^r >$. $|x^r| = s$ and $|x^s| = r$, so H is a cyclic group of order r and K is a cyclic group of order s.

Since r and s are relatively prime, we see $|H \cap K| = 1$, so $H \cap K = \{1\}$.

r and s being relatively prime implies there exists integers k and l such that $rk + sl = 1$. So for any $m \in \mathbb{Z}$, $m = rkm + slm$. This means

$$x^m = x^{rkm+slm} = (x^s)^{lm}(x^r)^{km} \in HK$$

so $G = HK$.

H and K are normal subgroups in G since G is cyclic, in particular, it is abelian.

Applying the theorem above, we can conclude $G \cong H \times K$. □

Remark 3.5.6. We know a cyclic group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$, so given relatively prime numbers r and s, the above corollary can be expressed as

$$\mathbb{Z}/rs\mathbb{Z} \cong \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$$

And an isomorphism can be explicitly given by

$$\mathbb{Z}/rs\mathbb{Z} \longrightarrow \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$$

$$\bar{k}_{rs} \mapsto \bar{k}_r \times \bar{k}_s$$

This is called the **Chinese Reminder Theorem** (group version). It implies that the system of congrence equations

$$\begin{cases} x \equiv a \ (mod\ r) \\ x \equiv b \ (mod\ s) \end{cases}$$

has a unique solution up to congruence modulo rs if r and s are relatively prime.

Later when we discuss about ring theory, we will show the ring version of the theorem, and the group version describes parts of the results in the ring version.

Exercise 3.5.7. *Prove the map defined in the above remark*

$$\mathbb{Z}/rs\mathbb{Z} \longrightarrow \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$$

$$\bar{k}_{rs} \mapsto \bar{k}_r \times \bar{k}_s$$

is well-defined, then show it is an isomorphism.

Example 3.5.8. *Recall that the Klein Four Group $k_4 = \{1, a, b, c\}$ has multiplication table*

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Consider the cyclic subgroups $< a >$ and $< b >$. Both of them are of order 2.

$< a > \cap < b >= \{1\}$ *since* $< a >= \{1, a\}$, $< b >= \{1, b\}$

$< a >< b >= K_4$: $1.1 = 1, a.1 = a, 1.b = b, a.b = c$

The multiplication table implies K_4 is abelian, so $< a >$ and $< b >$ are normal subgroups.

We conclude $K_4 \cong < a > \times < b > \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

This example in particular tells us that in the corollary above, if we delete the condition r and s being relatively prime, then the product of two cyclic groups may not be a cyclic group.

Exercise 3.5.9. *If $x \in G$ and $y \in G'$ such that $|x| = m$, $|y| = n$, then what is the order of $|(x, y)|$ as an element of $G \times G'$?*

Exercise 3.5.10. *Show that If r, s are not relatively prime, then $\mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/rs\mathbb{Z}$.*

4 Groups and Symmetries

4.1 Cycles in Symmetric Groups

We are going to discover more properties of the symmetric groups (also called permutation groups) S_n in this chapter.

Notation 4.1.1. *One way to express an element $\sigma \in S_n$ is to list the image of each number $1, 2, ..., n$ via σ as follows:*

$$\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix}$$

Example 4.1.2. *If $\sigma \in S_3$ interchanges 1 and 2 while fixes 3, we can write*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

This notation is very clear, but sometimes takes much time and/or ink...

Another way to express a permutation is to make use of cycles that we have defined before.

Definition 4.1.3. Two cycles $(a_1 \ \ a_2 \ \ ... \ \ a_k)$ and $(b_1 \ \ b_2 \ \ ... \ \ b_l)$ are **disjoint** if $a_1, a_2, ..., a_k, b_1, b_2, ..., b_l$ are all distinct.

Lemma 4.1.4. *Two disjoint cycles commute with each other.*

Proof. We can let $(a_1 \ \ a_2 \ \ ... \ \ a_k)(b_1 \ \ b_2 \ \ ... \ \ b_l)$ and $(b_1 \ \ b_2 \ \ ... \ \ b_l)(a_1 \ \ a_2 \ \ ... \ \ a_k)$ act on any number in $\{1, 2, ..., n\}$, and we will find the images are always equal. □

Remark 4.1.5. One cycle may have more than one expressions. Indeed, there are k equivalent expressions for each k-cycle. For example,

$$(1 \ \ 2 \ \ 3) = (2 \ \ 3 \ \ 1) = (3 \ \ 1 \ \ 2)$$

When we compute composition of cycles, we will use the convention that the one on the right evaluate on $\{1, 2, ..., n\}$ first, following the definition that a permutation is a bijective function.

Theorem 4.1.6. *Each element in S_n can be written as a product of disjoint cycles in a unique way, up to reordering the cycles.*

Proof. Let $\sigma \in S_n$. Define an equivalence relation on $\{1, 2, ..., n\}$ by $i \sim j$ if there exists $l \in \mathbb{Z}$ such that $\sigma^l(i) = j$. It is not hard to check this defines an equivalence relation, which brings a partition of $\{1, 2, ..., n\}$ into equivalence classes. We take a representative from each class: $a_1, ..., a_k$.

Suppose $m_i = \min\{m > 0 | \sigma^m(a_i) = a_i\}$. The equivalence class represented by a_i then can be expressed by $\{a_i, \sigma(a_i), ..., \sigma^{m-1}(a_i)\}$, and we see σ permutes these elements in a cyclic manner. So we can write

$$\sigma = (a_1 \ \ \sigma(a_1) \ \ ... \ \ \sigma^{m_1-1}(a_1))...(a_k \ \ \sigma(a_k) \ \ ... \ \ \sigma^{m_k-1}(a_k))$$

which is a product of disjoint cycles.

If σ is written as a product of disjoint cycles, then for any $k \in \{1, 2, ..., n\}$, the number after k in the cycle that contains k has to be $\sigma(k)$, which implies the uniqueness up to reordering the cycles. □

Definition 4.1.7. Write $\sigma \in S_n$ as a product of disjoint cycles, and we list the lengths of the cycles in an increasing order:

$$1 \leq n_1 \leq n_2 \leq ... \leq n_r$$

so that $n_1 + n_2 + ... + n_r = n$. We define the **cycle type** of σ to be $(n_1, n_2, ..., n_r)$, or written as $n_1 + n_2 + ... + n_r$.

Remark 4.1.8. When we write an element in S_n as a product of disjoint cycles, we usually omit the cycle of length one. For example, we write $(1 \ \ 2 \ \ 3)$ instead of $(4)(1 \ \ 2 \ \ 3)$. But when writing the cycle type, we need to write down the cycles of length one, so $(1 \ \ 2 \ \ 3) \in S_4$ has cycle type $1 + 3$.

Example 4.1.9. *The cycle type of* $\sigma = (4 \ \ 3)(1 \ \ 5)(6 \ \ 2 \ \ 7) \in S_9$ *is expressed by* $1 + 1 + 2 + 2 + 3$.

We are interested in cycle types because of the following theorem:

Theorem 4.1.10. *Two elements in* S_n *are conjugate to each other if and only if they have the same cycle type.*

Proof. First, for a cycle $(a_1 \ \ ... \ \ a_k) \in S_n$, we can show that for any $\tau \in S_n$,

$$\tau(a_1 \ \ ... \ \ a_k)\tau^{-1} = (\tau(a_1) \ \ ... \ \ \tau(a_k))$$

Next, since each $\sigma \in S_n$ can be written as a product of disjoint cycles, if we apply the first step to each cycle, we see σ and $\tau\sigma\tau^{-1}$ have the same cycle type.

Conversely, if two elements σ_1, σ_2 have the same cycle type, then by the formula

$$\tau(a_1 \ \ ... \ \ a_k)\tau^{-1} = (\tau(a_1) \ \ ... \ \ \tau(a_k))$$

we can find a $\tau \in S_n$ such that $\sigma_1 = \tau\sigma_2\tau^{-1}$. □

Example 4.1.11. *Find some $\tau \in S_6$ such that $\tau(1 \ \ 3 \ \ 5)\tau^{-1} = (2 \ \ 4 \ \ 6)$.*

By the formula

$$\tau(1 \ \ 3 \ \ 5)\tau^{-1} = (\tau(2) \ \ \tau(4) \ \ \tau(6))$$

we can let $\tau(1) = 2$, $\tau(3) = 4$ and $\tau(5) = 6$. We also need to assign values to $\tau(2), \tau(4), \tau(6)$, but there are no restrictions, as long as

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

so we may let $\tau(2) = 1, \tau(4) = 3, \tau(6) = 5$, then $\tau = (1 \ \ 2)(3 \ \ 4)(5 \ \ 6)$

Exercise 4.1.12. *How many possibilities of $\tau \in S_n$ are there if $\tau(1 \ \ 3 \ \ 5)\tau^{-1} = (2 \ \ 4 \ \ 6)$ in S_6?*

Exercise 4.1.13. *Find a $\tau \in S_7$ such that $\tau(1 \ \ 2)(3 \ \ 4 \ \ 5)\tau^{-1} = (1 \ \ 3)(5 \ \ 6 \ \ 7)$.*

Corollary 4.1.14. *If N is a normal subgroup of S_n, then N consists of several conjugacy classes of S_n.*

4.2 Signature Functions and Alternating Groups

Lemma 4.2.1. *Every element of S_n can be written as a product of 2-cycles.*

Proof. We know each element in S_n can be written as a product of disjoint cycles, so it suffices to verify the statement for a cycle, which is true by the following identity:

$$(a_1 \ \ ... \ \ a_k) = (a_1 \ \ a_k)(a_1 \ \ a_{k-1})...(a_1 \ \ a_2)$$

□

Now define a homomorphism $\eta : S_n \longrightarrow GL_n(\mathbb{R})$ by sending the permutation $\sigma \in S_n$ to the $n \times n$ matrix whose j-th column is the unit vector $\vec{e}_{\sigma(j)}$. In other words, $\eta(\sigma)$ is the matrix with the ij entry to be

$$\begin{cases} 0, \text{ if } i \neq \sigma(j) \\ 1, \text{ if } i = \sigma(j) \end{cases}$$

Lemma 4.2.2. *$\eta : S_n \longrightarrow GL_n(\mathbb{R})$ defined above is an injective homomorphism.*

Proof. We will first prove it is a homomorphism. For any $\sigma, \tau \in S_n$, $\eta(\tau)$ sends $\vec{e}_j$ to $\vec{e}_{\tau(j)}$, and $\eta(\sigma)$ sends $\vec{e}_{\tau(j)}$ to $\vec{e}_{\sigma\circ\tau(j)}$, so $\eta(\sigma)\eta(\tau)$ sends $\vec{e}_j$ to $\vec{e}_{\sigma\circ\tau(j)}$.

On the other hand, $\eta(\sigma \circ \tau)$ sends $\vec{e}_j$ to $\vec{e}_{\sigma\circ\tau(j)}$ as well. We conclude $\eta(\sigma)\eta(\tau)$ and $\eta(\sigma \circ \tau)$ are the same matrix, i.e., $\eta(\sigma)\eta(\tau) = \eta(\sigma \circ \tau)$, η is a homomorphism.

It is injective since by the definition of η, it is easy to see different permutations correspond to different matrices.

□

Lemma 4.2.3. *If $\sigma \in S_n$, then* $\det(\eta(\sigma)) \in \{\pm 1\}$.

Proof. By the definition of η, we know $\eta(\sigma)$ is a matrix with exactly one entry to be 1 on each row and each column, and all the remaining entries are 0, so $\eta(\sigma)$ can be obtained from the identity matrix by a finite number of row-switching, and each time the determinant will change the sign but keep the absolute value, which implies the determinant of the identity matrix and $\eta(\sigma)$ differ at most by a factor of -1. □

Definition 4.2.4. The **signature** (also called **parity**) function is defined to be

$$\text{sgn} : S_n \xrightarrow{\eta} GL_n(\mathbb{R}) \xrightarrow{\det} \{\pm 1\} \subseteq \mathbb{R}^\times$$

The following proposition shows $\text{sgn} : S_n \longrightarrow \{\pm 1\}$ is surjective.

Proposition 4.2.5. *If $\sigma \in S_n$ is a 2-cycle, then* $\text{sgn}(\sigma) = -1$.

Proof. Follows directly from the definition of η. □

Proposition 4.2.6. *If $\sigma \in S_n$ is a k-cycle, then* $\text{sgn}(\sigma) = (-1)^{k-1}$

Proof. We know that if $\sigma = (a_1 \ \ldots \ a_k)$, then we can write

$$\sigma = (a_1 \ \ a_k)(a_1 \ \ a_{k-1})\ldots(a_1 \ \ a_2)$$

sgn is a homomorphism, so

$$\text{sgn}(\sigma) = \text{sgn}((a_1 \ \ a_{k-1}))\ldots \text{sgn}((a_1 \ \ a_2)) = (-1)^{k-1}$$

□

Example 4.2.7. *If* $\sigma = (1\ \ 2)(3\ \ 4\ \ 5)(6\ \ 7\ \ 8\ \ 9) \in S_{10}$*, compute* $\operatorname{sgn}(\sigma)$*.*

$$\operatorname{sgn}(\sigma) = \operatorname{sgn}((1\ \ 2))\operatorname{sgn}((3\ \ 4\ \ 5))\operatorname{sgn}((6\ \ 7\ \ 8\ \ 9)) = (-1)(+1)(-1) = +1$$

Remark 4.2.8. We see ths signature of a permutation depends on the cycle type. Two elements of the same cycle type will have the same signature.

Definition 4.2.9. $\sigma \in S_n$ is called an **odd permutation** if $\operatorname{sgn}(\sigma) = -1$; it is called an **even permutation** if $\operatorname{sgn}(\sigma) = +1$.

Definition 4.2.10. The subgroup of S_n defined by $A_n = \ker(\operatorname{sgn})$ is called the **alternating subgroup** of n elements. It consists of all the even permutations in S_n.

By the First Isomorphism Theorem, $S_n/A_n \cong \{\pm 1\}$. This implies the order of A_n is $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$. Also this index 2 condition implies A_n is a normal subgroup of S_n.

Definition 4.2.11. A group G is **simple** if it has no proper normal subgroups, i,e., its only normal subgroups are $\{1\}$ and G.

Example 4.2.12. *A_4 is not a simple group, since it has a proper normal subgroup*

$$K = \{id, (1\ \ 2)(3\ \ 4), (1\ \ 3)(2\ \ 4), (1\ \ 4)(2\ \ 3)\}$$

Remark 4.2.13. A_4 is isomorphic to the group of all rotational symmetries of a tetrahedron.

Theorem 4.2.14. *For any $n \geq 5$, A_n is a simple group.*

Proof. Step 1. For $n \geq 5$, A_n is generated by the set of 3-cycles.

This is because each element in A_n is a product of even number of 2-cycles, and we can put 2-cycles in pairs to obtain 3-cycles by:

$$\begin{cases} (a\ \ b)(a\ \ c) = (a\ \ c\ \ b) \text{ if } a, b, c \text{ are distinct} \\ (a\ \ b)(c\ \ d) = (a\ \ b\ \ c)(b\ \ c\ \ d) \text{ if } a, b, c, d \text{ are distinct} \end{cases}$$

Step 2. If $n \geq 5$, all 3-cycles are conjugate in A_n.

If σ and σ' are two 3-cycles, we know they are conjugate in S_n, so there exists $\tau \in S_n$ such that $\sigma' = \tau\sigma\tau^{-1}$.

If $\tau \in A_n$, done.

If $\tau \notin A_n$, then assume $\sigma = (a_1 \;\; a_2 \;\; a_3)$. Choose $a_4, a_5 \in \{1, 2, ..., n\}$ such that a_1, a_2, a_3, a_4, a_5 are all distinct. Let $\tau' = \tau(a_4 \;\; a_5)$, we have

$$\begin{aligned}\tau'\sigma\tau'^{-1} &= (\tau(a_4 \;\; a_5))(a_1 \;\; a_2 \;\; a_3)(\tau(a_4 \;\; a_5))^{-1} \\ &= \tau(a_4 \;\; a_5)(a_1 \;\; a_2 \;\; a_3)(a_4 \;\; a_5)\tau^{-1} \\ &= \tau\sigma\tau^{-1} \\ &= \sigma^{-1}\end{aligned}$$

and $\text{sgn}(\tau') = -\tau(\tau) = +1$, so $\tau' \in S_n$.

Step 3. If $n \geq 5$, N is a nontrivial normal subgroup of A_n, then N contains a 3-cycle.

Let $\sigma \in N$ with $\sigma \neq id$.

Case (a). If σ contains a cycle of length ≥ 4, i.e., $\sigma = (x_1 \;\; ... \;\; x_r)\tau$, $r \geq 4$, and τ is disjoint from $x_1 \;\; ... \;\; x_r$, then

$$\sigma^{-1}(x_1 \;\; x_2 \;\; x_3)^{-1}\sigma(x_1 \;\; x_2 \;\; x_3) = (x_2 \;\; x_3 \;\; x_r) \in N$$

Case (b). If σ contains at least two cycles of length 3, i.e., $\sigma = (x_1 \;\; x_2 \;\; x_3)(x_4 \;\; x_5 \;\; x_6)\tau$ and τ is disjoint from $(x_1 \;\; x_2 \;\; x_3)$ and $(x_4 \;\; x_5 \;\; x_6)$, then

$$\sigma^{-1}(x_1 \;\; x_2 \;\; x_4)^{-1}\sigma(x_1 \;\; x_2 \;\; x_4) = (x_1 \;\; x_2 \;\; x_4 \;\; x_3 \;\; x_6) \in N$$

We then apply Case (a) to $(x_1 \;\; x_2 \;\; x_4 \;\; x_3 \;\; x_6)$ to obtain a 3-cycle in A_n.

Case (c). If σ contains exactly one cycle of length 3, i.e., $\sigma = (x_1 \;\; x_2 \;\; x_3)\tau$, where τ is p product of disjoint cycles of length 2, all of which are disjoint from $(x_1 \;\; x_2 \;\; x_3)$. Then

$$\sigma^2 = ((x_1 \;\; x_2 \;\; x_3)\tau)^2 = (x_1 \;\; x_2 \;\; x_3)^2 = (x_1 \;\; x_3 \;\; x_2)$$

Case (d). If σ only contains 2-cycles, i.e. $\sigma = (x_1 \;\; x_2)(x_3 \;\; x_4)\tau$, and $(x_1 \;\; x_2), (x_3 \;\; x_4), \tau$ are all disjoint.

Take $x_5 \in \{1, 2, ..., n\} \setminus \{x_1, x_2, x_3, x_4\}$, then

$$\sigma^{-1}(x_1 \;\; x_2 \;\; x_3)^{-1}\sigma(x_1 \;\; x_2 \;\; x_3) = (x_1 \;\; x_4)(x_2 \;\; x_3)$$

$$(x_1 \;\; x_5 \;\; x_2)(x_1 \;\; x_4)(x_2 \;\; x_3)(x_1 \;\; x_5 \;\; x_2)^{-1} = (x_1 \;\; x_3)(x_4 \;\; x_5)$$

$$(x_1 \;\; x_4)(x_2 \;\; x_3)(x_1 \;\; x_3)(x_4 \;\; x_5) = (x_1 \;\; x_2 \;\; x_3 \;\; x_4 \;\; x_5)$$

We then apply Case (a) to $(x_1 \;\; x_2 \;\; x_4 \;\; x_3 \;\; x_6)$ to obtain a 3-cycle in A_n.

Step 4. Now we can conclude A_n is simple for $n \geq 5$. If N is a nontrivial normal subgroup of A_n, by Step 3, N contains a 3-cycle. By Step 2, all 3-cycles in A_n are conjugate, so N contains all the 3-cycles. By Step 1, each element in A_n can be written as a product of 3-cycles, so $A_n = N$. We thus conclude A_n has no proper normal subgroups.

□

4.3 Isometry on Euclidean Spaces

In the following discussion, we will take the standard basis $(\vec{e}_1, ..., \vec{e}_n)$ for the n-dimensional real vector space $\mathbb{R}^n$.

Definition 4.3.1. The **dot product** of two vectors $\vec{u}, \vec{v} \in \mathbb{R}^n$ is

$$< \vec{u}, \vec{v} >= \vec{u}^T \vec{v}$$

Definition 4.3.2. The **length** of $\vec{v} \in \mathbb{R}$ is

$$|\vec{v}| = \sqrt{< \vec{v}, \vec{v} >}$$

Definition 4.3.3. The **distance** between two vectors $\vec{u}, \vec{v}$ of $\mathbb{R}^n$ is the length $|\vec{u} - \vec{v}|$.

Definition 4.3.4. An **isometry** of $\mathbb{R}^n$ is a distance preserving map $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$, i.e., for any $\vec{u}, \vec{v} \in \mathbb{R}^n$, $|f(\vec{u}) - f(\vec{v})| = |\vec{u} - \vec{v}|$

Example 4.3.5. *Each $\vec{a} \in \mathbb{R}^n$ induces a translation map:*

$$t_{\vec{a}} : \mathbb{R}^n \longrightarrow \mathbb{R}^n$$

$$\vec{u} \mapsto \vec{u} + \vec{a}$$

This is an isometry since for any $\vec{u}, \vec{v} \in \mathbb{R}^n$:

$$|t_{\vec{a}}(\vec{u}) - t_{\vec{a}}(\vec{v})| = |(\vec{u} + \vec{a}) - (\vec{v} + \vec{a})| = |\vec{u} - \vec{v}|$$

Proposition 4.3.6. *Composition of isometries on $\mathbb{R}^n$ is an isometry on $\mathbb{R}^n$.*

Proof. If f_1, f_2 are isometries on $\mathbb{R}^n$, then for any $\vec{u}, \vec{v} \in \mathbb{R}^n$:

$$|f_1 \circ f_2(\vec{u}) - f_1 \circ f_2(\vec{v})| = |f_2(\vec{u}) - f_2(\vec{v})| = |\vec{u} - \vec{v}|$$

□

Definition 4.3.7. $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ is a **linear operator** if:

1. for any $\vec{u}, \vec{v} \in \mathbb{R}^n$, $T(\vec{u} + \vec{v}) = T(\vec{u}) + T(\vec{v})$
2. for any $c \in \mathbb{R}, \vec{u} \in \mathbb{R}^n$, $T(c\vec{u}) = cT(\vec{u})$

Definition 4.3.8. $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ is an **orthogonal linear operator** if it is a linear operator such that for any $\vec{u}, \vec{v} \in \mathbb{R}^n$, $< T(\vec{u}), T(\vec{v}) >=< \vec{u}, \vec{v} >$

Lemma 4.3.9. *An orthogonal linear operator preserves length of vectors.*

Proof. If $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ is an orthogonal linear operator, then for any $\vec{u} \in \mathbb{R}^n$:

$$|T(\vec{u})| = \sqrt{< T(\vec{u}), T(\vec{u}) >} = \sqrt{< \vec{u}, \vec{u} >} = |\vec{u}|$$

□

Corollary 4.3.10. *An orthogonal linear operator is an isometry preserving* $\vec{0}$.

Proof. If $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ is an orthogonal linear operator, then for any $\vec{u}, \vec{v} \in \mathbb{R}^n$,

$$|T(\vec{u}) - T(\vec{v})| = |T(\vec{u} - \vec{v})| = |\vec{u} - \vec{v}|$$

so it is an isometry. $T(\vec{0}) = \vec{0}$ since it is a linear operator. □

Recall it has been known in Linear Algebra that linear operators can be represented by matrices when basis is fixed. In particular, we can represent orthogonal linear operators by matrices.

Definition 4.3.11. A $n \times n$ invertible matrix A is **orthogonal** if $A^t = A^{-1}$. The set of all $n \times n$ orthogonal matrices, denoted by $O_n(\mathbb{R})$, forms a subgroup of $GL_n(\mathbb{R})$, called the **orthogonal linear group**.

Proposition 4.3.12. *Fix an standard basis* $(e_1, e_2, ..., e_n)$ *for* $\mathbb{R}^n$. *Each orthogonal linear operator* $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ *is represented by an orthogonal matrix* $A \in O_n(\mathbb{R})$, *and conversely, each* $A \in O_n(\mathbb{R})$ *induces an orthogonal linear operator* $T(\vec{v}) = A\vec{v}$.

Proof. If $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ is an orthogonal linear operator, let A be the $n \times n$ matrix whose i-th colume is the coordinates of $T(e_i)$. We need to show A is an orthogonal matrix.

Since T is an orthogonal linear operator, it preserves dot product and length, so

$$|T(\vec{e}_1)| = |T(\vec{e}_2)| = ... = |T(\vec{e}_n)| = 1$$

and

$$< T(\vec{e}_i), T(\vec{e}_j) >=< \vec{e}_i, \vec{e}_j >= \begin{cases} 1 \text{ if } i = j \\ 0 \text{ if } i \neq j \end{cases}$$

So $(T(\vec{e}_1), ..., T(\vec{e}_1))$ forms an orthonormal basis of $\mathbb{R}^n$. The (i, j)-th entry of $A^T A$ is

$$T(\vec{e}_i)^t T(\vec{e}_j) =< T(\vec{e}_i), T(\vec{e}_j) >= \begin{cases} 1 \text{ if } i = j \\ 0 \text{ if } i \neq j \end{cases}$$

we see $A^t A = I_n$, so A is an orthogonal matrix.

Conversely, if A is an orthogonal matrix, let $T_A : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ be

$$T_A(\vec{x}) = A\vec{x}$$

then for any $\vec{u}, \vec{v} \in \mathbb{R}^n$,

$$< T_A(\vec{u}), T_A(\vec{v}) >=< A\vec{u}, A\vec{v} >= (A\vec{u})^t A\vec{u} = \vec{u}^t A^t A\vec{v} = \vec{u}^t \vec{v} =< \vec{u}, \vec{v} >$$

This verifies T_A is an orthogonal linear operator. □

Theorem 4.3.13. *The following conditions on a map $f : \mathbb{R} \longrightarrow \mathbb{R}$ are equivalent:*

1. *f is an isometry that fixes $\vec{0}$.*
2. *f preserves dot product.*
3. *f is an orthogonal linear operator.*
4. *Fix a standard basis $(e_1, e_2, ..., e_n)$ for $\mathbb{R}^n$, then $f(\vec{v}) = A\vec{v}$ for some $A \in O_n(\mathbb{R})$.*

Proof. We have shown (3) $\iff$ (4) and (3)$\Longrightarrow$(1), so it suffices to show (1)$\Longrightarrow$(2) and (2)$\Longrightarrow$(3).

(1)$\Longrightarrow$(2): If f is an isometry such that $f(\vec{0}) = \vec{0}$, then for any $\vec{u}, \vec{v} \in \mathbb{R}^n$:

$$\begin{aligned} < f(\vec{u}), f(\vec{u}) > &=< f(\vec{u}) - f(\vec{0}), f(\vec{u}) - f(\vec{0}) > \\ &= |f(\vec{u}) - f(\vec{0})|^2 \\ &= |\vec{u} - \vec{0}|^2 \\ &= |\vec{u}|^2 \\ &=< \vec{u}, \vec{u} > \end{aligned}$$

Similarly we can obtain $< f(\vec{v}), f(\vec{v}) >=< \vec{v}, \vec{v} >$.

$$\begin{aligned} < f(\vec{u}) - f(\vec{v}), f(\vec{u}) - f(\vec{v}) > &= |f(\vec{u}) - f(\vec{v})|^2 \\ &= |\vec{u} - \vec{v}|^2 \\ &=< \vec{u} - \vec{v}, \vec{u} - \vec{v} > \end{aligned}$$

Expanding both sides we have

$$\begin{aligned} &< f(\vec{u}), f(\vec{u}) > - < f(\vec{v}), f(\vec{u}) > - < f(\vec{u}), f(\vec{v}) > + < f(\vec{v}), f(\vec{v}) > \\ &= < \vec{u}, \vec{u} > - < \vec{v}, \vec{u} > - < \vec{u}, \vec{v} > + < \vec{v}, \vec{v} > \end{aligned}$$

We therefore conclude

$$< f(\vec{u}), f(\vec{v}) >=< \vec{u}, \vec{v} >$$

which shows that f preserves dot product.

(2)$\Longrightarrow$(3): Given a map $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ preserving dot product, we only need to show it is linear if we want to show it's an orthogonal linear operator.

Claim: $\vec{u}, \vec{v} \in \mathbb{R}^n$. If $< \vec{u}, \vec{u} >=< \vec{u}, \vec{v} >=< \vec{v}, \vec{v} >$, then $\vec{u} = \vec{v}$.

Proof of Claim: If $< \vec{u}, \vec{u} >=< \vec{u}, \vec{v} >=< \vec{v}, \vec{v} >$, then

$$|\vec{u} - \vec{v}|^2 =< \vec{u} - \vec{v}, \vec{u} - \vec{v} >=< \vec{u}, \vec{u} > -2 < \vec{u}, \vec{v} > + < \vec{v}, \vec{v} >= 0$$

So we conclude $\vec{u} = \vec{v}$.

Now let $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ be a map preserving dot product. We need to show: for any $\vec{u}, \vec{v} \in \mathbb{R}^n$, $c \in \mathbb{R}$

$$f(\vec{u} + \vec{v}) = f(\vec{u}) + f(\vec{v}), f(c\vec{u}) = cf(\vec{u})$$

In order to show $f(\vec{u}+\vec{v}) = f(\vec{u}) + f(\vec{v})$, by the claim, we need to show

$$< f(\vec{u}+\vec{v}), f(\vec{u}+\vec{v}) >=< f(\vec{u}+\vec{v}), f(\vec{u})+f(\vec{v}) >=< f(\vec{u})+f(\vec{v}), f(\vec{u})+f(\vec{v}) >$$

This can be shown by the following computation:

$$\begin{aligned} < f(\vec{u}+\vec{v}), f(\vec{u})+f(\vec{v}) > &=< f(\vec{u}), f(\vec{u}+\vec{v}) > + < f(\vec{u}+\vec{v}), f(\vec{v}) > \\ &=< \vec{u}+\vec{v}, \vec{u} > + < \vec{u}+\vec{v}, \vec{v} > \\ &=< \vec{u}+\vec{v}, \vec{u}+\vec{v} > \end{aligned}$$

$$< f(\vec{u}+\vec{v}), f(\vec{u}+\vec{v}) >=< \vec{u}+\vec{v}, \vec{u}+\vec{v} >$$

$$\begin{aligned} & < f(\vec{u})+f(\vec{v}), f(\vec{u})+f(\vec{v}) > \\ &= < f(\vec{u}), f(\vec{u}) > + < f(\vec{u}), f(\vec{v}) > + < f(\vec{v}), f(\vec{u}) > + < f(\vec{v}), f(\vec{v}) > \\ &= < \vec{u}, \vec{u} > + < \vec{u}, \vec{v} > + < \vec{v}, \vec{u} > + < \vec{v}, \vec{v} > \\ &= < \vec{u}+\vec{v}, \vec{u}+\vec{v} > \end{aligned}$$

$f(c\vec{u}) = cf(\vec{u})$ can be shown in a similar way. □

Corollary 4.3.14. *Every isometry $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ is the composition of an orthogonal linear operator and a translation.*

Proof. $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ is an isometry. Define the translation

$$t_{-f(\vec{0})} : \mathbb{R}^n \longrightarrow \mathbb{R}^n$$

$$\vec{u} \mapsto \vec{u} - f(\vec{0})$$

Then the composition $t_{-f(\vec{0})} \circ f$ is an isometry on $\mathbb{R}^n$ such that

$$t_{-f(\vec{0})} \circ f(\vec{0}) = f(\vec{0}) - f(\vec{0}) = \vec{0}$$

so by Theorem 4.3.13, $t_{-f(\vec{0})} \circ f = \phi$ is an orthogonal linear operator, then

$$f = t^{-1}_{-f(\vec{0})} \circ \phi = t_{f(\vec{0})} \circ \phi$$

is a composition of an orthogonal linear operator and a translation. □

Corollary 4.3.15. *An isometry $f : \mathbb{R} \longrightarrow \mathbb{R}$ is a bijection.*

Proof. By the previous Corollary, f is a composition of an orthogonal linear operator and a translation, each of which is bijective, so f is also bijective. □

Corollary 4.3.16. *The set of all isometries on $\mathbb{R}^n$ with composition of functions form a group M_n, called the* ***group of isometry*** *on $\mathbb{R}^n$.*

Exercise 4.3.17. *Verify M_n is a group.*

Lemma 4.3.18. *If $t_{\vec{a}}$ is a translation and ϕ is an orthogonal linear operator, then*

$$\phi \circ t_{\vec{a}} = t_{\phi(\vec{a})} \circ \phi$$

Proof. For any $\vec{v} \in \mathbb{R}^n$,

$$\phi \circ t_{\vec{a}}(\vec{v}) = \phi(\vec{v} + \vec{a}) = \phi(\vec{v}) + \phi(\vec{a}) = t_{\phi(\vec{a})} \circ \phi(\vec{v})$$

□

Exercise 4.3.19. *Let T_n be the set of translations on $\mathbb{R}^n$, O_n be the set of orthogonal linear operators on $\mathbb{R}^n$. Prove that O_n is a subgroup of M_n and T_n is a normal subgroup of M_n.*

Exercise 4.3.20. *Show that $O_n \cap T_n = \{id\}$, and show that each $f \in M_n$ can be decomposed as $f = t \circ \phi$ where $t \in T_n, \phi \in O_n$ in a unique way.*

Proposition 4.3.21. *The function $\pi : M_n \longrightarrow O_n$ given by $\pi(f) = t_{-f(\vec{0})} \circ f$ is a surjective homomorphism.*

Proof. It is surjective since for any $\phi \in O_n$, $\pi(\phi) = \phi$.

It is a homomorphism: for any $f, g \in M_n$, we can write $f = t_{\vec{a}} \circ \phi$ and $g = t_{\vec{b}} \circ \psi$, where $t_{\vec{a}}, t_{\vec{b}} \in T_n$ and $\phi, \psi \in O_n$. We see $\pi(f) = \phi$ and $\pi(g) = \psi$.

$$\pi(f \circ g) = \pi(t_{\vec{a}} \circ \phi \circ t_{\vec{b}} \circ \psi) = \pi(t_{\vec{a}} \circ t_{\phi(\vec{b})} \circ \phi \circ \psi) = \phi \circ \psi = \pi(f)\pi(g)$$

□

We see that:

$$\ker \pi = \{t_{\vec{a}} \circ \phi \in M_n | \pi(t_{\vec{a}} \circ \phi) = id\} = \{t_{\vec{a}} \circ \phi \in M_n | \phi = id\} = T_n$$

So by First Isomorphism Theorem,

$$M_n/T_n \cong O_n$$

4.4 Isometry on the Plane

Based on the general discussion in the previous chapter, we know that each isometry of $\mathbb{R}^2$ is a composition of an orthogonal linear operator with a translation.

Also we know orthogonal linear operators are in one-to-one correspondence with the orthogonal matrices $O_n(\mathbb{R})$ once a standard basis is given.

Exercise 4.4.1. *A is a real $n \times n$ matrix. $A \in O_n(\mathbb{R})$ if and only if the rows (columns) of A are unit vectors that are pairwisely perpendicular.*

In $O_n(\mathbb{R})$, there is a subgroup $SO_n(\mathbb{R}) = \{A \in O_n(\mathbb{R}) | \det(A) = 1\}$. $SO_n(\mathbb{R})$ is the kernel of the restriction of the determinant map to $O_n(\mathbb{R})$.

Exercise 4.4.2. *The determinant of an orthogonal matrix can only be ± 1.*

The First Isomorphism Theorem implies

$$O_n(\mathbb{R})/SO_n(\mathbb{R}) \cong \{\pm 1\}$$

and it follows $[O_n(\mathbb{R}) : SO_n(\mathbb{R})] = 2$, which tells us $SO_n(\mathbb{R})$ is a normal subgroup of $O_n(\mathbb{R})$. Let r be the $n \times n$ matrix with entries

$$r_{ij} = \begin{cases} 1, \text{ if } 1 \leq i = j \leq n-1 \\ -1, \text{ if } i = j = n \\ 0, \text{ if } i \neq j \end{cases}$$

then

$$O_n(\mathbb{R}) = SO_n(\mathbb{R}) \sqcup (SO_n(\mathbb{R}))r$$

From now on we will concentrate on the case $n = 2$.

Lemma 4.4.3. *Every element in $SO_2(\mathbb{R})$ can be written as*

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

for some $\theta \in \mathbb{R}$.

Proof. Assume $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SO_2$, then $det(\begin{bmatrix} a & b \\ c & d \end{bmatrix}) = ad - bc = 1$, so

$$\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{T} = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$$

So $a = d$ and $b = -c$, the matrix becomes $\begin{bmatrix} a & -c \\ c & a \end{bmatrix}$, with $a^2 + c^2 = 1$. We know for a pair of real numbers a, c satisfying $a^2 + c^2 = 1$, the angle θ whose terminal edge passing through (a, c) has $\cos\theta = a$ and $\sin\theta = c$, hence the matrix can be written as $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ □

Proposition 4.4.4. *The map $\rho_\theta : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ defined by*

$$\begin{bmatrix} x \\ y \end{bmatrix} \mapsto \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

is the rotation of angle θ around origin.

Proof. We can write

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} R\cos\alpha \\ R\sin\alpha \end{bmatrix}$$

by polar coordinates.

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} R\cos\alpha \\ R\sin\alpha \end{bmatrix} = \begin{bmatrix} R\cos\alpha\cos\theta - R\sin\alpha\sin\theta \\ R\cos\alpha\sin\theta + R\sin\alpha\cos\theta \end{bmatrix} = \begin{bmatrix} R\cos(\alpha+\theta) \\ R\sin(\alpha+\theta) \end{bmatrix}$$

□

Proposition 4.4.5. *The map $r : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ defined by*

$$\begin{bmatrix} x \\ y \end{bmatrix} \mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ -y \end{bmatrix}$$

is the reflection with respect to x-axis.

Combining the above discussion we conclude:

Theorem 4.4.6. *Let m be an isometry of the plane, then $m = t_{\vec{a}}\rho_\theta$ or $m = t_{\vec{a}}\rho_\theta r$, where $\vec{a} \in \mathbb{R}^2$, ρ_θ and r are defined as above.*

Lemma 4.4.7. *The following identities hold:*

1. $\rho_\theta t_{\vec{a}} = t_{\rho_\theta(\vec{a})}\rho_\theta$
2. $r t_{\vec{a}} = t_{r(\vec{a})} r$
3. $r\rho_\theta = \rho_{-\theta} r$
4. $t_{\vec{a}} t_{\vec{b}} = t_{\vec{a}+\vec{b}}$, $\rho_\theta \rho_\eta = \rho_{\theta+\eta}$, $r^2 = id$

Geometrically, there is a simpler description of isometries of the plane.

Theorem 4.4.8. *Every isometry of the plane has one of the following forms:*

1. *Translation along $\vec{a} \in \mathbb{R}^2$*
2. *Rotation through a nonzero angle about a point*
3. *Reflection along a line l*
4. *Glide Reflection: reflection along a line l, followed by a translation along a nonzero vector parallel to l*

The first two are orientation preserving and the last two are orientation reversing.

Proof. If the isometry is of form $t_{\vec{a}}$, then it is a translation.

If the isometry is of form $t_{\vec{a}}\rho_\theta$, we are going to show it is a rotation through an angle θ about some point $\vec{p}$: by assumption, $\theta \neq 0$, so the matrix

$$id - \rho_\theta = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} = \begin{bmatrix} 1-\cos\theta & \sin\theta \\ -\sin\theta & 1-\cos\theta \end{bmatrix}$$

is invertible. Let $\vec{p} = (id - \rho_\theta)^{-1}\vec{a}$, then $\vec{a} = (id - \rho_\theta)\vec{p} = \vec{p} - \rho_\theta(\vec{p})$, we get

$$t_{\vec{a}}\rho_\theta = t_{\vec{p}-\rho_\theta(\vec{p})}\rho_\theta = t_{\vec{p}} t_{\rho_\theta(-\vec{p})}\rho_\theta = t_{\vec{p}}\rho_\theta t_{-\vec{p}}$$

and it is geometrically clear that $t_{\vec{p}}\rho_\theta t_{-\vec{p}}$ is the rotation about $\vec{p}$ of angle θ. □

If the isometry is of form $\rho_\theta r$, then

$$\rho_\theta r = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}$$

and

$$\begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} \begin{bmatrix} R\cos\alpha \\ R\sin\alpha \end{bmatrix} = \begin{bmatrix} R\cos(\theta-\alpha) \\ R\sin(\theta-\alpha) \end{bmatrix}$$

So $\rho_\theta r$ is the reflection along the line through origin with angle $\frac{\theta}{2}$ to x-axis.

If the isometry is of form $t_{\vec{a}}\rho_\theta r$, then it is a reflection along a line l passing through origin followed by a translation along $\vec{a}$. Decompose $\vec{a} = \vec{a}_1 + \vec{a}_2$ such that $\vec{a}_1$ is parallel to l and $\vec{a}_2$ is orthogonal to l. Then

$$t_{\vec{a}}\rho_\theta r = t_{\vec{a}_1}(t_{\vec{a}_2}\rho_\theta r)$$

and geometrically, $t_{\vec{a}_2}\rho_\theta r$ is the reflection along the line l', which is obtained by translating l along $\frac{1}{2}\vec{a}_2$. Note $\vec{a}_1$ is parallel to l', we conclude this corresponds to the last case in the statement of the theorem.

4.5 Dihedral Groups

Definition 4.5.1. n is a positive integer. Let $\rho = \rho_{\frac{2\pi}{n}}$. The **dihedral group** is the subgroup of O_2 defined by

$$D_n = \{\rho^i r^j \in O_2 | 0 \le i \le n-1, 0 \le j \le 1\}$$

Exercise 4.5.2. $\rho^n = 1$, $r^2 = 1$, $r\rho = \rho^{-1}r$

Proof. By direct computation. □

Corollary 4.5.3. *$r\rho^i r = \rho^{-i}$ for any $i \in \mathbb{Z}$*

Exercise 4.5.4. *Show that D_n is a subgroup of O_2.*

Geometrically, D_n is the group of symmetries of a regular n-gon. Each element of D_n permutes the n vertices of the n-gon, we can view D_n as a subgroup of S_n.

Example 4.5.5. *D_3 has 6 elements, same as S_3, and D_3 can be viewed as a subgroup of S_3, we get $D_3 \cong S_3$.*

Example 4.5.6. $D_1 = \{1, r\} \cong C_2$, $D_2 = \{1, \rho_\pi, r, \rho_\pi r\} \cong C_2 \times C_2 \cong K_4$.

4.6 Groups Actions

Definition 4.6.1. G is a group, and X is a set. A **group action** (also called **group operation**) of G on X is a map

$$G \times X \longrightarrow X$$

$$(g, x) \mapsto g.x$$

satisfying:
(1). $1.x = x$ for any $x \in X$
(2). $g_1.(g_2.x) = (g_1 g_2).x$ for any $g_1, g_2 \in G$, any $x \in X$.

We see from the definition that when a group action of G on X is given, each $g \in G$ induces a function $\tau_g : X \longrightarrow X$ sending x to $g.x$

Proposition 4.6.2. *If G acts on X, then any $g \in G$ induces a bijection:*

$$\tau_g : X \longrightarrow X$$

$$x \mapsto g.x$$

Proof. We need to verify τ_g is bijective, which can be done by verifying $\tau_{g^{-1}}$ is the inverse function of τ_g.

$$\tau_g \circ \tau_{g^{-1}}(x) = g.(g^{-1}.x) = (gg^{-1}).x = 1.x = x$$

$$\tau_{g^{-1}} \circ \tau_g(x) = g^{-1}.(\tau.x) = (g^{-1}g).x = 1.x = x$$

□

Example 4.6.3. *S_n acts on $X = \{1, 2, ..., n\}$ in a natural way: $\sigma \in S_n$ acts on $k \in X$ by $\sigma.k = \sigma(k)$*

Example 4.6.4. *G is a group, then G can act on itself by left multiplication: $g.x = gx$*

Example 4.6.5. *$GL_n(\mathbb{R})$ acts on $\mathbb{R}^n$ by matrix multiplication:*

$$GL_n(\mathbb{R}) \times \mathbb{R}^n \longrightarrow \mathbb{R}^n$$

$$(A, \vec{u}) \mapsto A\vec{u}$$

Example 4.6.6. *A group G acts on itself by conjugation: $g.x = gxg^{-1}$*

Definition 4.6.7. G is a group acting on a set X, and $x \in X$. The **orbit** of x is defined to be

$$O(x) = \{y \in X | g.x = y \text{ for some } g \in G\}$$

Lemma 4.6.8. *G acts on X. The relation on X defined by $x \sim y$ if $y = g.x$ for some $g \in G$ is an equivalence relation, and each orbit is an equivalence class.*

Proof. (i). For any $x \in X$, $1.x = x$, so $x \sim x$

(ii). If $x \sim y$, then $y = g.x$ for some $g \in G$, $x = 1.x = (g^{-1}g).x = g^{-1}.(g.x) = g^{-1}.y$, so $y \sim x$

(iii). If $x \sim y$ and $y \sim z$, then there exist $g_1, g_2 \in G$ such that $y = g_1.x$ and $z = g_2.y$, so $z = g_2.(g_1.x) = (g_1g_2).x$, $x \sim z$

We can thus conclude it is an equivalence relation. And it follows directly by definition that each equivalence class is an orbit. □

Corollary 4.6.9. *The orbits form a partition of X.*

Example 4.6.10. *In the example of $GL_n(\mathbb{R})$ acting on $\mathbb{R}^n$ by matrix multiplication, there are two orbits: $\mathbb{R}^n \setminus \{\vec{0}\}$ and $\{\vec{0}\}$.*

$\{\vec{0}\}$ is an orbit since for any $A \in GL_n(\mathbb{R})$, $A.\vec{0} = \vec{0}$

$\mathbb{R}^n \setminus \{\vec{0}\}$ is the only other orbit since for any $\vec{v} \neq \vec{0}$, we can extend $\vec{v}$ to a basis $(\vec{v}_1 = \vec{v}, \vec{v}_2, ..., \vec{v}_n)$. Then let the matrix $B \in GL_n(\mathbb{R})$ be the one whose i-th column is $\vec{v}_i$ for $1 \leq i \leq n$, we see that $\vec{v} = B.\vec{e}_1$, so $O(\vec{e}_1) = \mathbb{R}^n \setminus \{\vec{0}\}$ is an orbit.

Definition 4.6.11. A group G acts on a set X. If there is only one orbit for this action, we say the action is **transitive**.

Example 4.6.12. *G acting on itself by left multiplication is a transitive action: for any $x \in G$, let $g = x \in G$, then $x = g.1$, $x \in O(1)$, so there is only one orbit.*

Lemma 4.6.13. *An action of G on X is transitive if and only if for any $x \in X, y \in X$, there exists $g \in G$ such that $y = g.x$*

Proof. if G acts transitively on X, then there is only one orbit, we get $O(x) = O(y)$, in particular $y \in O(y) = O(x)$, so there exists $g \in G$ such that $y = g.x$

Conversely, for any $x \in X, y \in X$, if $x = g.y$ for some $g \in G$, then $O(x) = O(y)$, so there is only one orbit. □

Definition 4.6.14. G acts on X. Define the **stabiliser** of $x \in X$ to be

$$G_x = \{g \in G | g.x = x\}$$

Proposition 4.6.15. *G acts on X, and $x \in X$, then G_x is a subgroup of G.*

Proof. (1). If $g, g' \in G_x$, $(gg').x = g.(g'.x) = g.x = x$, so $gg' \in G_x$

(2). $1.x = x$, so $1 \in G_x$

(3). If $g \in G_x$, then $g.x = x \Longrightarrow g^{-1}.(g.x) = g^{-1}.x \Longrightarrow (g^{-1}g).x = g^{-1}.x \Longrightarrow 1.x = g^{-1}.x \Longrightarrow g^{-1} \in G_x$ □

Example 4.6.16. *G acts on G by left multiplication, then for any $x \in G$, $G_x = \{g \in G | gx = x\} = \{1\}$*

Example 4.6.17. *G acts on G by conjugation. Each orbit $O(x) = \{gxg^{-1} \in G | g \in G\}$ is called a **conjugacy class** of G.*

*$G_x = \{g \in G | gxg^{-1} = x\}$ is called the **normaliser** of x.*

Proposition 4.6.18. *G is a group acting on X. $x \in X$, $g_1, g_2 \in G$. Then $g_1.x = g_2.x$ if and only if $g_1 G_x = g_2 G_x$*

Proof. $g_1.x = g_2.x \iff g_2^{-1}.(g_1.x) = g_2^{-1}.(g_2.x) \iff (g_2^{-1}g_1).x = x \iff g_2^{-1}g_1 \in G_x \iff g_1 G_x = g_2 G_x$ □

Exercise 4.6.19. *G is a group acting on X. $x, x' \in X$ and $g \in G$ such that $x' = g.x$. Prove*

$$G_{x'} = gG_xg^{-1} = \{ghg^{-1} | h \in G_x\}$$

Proposition 4.6.20. *X is a set, $P(X)$ is the group of bijections $X \longrightarrow X$ with composition of functions. G is a group. Then there is a one-to-one correspondence between the groups actions of G on X and homomorphisms $G \longrightarrow P(X)$.*

Proof. If there is a G-action on X, then we can define a homomorphism

$$G \longrightarrow P(X)$$

where $\Phi(g) : X \longrightarrow X$ is defined by $\Phi(g)(x) = g.x$ (It is left as an exercise to check ϕ is a homomorphism.)

Conversely, given a homomorphism $\Phi : G \longrightarrow P(X)$, we can define a G-action on X by $g.x = \Phi(g)(x)$ (It is also left as an exercise to check this is a group action)

□

4.7 Applications of Group Actions

Theorem 4.7.1. *(The Counting Formula) G is a finite group acting on a set X. For each $x \in X$, let G_x be the stabiliser of x and $O(x)$ be the orbit of x. Then:*

$$|G| = |G_x||O(x)|$$

i.e. $|O(x)| = [G : G_x]$

Proof. Define $f : G/G_x \longrightarrow O(x)$ by $f(gG_x) = g.x$

By Proposition 4.6.18, $f(g_1G_x) = f(g_2G_x)$ if and only if $g_1G_x = g_2G_x$, it follows f is well-defined and also injective.

The surjectivity of f follows directly from the definition of orbit. □

Example 4.7.2. *D_n acts on the set V of n vertices of a regular n-gon. This is a transitive action, so for any vertex $v \in V$, its orbit $O(v) = V$. So*

$$G_v = \frac{|D_n|}{|V|} = \frac{2n}{n} = 2$$

And explicitly, the two elements in G_v are identity and reflection along the line passing through v and the centre of the n-gon.

Proposition 4.7.3. *If H, K are finite subgroup of G, then*

$$|HK| = \frac{|H| \times |K|}{|H \cap K|}$$

Proof. The product group $H \times K$ acts on G by $(h, k).g = hgk^{-1}$. (It is left as an exercise to verify that this is a group action.)

Consider then stabiliser of the identity:

$$G_1 = \{(h,k) \in H \times K | (h,k).1 = hk^{-1} = 1\} = \{(h,k) \in H \times K | h = k\} = \{(x,x) | x \in H \cap K\}$$

So $|G_1| = |H \cap K|$. The Counting Formula then can be applied to conclude

$$|HK| = |O(1)| = \frac{|H \times K|}{|G_1|} = \frac{|H| \times |K|}{|H \cap K|}$$

□

Recall that a group G can act on itself by conjugation. Each orbit of this action is a conjugacy class C_x, so all the conjugacy classes form a partition of G.

For $x \in G$, it is easy to see $|O(x)| = 1$ if and only if $gxg^{-1} = x$ for any $g \in G$, which is same as $x \in Z(G)$. So the partition described above implies:

Proposition 4.7.4. *(Class Equation) $|G|$ is a finite group, then:*

$$|G| = |Z(G)| + \sum_{x \in S} |C_x| = |Z(G)| + \sum_{x \in S} \frac{|G|}{|N(x)|}$$

where S is a set of representatives of conjugacy classes with size at least 2, C_x is the conjugacy class of x, and $N(x)$ is the normaliser of x.

Proposition 4.7.5. *If p is a prime number, then every group of order p^2 is abelian.*

Proof. Let G be a group of order p^2. By the Class Equation:

$$p^2 = |G| = |Z(G)| + \sum_{x \in S} |C_x|$$

Since for any $x \in S$, $1 < |C_x| < |G| = p^2$ and $|C_x|$ is divisible by p, we see $|C_x| = p$, so the above class equation implies $|Z(G)|$ is divisible by p, i.e., $|Z(G)| = p$ or $|Z(G)| = p^2$.

Now we are going to show the case $|Z(G)| = p$ is impossible, then we conclude $|Z(G)| = G$, which is same as G abelian.

Suppose $|Z(G)| = p$, we take $g \in G \setminus Z(G)$. Note $Z(G) \subseteq N(g)$ and $g \in N(g)$, so $|N(g)| \geq |Z(G)| + 1 = p + 1$. But $|N(g)|$ divides $|G| = p^2$ since $N(g)$ is a subgroup of G, we get $|N(g)| = G$, which means $g \in Z(G)$, contradiction. □

Theorem 4.7.6. *(Cauchy's Theorem) If G is a group, and p is a prime number that divides $|G|$, then G has an element of order p.*

Proof. Let $C_p =< a >$, the cyclic group of order p. C_p acts on

$$Y = \{(g_1, g_2, ..., g_p) \in G \times ... \times G | g_1 g_2 ... g_p = 1\}$$

by the rule

$$a.(g_1, g_2, ..., g_{p-1}, g_p) = (g_2, g_3, ..., g_p, g_1)$$

(Note that if $g_1 g_2 ... g_p = 1$, then the product of a cyclic permutation of them is still 1)

$|Y| = |G|^{p-1}$, since the last coordinate is determined by the first $n-1$ coordinates.

And observe that $(g_1, ..., g_p)$ is a fixed point if and only if $g_1 = g_2 = ... = g_p = g$ for some $g \in G$ such that $g^p = 1$.

Since the size of each orbit divides $|C_p| = p$, and $|Y| = |G|^{p-1}$ is divisible by p, there must be some other fixed points besides $(1, ..., 1)$, and those fixed points $(x, ..., x)$ where $x \neq 1$ give elements $x \in G$ of order p.

□

5 Classification of Groups

5.1 Sylow Subgroups and Sylow Theorems

Definition 5.1.1. p is a prime and G is a group whose order is divisible by p. A subgroup H of G is a **p-subgroup** if $|H| = p^r$ for some positive integer r.

Definition 5.1.2. G is a group such that $|G| = p^e m$, where p is a prime, e is a positive integer and p doesn't divide m. A subgroup H of G is a **Sylow p-subgroup** if $|H| = p^e$.

Theorem 5.1.3 (Sylow Theorem)**.** *G is a group such that $|G| = p^e m$, where p is a prime, e is a positive integer and p doesn't divide m. Then;*

(i). There exists a Sylow p-subgroup of G

(ii). If H is a Sylow p-subgroup of G and K is a p-group of G, then there exists $g \in G$ such that $K \subseteq gHg^{-1}$

(iii). The number of Sylow p-subgroups divides m and congruent to 1 modulo p.

We will prove this significant theorem in the next section, and we will first see some applications instead.

Corollary 5.1.4. *All the Sylow p-subgroups are conjugate to each other, and a Sylow p-subgroup is a normal subgroup of G if and only it is the only Sylow p-subgroup of G.*

Proof. Take both H and K be Sylow p-subgroups in part (ii) of Sylow's Theorem, we get H is conjugate to K.

Let H be a Sylow p-subgroup of G. G acts on S, the set of all Sylow p-subgroups of G, by conjugation, then this action is transitive by the previous paragraph, $S = O(H)$. H is a normal subgroup of $G \iff G_H = G \iff S = O(H) = \{H\} \iff H$ is the unique Sylow p-subgroup. □

Example 5.1.5. *We will show that any group of order 15 is isomorphic to $\mathbb{Z}/15\mathbb{Z}$*

If G is a group of order $15 = 3 \times 5$, it will have Sylow 3-subgroups and Sylow 5-subgroups, i.e. subgroups of order 3 and order 5. (This can also be

seen from the Cauchy's Theorem). The number of Sylow 3*-subgroups divides* 5 *and is congruent to* 1 *modulo* 3*, so it has to be* 1*, which then implies this unique Sylow* 3*-subgroup is a normal subgroup of* G*, and call it* H*. Similarly, we can show that there is a unique Sylow* 5*-subgroup of* G *that is a normal subgroup, and call it* K*. Since* 3 *and* 5 *are primes, we know* $H \cong \mathbb{Z}/3\mathbb{Z}$ *and* $K \cong \mathbb{Z}/5\mathbb{Z}$*.*

$|H| = 3$ *and* $|K| = 5$ *implies* $|H \cap K| = 1$*, so* $H \cap K = \{1\}$*.*

$|HK| = \frac{|H|\times|K|}{|H\cap K|} = \frac{3\times 5}{1} = 15 = |G|$*, so* $HK = G$

and together with the fact H, K *are normal subgroups of* G*, we conclude*

$$G \cong H \times K \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$$

Example 5.1.6. *Consider the alternating group* A_5*.* $|A_5| = \frac{|S_5|}{2} = \frac{5!}{2} = 60 = 2^2 \times 3 \times 5$*. By Sylow Theorem, the number of Sylow* 5*-subgroups divides* $2^2 \times 3 = 12$ *and is congruent to* 1 *modulo* 5*, so it is* 1 *or* 6*. We know* A_5 *is a simple group, so it has no proper normal subgroups, the Sylow* 5*-subgroups cannot be unique, so the number of Sylow* 5*-subgroups has to be* 6*.*

Note the union of these 6 *Sylow* 5*-subgroups consists of the identity and* $6 \times (5 - 1) = 24$ *non-identity elements.*

Example 5.1.7. *We will show that a group of order* 30 *is not simple.*

$30 = 2 \times 3 \times 5$*. By Sylow Theorem, there exists Sylow* 3*-subgroup of order* 3 *and Sylow* 5*-subgroup of order* 5*. The number of Sylow* 3*-subgroup divides* 10 *and congruent to* 1 *modulo* 3*, so it may be* 1 *or* 10*. The number of Sylow* 5*-subgroup divides* 6 *and congruent to* 1 *modulo* 5*, so it may be* 1 *or* 6*.*

Suppose there are 10 *subgroups of order* 3 *and* 6 *subgroups of order* 5*. Since* 3 *and* 5 *are prime numbers, the intersection of any two of these* $10 + 6$ *subgroups is* $\{1\}$*. So the union of these* 16 *subgroups have* $1 + 10 \times (3 - 1) + 6 \times (5 - 1) = 45 > 30$*, contradiction. We conclude at least one of the number of Sylow* 3*-subgroups and the number of Sylow* 5*-subgroups is* 1*, so either the Sylow* 3*-subgroup or the Sylow* 5*-subgroup is a proper normal subgroup.*

Example 5.1.8. *We will show that any group of order* 224 *is not simple.*

If $|G| = 224 = 2^5 \times 7$*, then it has Sylow* 2*-subgroup of order* 32 *and Sylow* 7*-subgroup of order* 7*. The number of Sylow* 2*-subgroups divides* 7 *and is congruent to* 1 *modulo* 2*, so it may be* 1 *or* 7*.*

If the number of Sylow 2-subgroups is 1, then this unique Sylow 2-subgroup is a proper normal subgroup, so G is not simple.

If the number of Sylow 2-subgroups is 7, let S be the set of all Sylow 2-subgroups, and G acts on S by conjugation, and this group action corresponds to a homomorphism

$$\Phi : G \longrightarrow S_7$$

Φ is not the trivial homomorphism, since the action is transitive, which implies the action is not the trivial action. Also Φ cannot be injective, since $|G| = 2^5 \times 7$ does not divide $|S_7| = 7!$. So $\ker \Phi$ is neither G nor $\{1\}$, we conclude $\ker \Phi$ is a proper normal subgroup of G, so G is not simple.

5.2 Proof of Sylow Theorem

Lemma 5.2.1. *If $n = p^e m$ where p is a prime, $e > 0$ and p doesn't divide m, then p does not divide $\binom{n}{p^e}$, which the number of ways to choose p^e elements from a set of n elements.*

Lemma 5.2.2. *G is a group and k is a positive integer with $k \leq |G|$. S is the set of all subsets of cardinality k of G. G has an action on S by left multiplication:*

$$g.\{x_1, ..., x_k\} = \{gx_1, ..., gx_k\}$$

and for this action, $|G_U|$ divides k for any $U \in S$.

Proof. It is easy to see $g.\{x_1, ..., x_k\} = \{gx_1, ..., gx_k\}$ defines a group action, so we leave this part as an exercise.

To show G_U divides k, it suffices to show U is a disjoint union of some right cosets of G_U in G, since all the right cosets of G_U in G are disjoint and have the same number of elements.

If $G_U g \cap U \neq \emptyset$, then there exists $g' \in G$ such that $g' \in G_U g \cap U$, so $G_U g = G_U g'$. G_U is the stabiliser of U, and $g' \in U$, so $G_U g' \subseteq U$. We thus see U is a disjoint union of some right cosets of G_U in G. □

Lemma 5.2.3 (Fixed Point Theorem)**.** *G is a group acting on a set X. $|G| = p^k$, where p is a prime and $k > 0$. If p does not divide $|X|$, then there exists a fixed point $x \in X$ under this action, i.e. $g.x = x$ for any $g \in G$.*

Proof. Suppose there is no fixed point. Then for any $y \in X$, the orbit $O(y)$ has size $|O(y)| > 1$, and $|O(y)| = \frac{|G|}{|G_y|} = \frac{p^k}{|G_y|}$, so $|O(y)|$ is a positive power of p, in particular, p divides $O(y)$.

X is the disjoint union of all the orbits, so it follows $|X|$ is divisible by p, contradiction. □

Lemma 5.2.4. *G is a group acting on X. For any $g \in G$, any $x \in X$:*

$$G_{g.x} = gG_xg^{-1}$$

Proof. $h \in G_{g.x} \iff h.(g.x) = g.x \iff (hg).x = g.x \iff (g^{-1}hg).x = x \iff g^{-1}hg \in G_x \iff h \in gG_xg^{-1}$ □

Now we shall begin the proof of Sylow Theorem.

5.2.1 Proof of (i)

We are going to show that G has a Sylow p-subgroup.

Let G act on S, the set of all subsets of G with p^e elements. $|S| = \binom{n}{p^e}$, and by Lemma 5.2.1, p does not divide $|S|$, so there exists $U \in S$ such that p does not divide $|O(U)|$.

Applying the Counting Formula,

$$|O(U)||G_U| = |G| = p^e m$$

so p not dividing $|O(U)|$ implies p^e dividing $|G_U|$

if we apply Lemma 5.2.2, we get $|G_U|$ divides p^e as well, so we conclude $|G_U| = p^e$, and thus we have found a Sylow p-subgroup of G.

5.2.2 Proof of (ii)

Let H be a Sylow p-subgroup of G and K a p-subgroup of G, so $|H| = p^e$ and $|K| = p^r$ for some $1 \leq r \leq e$.

G acts on $X = G/H$, the set of left cosets of H in G, by left multiplication:

$$g.xH = (gx)H$$

it is left as an exercise to show that $G_H = H$.

Now restrict the action to the subgroup K. $|K| = p^r$, and by Lagrange Theorem, $|X| = \frac{|G|}{|H|} = m$, which is not divisible by p. So we can apply

Lemma 5.2.3, there exists a fixed point $gH \in X$ for this K-action on X, i.e. $K_{gH} = K$.

In particular, we get $K \subseteq G_{gH} = gG_Hg^{-1} = gHg^{-1}$ by Lemma 5.2.4.

5.2.3 Proof of (iii)

Let Y be the set of Sylow p-subgroups of G. By Corollary 5.1.4 (which is a consequence of (ii) and (ii) has been proved), G acts on Y by conjugation transitively.

let $H \in Y$, then $G_H = \{g \in G | gHg^{-1} = H\} = N(H)$, the normaliser of H. We leave it as an exercise to show that H is a normal subgroup of $N(H)$. In particular, $|H|$ divides $N(H)$, $\frac{|G|}{N(H)}$ divides $\frac{|G|}{|H|}$

The Counting Formula implies $|Y| = |O(H)| = \frac{|G|}{|N(H)|}$, which divides $\frac{|G|}{|H|} = \frac{p^e m}{p^e} = m$, i.e. $|Y|$ divides m.

Now we restrict the group action to the subgroup H, that is, let H act on Y by conjugation.

$H \subseteq N(H)$ implies $O(H) = \{H\}$, $|O(H)| = 1$. Note $|H| = p^e$, so the number of elements in any orbit divides p^e. We know $|Y|$ is the summation of the cardinality of all its orbits, so in order to show $|Y| \equiv 1 \pmod{p}$, it suffices to show the number of elements in any orbit other than $\{H\}$ is more than one:

If $H' \in Y$ and $O(H') = \{H'\}$, then $H \subseteq N(H')$, we see both H and H' are Sylow p-subgroups of $N(H')$. But H' is a normal subgroup in $N(H')$, which implies H' is the only Sylow p-subgroup of $N(H')$, hence $H = H'$. So $\{H\}$ is the only orbit with one element.

5.3 Semidirect Product Construction

Definition 5.3.1. G and G' are groups, and $\phi : G' \longrightarrow Aut(G)$ is a homomorphism. The **semidirect product** of G and G' with respect to ϕ is the group $G \rtimes_\phi G'$ whose underlying set is same as that of $G \times G'$, and the law of composition is defined by

$$(g_1, g_1')(g_2, g_2') = (g_1 \phi_{g_1'}(g_2), g_1' g_2')$$

Proposition 5.3.2. *$G \rtimes_\phi G'$ defined above is a group.*

Proof. (1). For any $(g_1, g_1'), (g_2, g_2'), (g_3, g_3') \in G \rtimes_\phi G'$,

$$\begin{aligned}((g_1, g_1')(g_2, g_2'))(g_3, g_3') &= (g_1\phi_{g_1'}(g_2), g_1'g_2')(g_3, g_3') \\ &= (g_1\phi_{g_1'}(g_2)\phi_{g_1'g_2'}(g_3), (g_1g_2)g_3) \\ &= (g_1\phi_{g_1'}(g_2)\phi_{g_1'}(\phi_{g_2'}(g_3)), g_1'(g_2'g_3')) \\ &= (g_1\phi_{g_1'}(g_2\phi_{g_2'}(g_3)), g_1'(g_2'g_3')) \\ &= (g_1, g_1')(g_2\phi_{g_2'}(g_3), g_2'g_3') \\ &= (g_1, g_1')((g_2, g_2')(g_3, g_3'))\end{aligned}$$

(2). The identity element is $(1, 1')$: for any (g, g')

$(1, 1')(g, g') = (1\phi_{1'}(g), 1'g') = (g, g')$ and $(g, g')(1, 1') = (g\phi_{g'}(1), g'1') = (g, g')$

(3). $(g, g')^{-1} = (\phi_{(g')^{-1}}(g^{-1}), (g')^{-1})$:

$(g, g')(\phi_{(g')^{-1}}(g^{-1}), (g')^{-1}) = (g\phi_{g'}(\phi_{(g')^{-1}}(g^{-1})), g'(g')^{-1}) = (g\phi_{g'(g')^{-1}}(g^{-1}), 1') = (1, 1')$

$(\phi_{(g')^{-1}}(g^{-1}), (g')^{-1})(g, g') = (\phi_{(g')^{-1}}(g^{-1})\phi_{(g')^{-1}}(g), (g')^{-1}g') = (\phi_{(g')^{-1}}(g^{-1}g), 1') = (1, 1')$

□

Example 5.3.3. *If $G' \longrightarrow Aut(G)$ is the trivial homomorphism, then $G \rtimes_\phi G' = G \times G'$, so the product group is a special case of the semidirect product group.*

We can regard G and G' as subgroups of $G \rtimes_\phi G'$ via the inclusion maps

$$i_1 : G \longrightarrow G \rtimes_\phi G'$$

$$g \mapsto (g, 1')$$

$$i_2 : G' \longrightarrow G \rtimes_\phi G'$$

$$g \mapsto (1, g')$$

Proposition 5.3.4. *$i_1(G)$ is a normal subgroup of $G \rtimes_\phi G'$. In particular, for any $g \in G$, $g' \in G'$:*

$$(1, g')(g, 1')(1, g')^{-1} = (\phi_{g'}(g), 1')$$

Proof. For any $(x,y) \in G \rtimes_\phi G'$, $(g,1') \in i_1(G)$:

$$\begin{aligned}(x,y)(g,1')(x,y)^{-1} &= (x\phi_y(g),y)(\phi_{y^{-1}}(x^{-1}),y^{-1}) \\ &= (x\phi_y(g)\phi_y(\phi_{y^{-1}}(x^{-1})),yy^{-1}) \\ &= (x\phi_y(g)x^{-1},yy^{-1})\end{aligned}$$

So $i_1(G)$ is a normal subgroup of $G \rtimes_\phi G'$, and the above computation implies

$$(1,g')(g,1')(1,g')^{-1} = (\phi_{g'}(g),1')$$

by taking $(x,y) = (1,g')$ □

Corollary 5.3.5. *If $\phi : G' \longrightarrow Aut(G)$ is not the trivial homomorphism, then $G \rtimes_\phi G'$ is a non-abelian group.*

Similar to the study of product groups, we are interested in the question: Given a group G, can we find its subgroups H and K such that G is the semidirect product of H and K?

More specifically, if G is a group, H is a normal subgroup of G and K is a subgroups of G, define $\phi : K \longrightarrow Aut(H)$ by $\phi_k(h) = khk^{-1}$. Then we can define a map

$$\begin{aligned}f : H \rtimes_\phi K &\longrightarrow G \\ (h,k) &\mapsto hk\end{aligned}$$

and we would like to see when f is an isomorphism.

Theorem 5.3.6. *G is a group, H is normal subgroup of G and K is a subgroup of G. Then*

$$f : H \rtimes_\phi K \longrightarrow G$$

defined above is an isomorphism if and only if $H \cap K = \{1\}$, and $HK = G$.

Proof. If f is an isomorphism, it follows easily that $H \cap K = \{1\}$, and $HK = G$.

If $H \cap K = \{1\}$, and $HK = G$, we will show that f is an isomorphism.

First, for any $(h_1,k_1),(h_2,k_2) \in H \rtimes_\phi K$:

$$\begin{aligned}f((h_1,k_1)(h_2,k_2)) &= f((h_1(k_1h_2k_1^{-1}),k_1k_2)) \\ &= h_1(k_1h_2k_1^{-1})k_1k_2 \\ &= h_1k_1h_2k_2 \\ &= f((h_1,k_1))f(h_2,k_2)\end{aligned}$$

So f is a homomorphism.

If $f((h,k)) = hk = 1$, then $h = k^{-1} \in H \cap K = \{1\}$, $h = k = 1$, so $\ker(f)$ is trivial, f is injective.

f is surjective since $G = HK = Im(f)$. □

Remark 5.3.7. If the above map $f : H \rtimes_\phi K \longrightarrow G$ is an isomorphism, we usually write $G = H \rtimes K$. The symbol ϕ, which stands for the conjugation action of K on H, is omitted.

Example 5.3.8. *Consider the group M_n of isometries on $\mathbb{R}^n$. We know it has a normal subgroup T_n (the subgroup of translations) and a subgroup O_n (the subgroup of orthogonal linear operators). Since $T_n \cap O_n = \{id\}$ and $T_nO_n = M_n$ (recall that each isometry can be written as a composition of the form $t_{\vec{a}}\phi$), so we conclude $M_n = T_n \rtimes O_n$*

Example 5.3.9. *S_3 has a normal subgroup $H =< (1\ \ 2\ \ 3) >$ and a subgroup $K =< (1\ \ 2) >$. $H \cap K = \{id\}$ and $HK = S_3$, so $S_3 = H \rtimes K$.*

5.4 Rubik's Cube Group

The Rubik's Cube is a famous mathematical toy that is invented by Ernö Rubik in 1974. It is a cube each of whose faces has a distinct colour. For the classic $3 \times 3 \times 3$ Rubik's Cube, each face is subdivided into 9 sub-faces so that the cube is made up by 26 blocks of small cubes: 8 corner blocks (each contains 3 colours), 12 edge blocks (each contains 2 colours) and 6 centre blocks (each contains 1 colour). The 9 pieces forming one of the faces of the cube can be rotated together by multiples of 90 degrees. The goal of the game is to recover a given rotated cube to its original configuration.

After invention, solution algorithms have been found (if you search online, you can find many articles about how to solve a Rubik's Cube), and generalisations to higher orders and other shapes have also been developed. From a mathematical point of view, it is a good game for the applications of group theory.

Definition 5.4.1. The **Rubik's Cube Groups** Γ is the group of all moves of a $3 \times 3 \times 3$ Rubik's Cube, with the law of composition be the composition of moves. (Two moves are identified to be the same if the configurations of the Rubik's cube under these moves are the same)

An important but obvious observation is that each element in Γ can be written as a finite sequence of composition of the following elements:

$$U, D, F, B, L, R$$

These elements denotes the clockwise rotation by 90 degree of the Up, Down, Front, Back, Left and Right face respectively. Each of these six elements is of order 4.

Let V denote the set of 8 corner blocks and E the set of 12 edge blocks of the Rubik's Cube. Each move will induce a permutation on V and on E respectively. We obtain a homomorphism:

$$\psi : \Gamma \longrightarrow S_V \times S_E$$

sending each move to its permutation effect on V and E, where $S_V \cong S_8$ and $S_E \cong S_{12}$ are the permutation groups of V and E respectively.

The kernel of this homomorphism, $\Gamma_0 = \ker \psi$, is the normal subgroup of Γ consisting of those moves that do not permute the blocks.

Next, we can mark some of the faces of the Rubik's cube in the way that there is a unique marked face in each Vertex block and each edge block. We call a way of such markings an orientation. Once the orientation is determined, the moves that will fix the position of the set of marks will be denoted by Γ_1.

If a move lies in $\Gamma_0 \cap \Gamma_1$, the it will not permute the blocks and will not change the orientation of any block, so it has to be the identity move, we get $\Gamma_0 \cap \Gamma_1 = \{1\}$

Each move can be decomposed into a move that changes the orientations while fixing the blocks followed by a move that permute the blocks while keeping the orientations, so $\Gamma = \Gamma_0\Gamma_1$

We conclude that

$$\Gamma = \Gamma_0 \rtimes \Gamma_1$$

There are also further decomposition of Γ_0 and Γ_1 into direct or semidirect products of smaller subgroups. With more work, it can be shown that:

$$\Gamma_0 \cong \underbrace{\mathbb{Z}/3\mathbb{Z} \times ... \times \mathbb{Z}/3\mathbb{Z}}_{\text{7 copies}} \times \underbrace{\mathbb{Z}/2\mathbb{Z} \times ... \times \mathbb{Z}/2\mathbb{Z}}_{\text{11 copies}}$$

and

$$\Gamma_1 \cong (A_8 \times A_{12}) \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$$

There are many interesting topics and results related to the Rubik's Cube Group Γ. For example, $|\Gamma| = 2^{27} \times 3^{14} \times 5^3 \times 7^2 \times 11$. It is a finite group implies each element is of finite order, so it follows that if you repeat any move for some finite number of times, you will turn the Rubik's cube back to its starting configuration.

What's more, it has been shown that any element in Γ can be written as a composition of at most 26 letters in $U^{\pm 1}, D^{\pm 1}, F^{\pm 1}, B^{\pm 1}, L^{\pm 1}, R^{\pm 1}$. This means the Rubik's Cube can always be solved within 26 steps of counter clockwise or clockwise 90 degree rotations. If we also count each of U^2, D^2, F^2, B^2, L^2, R^2 as a letter, then it can be shown that any element in Γ can be written as a composition of at most 20 letters. This means the Rubik's cube can always be solved within 20 steps of rotations. This number 20 is often referred to as the "God's number" for Rubik's Cube.

The reader may refer to some books and articles for more explorations and discussions, for example, "Inside Rubik's Cube and Beyond" (Birkhuser Boston, 1982) by Christoph Bandelow, and "Adventures in Group Theory" (The Johns Hopkins University Press, 2008) by David Joyner.

5.5 Groups of Order $2p$

Theorem 5.5.1. *If p is a prime and G is a group of order $2p$, then G is isomorphic to either $\mathbb{Z}/2p\mathbb{Z}$ or D_p.*

Proof. If $|G| = 2 \times 2 = 4$, we have done the classification before.

If $|G| = 2p$ for some odd prime p, by Sylow Theorem, there exists Sylow p-subgroup H and Sylow 2-subgroup K of G. The number of Sylow p-subgroups divides 2 and congruent to 1 modulo p, so it has to be 1, we get H is a normal subgroup of G.

$H \cap K = \{1\}$ since $|H| = p$ and $|K| = 2$ are relatively prime.

$HK = G$ since $|HK| = \frac{|H| \times |K|}{|H \cap K|} = 2p = |G|$

We thus have

$$G = H \rtimes K \cong \mathbb{Z}/p\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$$

where $\phi : \mathbb{Z}/2\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/p\mathbb{Z})$ is a homomorphism.

The homomorphism is determined by $\phi(\bar{1})$. Since the order of $\bar{1} \in \mathbb{Z}/2\mathbb{Z}$ is 2, the order of $\phi(\bar{1}) \in Aut(\mathbb{Z}/p\mathbb{Z})$ has to be 1 or 2.

Recall that $Aut(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$, the group of units. If $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$ satisfies $\bar{a}^2 = \bar{1}$, then p divides $a^2 - 1 = (a-1)(a+1)$, so p divides $a-1$ or p divides $a+1$, i.e. $\bar{a} = \bar{1}$ or $\bar{a} = -\bar{1}$. This implies the only automorphisms whose order is divisible by 2 is the identity map $\phi(\bar{1})(\bar{k}) = \bar{k}$ and the map $\phi(\bar{1})(\bar{k}) = -\bar{k}$.

If $\phi(\bar{1})(\bar{k}) = \bar{k}$, then $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2p\mathbb{Z}$.

If $\phi(\bar{1})(\bar{k}) = -\bar{k}$, then $G \cong \mathbb{Z}/p\mathbb{Z} \times_\phi \mathbb{Z}/2\mathbb{Z}$ is not abelian, so it is not isomorphic to the first case.

Since these are the only two possible isomorphic classes for a group of order $2p$, and $|D_p|$ is a non-abelian group of order $2p$, so D_p has to be isomorphic to the second case. We conclude that a group of order $2p$ is isomorphic to either $\mathbb{Z}/2p\mathbb{Z}$ or D_p. $\square$

5.6 Groups of Order 12

The process of classification of groups of order 12 is a great summary of what we have learned about group theory in this course.

Theorem 5.6.1. *There are five isomorphic classes of groups of order* 12*.*

Proof. $|G| = 12 = 2^2 \times 3$, so it has a Sylow 2-subgroup H and a Sylow 3-subgroup K. The number of Sylow 2-subgroups can be 1 or 3, and the number of Sylow 3-subgroups can be 1 or 4.

If there are 4 subgroups of order 3, then there are only $12-1-4\times(3-1) = 3$ elements outside the union of there four Sylow 3-subgroups, so there is only space for at most 1 Sylow 2-subgroup. We conclude either H or K is a normal subgroup of G.

$|H|$ and $|K|$ are relatively prime, so $H \cap K = \{1\}$. $|KH| = |HK| = \frac{|H|\times|K|}{|H\cap K|} = 12$, so $G = HK = KH$.

$|H| = 4$ implies $H \cong \mathbb{Z}/4\mathbb{Z}$ or $H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; $|K| = 3$ implies $K = \mathbb{Z}/3\mathbb{Z}$.

Case 1. If both of $|H|$ and $|K|$ are normal subgroups of G, then $G = H \times K$.

Case 1a. $G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Case 1b. $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Case 2. If H is normal and K is not normal, $G = H \rtimes K$ and it is not direct product.

Case 2a. $G \cong \mathbb{Z}/4\mathbb{Z} \rtimes_\phi \mathbb{Z}/3\mathbb{Z}$, $\phi : \mathbb{Z}/3\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/4\mathbb{Z}) \cong (\mathbb{Z}/4\mathbb{Z})^\times = \{\bar{1}_4, \bar{3}_4\}$. So $|Aut(\mathbb{Z}/4\mathbb{Z})| = 2$ and $|\mathbb{Z}/3\mathbb{Z}| = 3$, there is no nontrivial homomorphism ϕ in this case.

Case 2b. $G \cong (\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}) \rtimes_\phi \mathbb{Z}/3\mathbb{Z}$, $\phi : \mathbb{Z}/3\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}) \cong S_3$. ϕ is determined by $\phi(\bar{1}_3)$, and $|\bar{1}_3| = 3$, so $\bar{1}$ is mapped to one of the two 3-cycles in S_3. These two choices will give isomorphic semi-direct product group structure since there is an automorphism of S_3 switching the two

3-cycles. In this case there is a unique semi-direct product structure.

Case 3. If K is normal and H is not normal, $G = K \rtimes H$ and it is not direct product.

Case 3a. $G \cong \mathbb{Z}/3\mathbb{Z} \rtimes_\phi \mathbb{Z}/4\mathbb{Z}$, $\phi : \mathbb{Z}/4\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/3\mathbb{Z}) \cong (\mathbb{Z}/3\mathbb{Z})^\times = \{\bar{1}_3, \bar{2}_3\}$. ϕ is determined by $\phi(\bar{1}_4)$ and ϕ is not trivial, so $\phi(\bar{1}_4)$ is the map $\bar{k}_3 \mapsto 2\bar{k}_3 = -\bar{k}_3$, and $\phi(\bar{m}_4) = (\bar{k}_3 \mapsto (-1)^m \bar{k}_3)$. In this case there is a unique semi-direct product structure.

Case 3b. $G \cong \mathbb{Z}/3\mathbb{Z} \rtimes_\phi (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$, $\phi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/3\mathbb{Z}) \cong (\mathbb{Z}/3\mathbb{Z})^\times = \{\bar{1}_3, \bar{2}_3\}$. The three non-identity elements in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ are all of order 2, so if ϕ is not trivial, it has to be the case two of these three elements map to $\bar{2}_3$ and the remaining one maps to $\bar{1}_3$. And the difference choices of the element sending to $\bar{1}_4$ give isomorphic semidirect product groups. In this case this is a unique semi-direct product structure.

The above discussion produces all the five possible isomorphic classes of groups of order 12.

□

Remark 5.6.2. The group A_4 is isomorphic Case 2b, and the group D_6 is isomprphic to Case 3b.

5.7 Groups of Order 8

We are going to classify isomorphic classes of groups of order 8 in this section. Note $8 = 2^3$, so Sylow Theorem doesn't help in this case, we need to figure out some other methods.

Lemma 5.7.1. *If all the non-identity elements of a group G are of order 2, then G is abelian.*

Proof. $g^2 = 1$ for any $g \in G$, so $g = g^{-1}$ for any $g \in G$.

For any $a, b \in G$, $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$. So the group is abelian. □

Lemma 5.7.2. *H and K are subgroups of a group G. Then HK is a subgroups of G if and only if $HK = KH$.*

Proof. If $HK = KH$, for any $h_1k_1, h_2k_2 \in HK$, $(h_1k_1)^{-1}(h_2k_2) = k_1^{-1}h_1^{-1}h_2k_2$.

$k_1^{-1} \in K$ and $h_1^{-1}h_2 \in H$, so $k_1^{-1}h_1^{-1}h_2 \in KH = HK$, there exists $h \in H$ and $k \in K$ such that $k_1^{-1}h_1^{-1}h_2 = hk$. We see $k_1^{-1}h_1^{-1}h_2k_2 = hkk_2 = h(kk_2) \in$

HK. We conclude HK is a subgroup of G.

Conversely, assume HK is a subgroup of G.

For any $kh \in KH$, $kh = (h^{-1}k^{-1})^{-1}$. Since $h^{-1}k^{-1} \in HK$, and HK is a subgroup of G, $(h^{-1}k^{-1})^{-1} \in HK$, so $KH \subseteq HK$.

For any $hk \in HK$, since HK is a subgroup of G, $(hk)^{-1} \in HK$, so there exists $h' \in H$ and $k' \in K$ such that $(hk)^{-1} = h'k'$. So $hk = k'^{-1}h'^{-1} \in KH$, we get $HK \subseteq KH$. Thus we conclude $HK = KH$. □

Lemma 5.7.3. *G is a group, and z is the only element of order 2 in G, then $z \in Z(G)$, the centre of G.*

Proof. For any $g \in G$, $|gzg^{-1}| = |z| = 2$, and z is the only element of order 2 in G, we get $gzg^{-1} = z$, i.e., $gz = zg$, so $z \in Z(G)$. □

Theorem 5.7.4. *There are five isomorphic classes of groups of order 8.*

Proof. G is a group of order 8. Let $m = \max_{g \in G} |g|$, the maximal order of elements in G. The possibilities are $m = 2$, $m = 4$ or $m = 8$.

Case 1. $m = 8$: In this case, there exists $g \in G$ with $|g| = 8 = |G|$, so $G =< g >$ is a cyclic group of order 8:

$$G \cong \mathbb{Z}/8\mathbb{Z}$$

Case 2. $m = 2$: In this case, all the non-identity elements have order 2. By Lemma 5.7.1, G is an abelian group. Take $x, y \in G \setminus \{1\}$ with $x \neq y$, then $< x >< y >=< y >< x >$ since G is abelian, by Lemma 5.7.2, $H =< x >< y >= \{1, x, y, xy\}$ is a subgroup of G, and $H \cong < x > \times < y > \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Take $z \in G \setminus H$, let $K =< z >$. Then $H \cap K = \{1\}$, $|HK| = \frac{|H| \times |K|}{|H \cap K|} = 8 = |G|$, so $G = HK$, and we thus conclude

$$G \cong H \times K \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Case 3. $m = 4$: Let $i \in G$ with $|i| = 4$, and $N =< i >$ is a cyclic group of order 4. $[G : N] = 2$, so N is a normal subgroup of G.

Case 3.(a). If there exists $w \in G \setminus N$ such that $|w| = 2$, let $L =< w >$, then $N \cap L = \{1\}$, $|NL| = \frac{|N| \times |L|}{|N \cap L|} = 8 = |G|$, so $G = NL$, we get

$$G = N \rtimes L \cong \mathbb{Z}/4\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$$

$\phi : \mathbb{Z}/2\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/4\mathbb{Z}) \cong (\mathbb{Z}/4\mathbb{Z})^\times = \{\bar{1}_4, \bar{3}_4\}$. There are two possibilities:

If $\phi(\bar{1}_2)$ maps to identity, then ϕ is the trivial homomorphism, so

$$G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

If $\phi(\bar{1}_2)$ maps to the only non-identity element in $Aut(\mathbb{Z}/4\mathbb{Z})$, which is the map $\bar{k} \mapsto -\bar{k}$, then $\phi(\bar{n}_2)(\bar{k}_4) = \overline{(-1)^n k}_4$,

$$G \cong \mathbb{Z}/4\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z} \cong D_4$$

Case 3.(b). If all the elements in $G \setminus N$ are of order 4, then i^2 is the only element of order 2 in G. We denote $-1 = i^2$. -1 being the only element of order 2 in G implies $-1 \in Z(G)$ by Lemma 5.7.3.

Take $j \in G \setminus < i >$, then $|j| = 4$ and $< j >= \{1, j, -1, j^{-1}\}$. Next let $k = ij$, and it is easy to see $k \notin < i > \cup < j >$, so $|k| = 4$, $< k >= \{1, k, -1, k^{-1}\}$, and

$$G = \{1, -1, i, i^{-1}, j, j^{-1}, k, k^{-1}\}$$

Its multiplication table is already determined by the construction. For example, to find the composition jk: $ij = k \Longrightarrow ijk = k^2 = -1 \Longrightarrow jk = i^{-1}(-1) = i^{-1}i^2 = i$. Using the similar computation, we obtain the only possible multiplication table for G in this case (Since $i^{-1} = i^3 = (-1)i$, we will denote i^{-1} by $-i$, and similarly, we will denote j^{-1} and k^{-1} by $-j$, $-k$ respectively):

	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-1	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	k	-k	-j	j
-i	-i	i	1	-1	-k	k	j	-j
j	j	-j	-k	k	-1	1	i	-i
-j	-j	j	k	-k	1	-1	-i	i
k	k	-k	j	-j	-i	i	-1	1
-k	-k	k	-j	j	i	-i	1	-1

The group described by this multiplication table is called the **group of unit quaternions**, and denoted by Q_8. It takes some tedious but easy work to verify this multiplication table defines a group by checking the associativity case by case.

In summary, the five isomorphic classes of groups of order 8 are:

$$\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, D_4, Q_8$$

□

Remark 5.7.5. The group Q_8 is a subgroup of the group of units of the Quaternion ring $\mathbb{H}$. We will come to this point in the discussion of rings.

Exercise 5.7.6. *Show that the group Q_8 does not have a decomposition into semidirect product of its subgroups.*

6 Introduction to Rings

6.1 Definition of Rings

Definition 6.1.1. A **ring** $(R, +, \cdot)$ is a set R with two law of compositions $+$ and $\cdot$, called **addition** and **multiplication** respectively, that satisfy:

(i). R with $+$ forms an abelian group

(ii). Multiplication is associative and there is a multiplicative identity

(iii). (Distributive Law) For any $a, b, c \in R$:

$$(a+b)c = ac + bc, c(a+b) = ca + cb$$

Definition 6.1.2. A ring is called a **commutative ring** if the multiplication is commutative.

Remark 6.1.3. In this course we will follow the convention of the textbook that the term "**ring**" refers to "**commutative ring**", unless otherwise specified.

Notation 6.1.4. *In a ring, the additive identity is usually denoted by* 0 *and the multiplicative identity is usually denoted by* 1.

Example 6.1.5. *(i).* $(\mathbb{Z}, +, \times)$ *is a ring: the set is* $\mathbb{Z}$*, the addition and multiplication are those of integers.*

(ii). $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ *are also rings if we take the addition and multiplication of numbers.*

(iii). The zero ring is $\{0\}$*, with* $0 + 0 = 0$ *and* $0 \cdot 0 = 0$

(iv). $M_{n\times n}(\mathbb{R})$*, the set of* $n \times n$ *real matrices is a non-commutative ring with addition and multiplication of matrices.*

(v). $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ *is a ring if addition is* $\bar{a} + \bar{b} = \overline{a+b}$ *and multiplication is* $\bar{a} \cdot \bar{b} = \overline{ab}$

(vi). $R = \{f : \mathbb{R} \longrightarrow \mathbb{R} | f$ *is continuous*$\}$ *is a ring if addition is* $(f + g)(x) = f(x) + g(x)$ *and* $(fg)(x) = f(x)g(x)$

Proposition 6.1.6. *R is a ring, then:*

(i). For any $a \in R$, $0 \cdot a = a \cdot 0 = 0$

(ii). For any $a \in R$, $-a = (-1) \cdot a$

(iii). For any $a, b \in R$, $-(ab) = (-a)b = a(-b)$

Proof. (i). $0 \cdot a + a = 0 \cdot a + 1 \cdot a = (0+1) \cdot a = 1 \cdot a = a$, so $0 \cdot a = 0$
(ii). $(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = (-1+1) \cdot a = 0 \cdot a = 0$, so $(-1) \cdot a = -a$
(iii). $(-a)b + ab = (-a + a)b = 0 \cdot b = 0$, so $(-a)b = -(ab)$
Similarly we can prove $a(-b) = -(ab)$ □

Proposition 6.1.7. *R is a ring. $R = \{0\}$ if and only if $0 = 1$*

Proof. If $R = \{0\}$, then $0 \cdot 0 = 0$, so $0 = 1$
If $0 = 1$, then for any $a \in R$, $a = 1 \cdot a = 0 \cdot a = 0$, so $R = \{0\}$ □

Definition 6.1.8. R is a ring. $a \in R$ is called a **unit** if it has multiplication inverse $a^{-1} \in R$ such that $a \cdot a^{-1} = 1$

Example 6.1.9. *If R is a ring, then $1 \in R$ is a unit. We also call 1 the **unit element***

Example 6.1.10. *In the ring $\mathbb{Z}/n\mathbb{Z}$, we have studied the group of units, and we know $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ is a unit if and only if $\bar{a}$ is relatively prime to n.*

By a proof similar to that of the fact the units of $\mathbb{Z}/n\mathbb{Z}$ forms a group, we obtain the more general result:

Proposition 6.1.11. *R is a ring. The set of units in R forms a group with the composition to be the ring multiplication, denoted by $R^\times$*

Definition 6.1.12. A **field** is a nonzero ring $\mathbb{F}$ such that all the nonzero elements are units.

Example 6.1.13. *(i). $\mathbb{Z}/p\mathbb{Z}$ is a field if p is a prime number.*
(ii). $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.

Definition 6.1.14. R is a ring, $x, y \in R$. We say x is **associated to** y if there exists $u \in R^\times$ such that $x = uy$.

Proposition 6.1.15. *R is a ring. "$x \sim y$ if x is associated to y" is an equivalence relation on R.*

Exercise 6.1.16. *Prove the above proposition.*

6.2 Polynomial Rings

Definition 6.2.1. A **polynomial** with coefficients in a ring R is a finite linear combination of powers of the variable:

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$$

where the coefficients $a_i \in R$, and $a_n \neq 0$. n is called the **degree** of the polynomial, and a_n is called the **leading coefficient**.

Definition 6.2.2. The set of all polynomials with coefficients in R form a ring $R[x]$, with addition and multiplication defined as follows: if $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ and $g(x) = a_m x^m + b_{m-1}x^{m-1} + ... + b_1 x + b_0$, then

$$f(x) + g(x) = \sum_k (a_k + b_k)x^k, f(x)g(x) = \sum_{i,j} a_i b_j x^{i+j} = \sum_k \sum_{i=0}^{k} a_i b_{k-i} x^k$$

We call $R[x]$ the **polynomial ring** with coefficients in R.

Example 6.2.3. *$\mathbb{R}[x]$ is the polynomial ring with real coefficients, and $\mathbb{Z}[x]$ is the polynomial ring with integer coefficients.*

Remark 6.2.4. Each element in R can be regarded as a polynomial of degree zero in $R[x]$, called a constant polynomial.

Definition 6.2.5. A polynomial is **monic** if its leading coefficient is 1.

Proposition 6.2.6. *Let R be a ring. f is a monic polynomial in $R[x]$, and g is a polynomial in $R[x]$. Then there are uniquely determined polynomial q and r in $R[x]$ such that*

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

and $deg(r(x)) < deg(f(x))$ if $r(x) \neq 0$.

Proof. This follows from the same algorithm for division of polynomials in $\mathbb{Z}$. □

6.3 Ring Homomorphisms

Definition 6.3.1. A **ring homomorphism** $f : R \longrightarrow R'$ is a map from a ring R to a ring R' such that:

(i). For any $a, b \in R$, $f(a+b) = f(a) + f(b)$

(ii). For any $a, b \in R$, $f(ab) = f(a)f(b)$

(iii). $f(1_R) = 1_{R'}$

Example 6.3.2. *$f : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ defined by $f(k) = \bar{k}$ is a ring homomorphism:*

(i). For any $a, b \in \mathbb{Z}$, $f(a+b) = \overline{a+b} = \bar{a} + \bar{b} = f(a) + f(b)$

(ii). For any $a, b \in R$, $f(ab) = \overline{ab} = \bar{a}\bar{b} = f(a)f(b)$

(iii). $f(1) = \bar{1}$

Example 6.3.3. *R is a ring, $r \in R$. We can define the evaluation map:*

$$E : R[x] \longrightarrow R$$

$$f(x) \mapsto f(r)$$

This E is a ring homomorphism.

Definition 6.3.4. $f : R \longrightarrow R'$ is a **ring isomorphism** if it is a bijective ring homomorphism. Two rings R and R' are **isomorphic** if there exists a ring isomorphism between them.

Exercise 6.3.5. *Prove the inverse of a ring isomorphism is also a ring isomorphism.*

Proposition 6.3.6. *(Substitution Principle) $f : R \longrightarrow R'$ is a ring homomorphism, and $\alpha \in R'$. Then there is a unique ring homomorphism*

$$F : R[x] \longrightarrow R'$$

that agrees with f on constant polynomials and sends x to α.

Proof. Define $F : R[x] \longrightarrow R'$ by $F(\sum a_i x^i) = \sum f(a_i)\alpha^i$. Its restriction to R is the map f, and it is a ring homomorphism:

for any $f(x) = \sum a_i x^i$ and any $g(x) = \sum b_i x^i$ in $R[x]$,

$$\begin{aligned} F(\sum a_i x^i + \sum b_i x^i) &= F(\sum (a_i + b_i) x^i) \\ &= \sum f(a_i + b_i)\alpha^i \\ &= \sum (f(a_i) + f(b_i))\alpha^i \\ &= \sum f(a_i)\alpha^i + \sum f(b_i)\alpha^i \\ &= F(\sum a_i \alpha^i) + F(\sum b_i \alpha^i) \end{aligned}$$

$$\begin{aligned} F((\sum a_i x^i)(\sum b_j x^j)) &= F(\sum a_i b_j x^{i+j}) \\ &= \sum f(a_i b_j)\alpha^{i+j} \\ &= \sum f(a_i) f(b_j)\alpha^{i+j} \\ &= (\sum f(a_i)\alpha^i)(\sum f(b_j)\alpha^j) \\ &= F(\sum a_i x^i) F(\sum b_i x^i) \end{aligned}$$

$$F(1) = f(1) = 1$$

It is the unique one since if $F' : R[x] \longrightarrow R'$ is also a ring homomorphism such that $F'(r) = f(r)$ for $r \in R$ and $F'(x) = \alpha$, then:

$$F'(\sum a_i x^i) = \sum F'(a_i x^i) = \sum F'(a_i) F'(x)^i = \sum f(a_i)\alpha^i = F(\sum a_i x^i)$$

□

Corollary 6.3.7. *(Change of Coefficients) If $f : R \longrightarrow R'$ is a ring homomorphism, then there exists a unique homomorphism $F : R[x] \longrightarrow R'[x]$ sending x to x and $F(r) = f(r)$ for all $r \in R$.*

Proof. The composition $R \xrightarrow{f} R' \hookrightarrow R'[x]$ is a ring homoomorphism. Apply Substitution Principle to this ring homomorphism with x maps to x. □

Example 6.3.8. $\mathbb{Z}[x] \longrightarrow \mathbb{Z}/n\mathbb{Z}[x]$ *defined by* $\sum a_i x^i \mapsto \sum \bar{a}_i x^i$ *is a ring homomorphism.*

Definition 6.3.9. If $f : R \longrightarrow R'$ is a ring homomorphism, define the **kernel** of f to be

$$\ker(f) = \{r \in R | f(r) = 0_{R'}\}$$

Example 6.3.10. *$f : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ defined by $f(k) = \bar{k}$ has kernel* $\ker(f) = n\mathbb{Z}$.

6.4 Ideals

Definition 6.4.1. An **ideal** I of a ring R is a nonempty subset of R with the properties:

(i). I is closed under addition.

(ii). $rs \in I$ for any $r \in R$, any $s \in I$

Proposition 6.4.2. *If $f : R \longrightarrow R'$ is a ring homomorphism, then* $\ker(f)$ *is an ideal of R.*

Proof. First, we know if $x, y \in \ker(f)$, then $f(x) = f(y) = 0_{R'}$, so $f(x+y) = f(x) + f(y) = 0_{R'}$, $x + y \in \ker(f)$.

Next, for any $r \in R, s \in \ker(f)$, $f(rs) = f(r)f(s) = f(r)0_{R'} = 0_{R'}$, so $rs \in \ker(f)$.

We conclude $\ker(f)$ is an ideal of R. □

Proposition 6.4.3. *If I is an ideal of a ring R, then I is a subgroup of R with respect to addition.*

Proof. By the definition of ideal, we know I is closed under addition.

Pick any $s \in I$, then $0 = 0.s \in I$.

For any $s \in I$, $-s = (-1)s \in I$. □

Example 6.4.4. *$\{0\}$ is an ideal of a ring R, called the zero ideal.*

Example 6.4.5. *In the ring $\mathbb{Z}$, the ideals are $n\mathbb{Z}$.*

Example 6.4.6. *In the ring $\mathbb{Z}[x]$, $I = \{f(x) \in \mathbb{Z}[x] | f(0) = 0\}$ is an ideal:*

If $f, g \in I$, then $f(0) = g(0) = 0$, so $(f + g)(0) = f(0) + g(0) = 0$, $f + g \in I$.

For any $\phi \in \mathbb{Z}[x], f \in I$, $(\phi f)(0) = \phi(0)f(0) = \phi(0)0 = 0$, so $\phi f \in I$

Proposition 6.4.7. *I is an ideal of R. The following are equivalent:*

(i). $I = R$

(ii). $1 \in I$

(iii). $R^\times \cap I \neq \emptyset$

Proof. (i) $\Longrightarrow$ (iii): Obvious

(iii) $\Longrightarrow$ (ii): If $R^\times \cap I \neq \emptyset$, then there exists $s \in R^\times \cap I$, so $1 = s^{-1}s \in I$.

(ii) $\Longrightarrow$ (i): If $1 \in I$, then for any $r \in R$, $r = r.1 \in I$, so $I = R$. □

Corollary 6.4.8. *if I is an ideal of R such that $I \neq R$, then $I \cap R^\times = \emptyset$.*

Definition 6.4.9. R is a ring, $b \in R$. The **principal ideal** generated by b is

$$(b) = bR = \{br \in R | r \in R\}$$

Exercise 6.4.10. *Prove a principal ideal is an ideal.*

Example 6.4.11. *A ring is a principal ideal of itself:* $(1) = R$.

Example 6.4.12. *In the ring $\mathbb{Z}$, every ideal is a principal ideal.*

Definition 6.4.13. An ideal $I \subset R$ is called a proper ideal if $I \neq \{0\}$ and $I \neq R$.

Corollary 6.4.14. *A principal ideal $(b) \in R$ is proper if and only if $b \notin R^\times \cup \{0\}$.*

Proof. If $b = 0$, then $(b) = (0) = \{0\}$.

If $b \in R^\times$, then $(b) \cap R^\times \neq \emptyset$, so $(b) = R$.

If $b \notin R^\times \cup \{0\}$, then $b \in (b)$, so $(b) \neq \{0\}$. Suppose $(b) = R$, then $1 \in R = (b)$ implies $1 = rb$ for some $r \in R$, which means $b \in R^\times$, contradiction, so $(b) \neq R$. □

Corollary 6.4.15. *A nonzero ring R is a field if and only if it has no proper ideal.*

Proof. If I is an ideal of a field R such that $I \neq \{0\}$, then there exists $r \in I \setminus \{0\} = F^\times$, so $I \cap F^\times \neq \emptyset$, we get $I = R$.

Conversely, if R is a nonzero ring that has no proper ideals, then for any $r \in R \setminus \{0\}$, and $(r) = R$, so $r \in R^\times$, we conclude R is a field. □

Proposition 6.4.16. *F is a field. Every ideal in $F[x]$ is a principal ideal.*

Proof. If $I = \{0\}$, obvious.

If $I \neq \{0\}$, choose $f \in I$ such that f is a monic polynomial of minimal degree in I. We will show that $I = (f)$.

First, $f \in I$, so $(f) \subseteq I$.

Conversely, for any $g \in I$, we can find $q, r \in F[x]$ such that $g(x) = f(x)q(x) + r(x)$, with $r = 0$ or $deg(r) < deg(f)$. If $r \neq 0$, then $r = g - qf \in I$, and $deg(r) < deg(f)$, contradiction. We get $g = fq \in (f)$, so $I \subseteq (f)$. □

Example 6.4.17. *Note that $\mathbb{Z}$ is not a field. $\mathbb{Z}[x]$ has ideals that are not principal, for example, $I = \{f \in \mathbb{Z}[x] | f(0) \in 2\mathbb{Z}\}$. Suppose $I = (g)$, since $2 \in I = (g)$, there exists $f \in \mathbb{Z}[x]$ such that $2 = fg$, so $deg(f) = deg(g) = 0$, f is a nonzero constant. If $g = \pm 1$, then $I = \mathbb{Z}[x]$, contradiction. If $|g| > 1$, then $x \notin (g)$, contradiction. We thus conclude I is not a principal ideal.*

Definition 6.4.18. A ring R is called an **integral domain** if for any $a, b \in R \setminus \{0\}$, $ab \neq 0$.

Example 6.4.19. *All the fields are integral domains.*

Exercise 6.4.20. *Show that $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if n is a prime.*

Definition 6.4.21. A **principal ideal domain** (PID) is an integral domain all of whose ideals are principal.

Example 6.4.22. *$\mathbb{Z}$ is a principal ideal domain.*

Proposition 6.4.23. *If R is an integral domain, then $R[x]$ is also an integral domain.*

Proof. If R is an integral domain, for any nonzero $f(x) = a_n x^n + ... + a_1 x + a_0, g(x) = b_m x^m + ... + b_1 x + b_0 \in R[x]$, the leading coefficient of fg is $a_n b_m \neq 0$, so fg is not the zero polynomial. □

Exercise 6.4.24. *If R is an integral domain, then $(R[x])^\times = R^\times$*

Exercise 6.4.25. *Verify that $\bar{2}x + \bar{1}$ is a unit in $\mathbb{Z}/4\mathbb{Z}[x]$*

Proposition 6.4.26. *R is an integral domain. Then $R[x]$ is a principal ideal domain if and only if R is a field.*

Proof. If R is a field, by Proposition 6.4.16 and Proposition 6.4.23, $R[x]$ is a principal ideal domain.

Conversely, if $R[x]$ is a principal ideal domain, for any $a \in R \setminus \{0\}$, consider the ideal $I = \{f \in R[x] | f(0) \in (a)\}$.By assumption, $I = (f)$ for some $f \in R[x]$. Since $a \in I$ is a constant polynomial, we get f is also a constant polynomial. Observe that $x \in I = (f)$, so $f \in R^\times$, $R[x] = (f) = I$. it follows $1 \in R[x] = I$, so $1 \in (a)$, we conclude $a \in R^\times$. □

Example 6.4.27. *let* $\gamma = \sqrt[3]{2}$. *Define* $\Phi : \mathbb{Q}[x] \longrightarrow \mathbb{C}$ *by* $\Phi(f(x)) = f(\gamma)$. *By Proposition 6.3.6, it is a ring homomorphism. Since* $\mathbb{Q}$ *is a field, by Proposition 6.4.26,* $\mathbb{Q}[x]$ *is a principal ideal domain. In particular,* $\ker\Phi$ *is a principal ideal. Indeed,* $\ker\Phi = (x^3 - 2)$*: since* $x^3 - 2 \in \ker\Phi$, *and* $\sqrt[3]{2}$ *is not a root of any linear or quadratic polynomial in* $\mathbb{Q}[x]$, *we see* $x^3 - 2$ *is a monic polynomial of lowest degree in* $\ker\Phi$, *we get* $\ker\Phi = (x^3 - 2)$

6.5 Quotient Rings

Definition 6.5.1. R is a ring and I is an ideal of R, the **quotient ring** R/I is the set of cosets of I in R with addition $(a+I)+(b+I) = (a+b)+I$ and multiplication $(a+I)(b+I) = ab+I$.

Exercise 6.5.2. *Verify that* R/I *defined above is a ring.*

Example 6.5.3. *In the ring* $\mathbb{Z}$, $n\mathbb{Z}$ *is an ideal. We have the quotient ring* $\mathbb{Z}/n\mathbb{Z}$.

Definition 6.5.4. R is a ring and I is an ideal of R. Define $\pi : R \longrightarrow R/I$ given by $\pi(r) = r + I$ to be the canonical projection map.

Exercise 6.5.5. *Show that* $\pi : R \longrightarrow R/I$ *is a ring homomorphism.*

Similar to groups, we have a First Isomorphism Theorem for Rings:

Theorem 6.5.6. *(First Isomorphism Theorem for Rings)* $f : R \longrightarrow R'$ *is a surjective ring homomorphism, and* $I = \ker(f)$, *then there exists a unique ring homomorphism* $F : R/I \longrightarrow R'$ *such that* $f = F \circ \pi$.

The proof will be an analogue to that of the First isomorphic Theorem for Groups, and F is given by $F(a+I) = f(a)$.

Example 6.5.7. *Let* $R = \mathbb{R}[x]$, *and* $I = (x^2+1)$. *Define a ring homomorphism*

$$\phi : \mathbb{R}[x] \longrightarrow \mathbb{C}$$

$$f(x) \mapsto f(i)$$

Claim that $\ker(\phi) = (x^2+1)$*: We know* $\ker(\phi)$ *is an ideal of* $\mathbb{R}[x]$, *and* $\mathbb{R}$ *is a field, so* $\mathbb{R}[x]$ *is a principal ideal domain, so* $\ker(\phi) = (f_0)$ *for some* $f_0 \in \mathbb{R}[x]$.

Observe that $f(x^2+1)=0$, *so* $x^2+1 \in \ker(\phi)$. *Also,* $\phi(f)=f(i)\neq 0$ *for any polynomial of degree* 0 *or* 1 *in* $\mathbb{R}[x]$. *So* x^2+1 *is a monic polynomial of lowest degree in* $\ker(\phi)$. *We conclude* $\ker(\phi)=(x^2+1)$.

Now apply Theorem 6.5.6, we see

$$\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$$

We can also study the quotient ring $\mathbb{R}[x]/(x^2+1)$ *itself without using the First Isomorphism Theorem. Let* $p(x)=x^2+1$, $I=(p(x))$. *We will see directly that* $R[x]/I$ *is a field:*

Every element of $R[x]/I$ *can be expressed in the form* $a+bx+I$*: given any* $f(x)+I$, *we can apply the division algorithm to get* $f(x)=(x^2+1)q(x)+r(x)$, *where* $r(x)=0$ *or* $deg(r)<\deg(p)=2$, *so* $r(x)=a+bx$ *for some* $a,b\in\mathbb{R}$. *It follows*

$$f(x)+I=(x^2+1)q(x)+r(x)+I=r(x)+I=a+bx+I$$

and the multiplication in the ring $R[x]/I$ *is given by*

$$(a+bx+I)(c+dx+I)=ac+(ad+bc)x+bdx^2+I=(ac-bd)+(ad+bc)x+I$$

Using the above formula we can verify that the multiplicative inverse for nonzero $a+bx+I$ *is* $\frac{a}{a^2+b^2}-\frac{b}{a^2+b^2}x+I$.

Example 6.5.8. *Let* $p(x)=x^2-1\in\mathbb{R}$, $I=(p(x))$. $R[X]/I$ *is not an integral domain since*

$$((x-1)+I)((x+1)+I))=(x-1)(x+1)+I=(x^2-1)+I=0+I$$

Similar argument as the above example implies that every element of $R[x]/I$ *can be expressed in the form* $ax+b+I$, *and the multiplication is given by*

$$(ax+b+I)(cx+d+I)=acx^2+(ad+bc)x+bd+I=(ad+bc)x+(ac+bd)+I$$

Definition 6.5.9. A proper ideal I in a ring R is **maximal** if for any ideal J of R such that $I\subseteq J$, either $J=I$ or $J=R$.

Example 6.5.10. (x) *is a maximal ideal in* $\mathbb{R}[x]$*: if* $J\supseteq(x)$ *is an ideal, and* $J\neq(x)$, *then it follows* J *contains a polynomial of degree zero, i.e. a unit, so* $J=\mathbb{R}[x]$.

Exercise 6.5.11. *Prove $n\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$ if and only if n is a prime.*

Proposition 6.5.12. *R is a ring and I is an ideal in R. Then I is a maximal ideal if and only if R/I is a field.*

Proof. If I is a maximal ideal, for any $x \notin I$, $I + (x)$ is an ideal in R and $I + (x) \supsetneqq I$, so $I + (x) = R$. In particular, $1 \in I + (x)$, so there exists $r \in R$ and $s \in I$ such that $1 = s + rx$. This implies $1 + I = rx + I = (r + I)(x + I)$, so $x + I$ is a unit in R/I. We conclude R/I is a field.

Conversely, if R/I is a field, then the only two ideals of R/I are $\{I\}$ and R/I. Suppose I is not a maximal ideal in R, then there exists ideal J in R such that $I \subsetneqq J \subsetneqq R$. But then $\{I\} \subsetneqq J/I \subsetneqq R/I$, so J/I is a proper ideal of R/I, contradiction. We conclude I is a maximal ideal in R. □

Definition 6.5.13. $\mathbb{F}$ is a field. $p(x) \in \mathbb{F}[x]$ is **irreducible** if $p(x)$ not constant and $p(x)$ is not a product of two non-constant polynomials in $\mathbb{F}[x]$.

Proposition 6.5.14. *The maximal ideals of $\mathbb{F}[x]$ are $(p(x))$, where $p(x)$ is an irreducible polynomial.*

Proof. $\mathbb{F}[x]$ is a principal ideal domain, so all its ideals are of form $I = (p(x))$.

If $p(x)$ is not irreducible, then $p(x) = f(x)g(x)$ for some non-constant $f(x)$ and $g(x)$. Then

$$I = (p(x)) \subsetneqq (g(x)) \subsetneqq \mathbb{F}[x]$$

we see I is not maximal.

Conversely, if $I = (p(x))$ is not a maximal ideal, then $I \subsetneqq (g(x)) \subsetneqq \mathbb{F}[x]$, which implies in particular $p(x) \in (g(x))$, so $p(x) = f(x)g(x)$ for some $f(x) \in \mathbb{F}[x]$. Note that $g(x)$ is not a constant, otherwise $(g(x)) = \mathbb{F}[x]$; also $f(x)$ is not a constant, otherwise $I = (g(x))$, so we conclude $p(x)$ is not irreducible. □

Corollary 6.5.15. *$\mathbb{F}$ is a field, $p(x) \in \mathbb{F}[x]$ is a nonconstant polynomial. $\mathbb{F}[x]/(p(x))$ is a field if and only if $p(x)$ is an irreducible polynomial.*

Example 6.5.16. *$x^2 + 1$ is irreducible in $\mathbb{R}[x]$, so $\mathbb{R}[x]/(x^2 + 1)$ is a field;*

$x^2 - 1 = (x - 1)(x + 1)$ is not irreducible in $\mathbb{R}[x]$, so $\mathbb{R}[x]/(x^2 + 1)$ is a not a field

Example 6.5.17. *The Fundamental Theorem of Algebra implies the irreducible polynomials of* $\mathbb{C}[z]$ *are the degree one polynomials* $z-a$*, where* $a \in \mathbb{C}$*. So we see there is a one-to-one correspondence between maximal ideals of* $\mathbb{C}[x]$ *and points on* $\mathbb{C}$*.*

Proposition 6.5.18. *R is a ring and $p(x) \in R[x]$ is a monic polynomial of degree n. Then each element of $R[x]/(p(x))$ is an R-linear combination of the elements $1+(p(x)), x+(p(x)), ..., x^{n-1}+(p(x))$.*

Proof. This can be proved by repeatedly applying the division algorithm. □

Definition 6.5.19. $\mathbb{F}$ and $\mathbb{E}$ are fields such that $\mathbb{F} \subseteq \mathbb{E}$. $\gamma \in \mathbb{E}$. If $p(x) \in \mathbb{F}[x]$ is the monic polynomial of least degree such that $f(\gamma) = 0$, we say $p(x)$ is the **minimal polynomial** of γ. γ is **algebrac** over $\mathbb{F}$ if its minimal polynomial exists, otherwise it is called **transcedental**.

Example 6.5.20. *The minimal polynomial of $\sqrt{2}$ in $\mathbb{Q}$ is $p(x) = x^2 - 2$, so $\sqrt{2}$ is algebraic over $\mathbb{Q}$.*

Example 6.5.21. *It can be proved that π and e are transcedental over $\mathbb{Q}$. You can find the proof in some textbooks such as Algebra by Serge Lang.*

Generalising the argument in Example 6.4.27, we have the following fact:

Proposition 6.5.22. *$\mathbb{F}$ and $\mathbb{E}$ are fields such that $\mathbb{F} \subseteq \mathbb{E}$. $\gamma \in \mathbb{E}$ has minimal polynomial $p(x) \in \mathbb{F}[x]$. Then the evaluation map $\Phi : \mathbb{F}[x] \longrightarrow \mathbb{E}$ defined by $\Phi(f(x)) = f(\gamma)$ is a homomorphism with $\ker(\Phi) = (p(x))$.*

Applying the First Isomorphism Theorem, we obtain an injective homomorphism $\bar{\Phi} : \mathbb{F}[x]/(p(x)) \longrightarrow \mathbb{E}$, and $\mathbb{F}[x]/(p(x)) \cong \mathrm{Im}(\bar{\Phi})$. We denote $\mathbb{F}(\gamma) = \mathrm{Im}(\bar{\Phi})$, so we finally get $\mathbb{F} \subseteq \mathbb{F}(\gamma) \cong \mathbb{F}[x]/(p(x))$, an extension of the field $\mathbb{F}$ that contains γ. This is indeed the smallest field that contains both $\mathbb{F}$ and γ.

6.6 Field of Fraction

The integer ring is not a field, since most of integers have no multiplicative inverse that are also integers. This makes the reversed operation of multiplication, i.e., division, not defined. We know from elementary school that the way to solve the issue is to introduce the concept of rational numbers,

the numbers which are fractions of integers. In this way, we obtain the ration number field $\mathbb{Q}$ that is an extension of the ring of integers, and it is the smallest field that contains the integers.

We can generalise the above construction for any integral domain R:

Lemma 6.6.1. *R is an integral domain. Define a relation on $S = R \times (R \setminus \{0\})$ by $(a, b) \sim (c, d)$ if $ad = bc$. This is an equivalence relation.*

Proof. 1. Reflexive: For any $(a, b) \in S$, $ab = ba$, so $(a, b) \sim (a, b)$

2. Symmetric: If $(a, b) \sim (c, d)$, then $ad = bc$, which is same as $cb = da$, so $(c, d) \sim (a, b)$

3. Transitive: If $(a, b) \sim (c, d)$ and $(c, d) \sim (g, h)$, then $ad = bc$ and $ch = dg$.

Case (i). $c = 0$. $ad = bc = 0$ and $gd = ch = 0$. Note $d \neq 0$ and R is an integral domain, we get $a = g = 0$, so $ah = bg = 0$, $(a, b) \sim (g, h)$.

Case (ii). $c \neq 0$. Take the product of the two equations, we have $(ad)(ch) = (bc)(dg)$, i.e., $(ah)(cd) = (bg)(cd)$. Then $(ah - bg)(cd) = 0$ and $cd \neq 0$, we conclude that $ah - bg = 0$, i.e., $ah = bg$, $(a, b) = (g, h)$.

□

From now on, The equivalence class of (a, b) will be written as a/b. The set of all equivalence classes is denoted by $F(R)$. $F(R)$ is a field if we define:

$$\begin{cases} \text{addition} : a/b + c/d = (ad + bc)/bd \\ \text{multiplication} : (a/b)(c/d) = (ac)/(bd) \end{cases}$$

This field is called the **field of fraction** of R.

Exercise 6.6.2. *Verify that $F(R)$ is a field.*

Exercise 6.6.3. *Verify that the additive identity of $F(R)$ is $0/1$, and the multiplicative identity of $F(R)$ is $1/1$.*

By this construction, we can include R into $F(R)$ in a natural way by identifying $r \in R$ with $r/1 \in F(R)$. So $F(R)$ is a field that contains R as a subset.

Example 6.6.4. *If R is already a field, then $F(R) = R$. Intuitively, there is no need to do extension since it is already a field.*

Example 6.6.5. *$\mathbb{F}$ is a field, then $\mathbb{F}[x]$ is an integral domain. The field of fraction of $\mathbb{F}[x]$ is the field of rational functions in one variable x with coefficients in $\mathbb{F}$. We usually denote this field as $\mathbb{F}(x)$. It is the smallest field that contain both $\mathbb{F}$ and x.*

The next theorems shows that $F(R)$ is the smallest extension of R:

Theorem 6.6.6. *R is an integral domain and K is a field. If $\varphi : R \longrightarrow K$ is an injective ring homomorphism with $\varphi(1_R) = 1_K$, then there is a unique extension of φ to a ring homomorphism $\Phi : F(R) \longrightarrow K$ given by $\Phi(a/b) = \varphi(a)\varphi(b)^{-1}$, and Φ is injective.*

Proof. First check Φ is a well defined map:

(1).If $a/b \in F(R)$, then $b \neq 0$, φ is injective $\Longrightarrow \varphi(b) \neq 0$, so in the field K, $\varphi(b)^{-1}$ exists.

(2).If $a/b = c/d$, then $ad = bc$, so $\varphi(a)\varphi(d) = \varphi(ad) = \varphi(bc) = \varphi(b)\varphi(c) \Longrightarrow \varphi(a)\varphi(b)^{-1} = \varphi(c)\varphi(d)^{-1} \Longrightarrow \Phi(a/b) = \Phi(c/d)$.

Next check it is a homomorphism:

$$\begin{aligned}\Phi(a/b) + \Phi(c/d) &= \varphi(a)\varphi(b)^{-1} + \varphi(c)\varphi(d)^{-1} \\ &= (\varphi(a)\varphi(d) + \varphi(b)\varphi(c))(\varphi(b)\varphi(d))^{-1} \\ &= (\varphi(ad + bc))\varphi(bd)^{-1} \\ &= \Phi((ad + bc)/bd) \\ &= \Phi(a/b + c/d)\end{aligned}$$

$$\begin{aligned}\Phi(a/b)\Phi(c/d) &= \varphi(a)\varphi(b)^{-1}\varphi(c)\varphi(d)^{-1} \\ &= \varphi(ac)\varphi(bd)^{-1} \\ &= \Phi(ac/bd) \\ &= \Phi((a/b)(c/d))\end{aligned}$$

Check the uniqueness: Suppose $\Psi : F(R) \longrightarrow K$ is a homomorphism extending φ, then $\Psi(r/1) = \varphi(r) = \Phi(r/1)$, and $\Psi(1/r)\Psi(r/1) = \Psi((1/r)(r/1)) = \Psi(1/1) = \varphi(1) = 1$ implies $\Psi(1/r) = \Psi(r/1)^{-1} = \varphi(r)^{-1}$. So $\Psi(a/b) = \Psi((a/1)(1/b)) = \Psi(a/1)\Psi(1/b) = \varphi(a)\varphi(b)^{-1} = \Phi(a/b)$.

Eventually we verify that Φ is injective: If $\Phi(a/b) = \Phi(c/d)$, then $\phi(a)\phi(b)^{-1} = \phi(c)\phi(d)^{-1}$. We get $\phi(ad) = \phi(bc)$, and ϕ is injective, so $ad = bc$, $a/b = c/d$, Φ is injective.

□