Basic Algebra

Dr. Arjun Paul

Assistant Professor
Department of Mathematics and Statistics
Indian Institute of Science Education and Research Kolkata,
Mohanpur - 741 246, Nadia,
West Bengal, India.
Email: arjun.paul@iiserkol.ac.in.

Version: August 8, 2023 at 9:23am (IST).

Note: This note will be updated from time to time.
If you find any potential mistakes/typos, please bring it to my notice.

To my students . . .

Contents

List of Symbols

$\emptyset$	Empty set
$\mathbb{Z}$	The set of all integers
$\mathbb{Z}_{\geq 0}$	The set of all non-negative integers
$\mathbb{N}$	The set of all natural numbers (i.e., positive integers)
$\mathbb{Q}$	The set of all rational numbers
$\mathbb{R}$	The set of all real numbers
$\mathbb{C}$	The set of all complex numbers
$<$	Less than
$\leq$	Less than or equal to
$>$	Greater than
$\geq$	Greater than or equal to
$\subset$	Proper subset
$\subseteq$	Subset or equal to
$\subsetneq$	Subset but not equal to (c.f. proper subset)
$\exists$	There exists
$\nexists$	Does not exists
$\forall$	For all
$\in$	Belongs to
$\notin$	Does not belong to
$\sum$	Sum
$\prod$	Product
$\pm$	Plus and minus
∞	Infinity
$\sqrt{a}$	Square root of a
$\cup$	Union
$\bigsqcup$	Disjoint union
$\cap$	Intersection
$A \to B$	A mapping into B
$a \mapsto b$	a maps to b
$\hookrightarrow$	Inclusion map
$A \setminus B$	A setminus B
$\cong$	Isomorphic to
$A := ...$	A is defined to be ...
$\square$	End of a proof

Symbol	Name	Symbol	Name
α	alpha	β	beta
γ	gamma	δ	delta
π	pi	ϕ	phi
φ	var-phi	ψ	psi
ϵ	epsilon	ε	var-epsilon
ζ	zeta	η	eta
θ	theta	ι	iota
κ	kappa	λ	lambda
μ	mu	ν	nu
υ	upsilon	ρ	rho
ϱ	var-rho	ξ	xi
σ	sigma	τ	tau
χ	chi	ω	omega
Ω	Capital omega	Γ	Capital gamma
Θ	Capital theta	Δ	Capital delta
Λ	Capital lambda	Ξ	Capital xi
Σ	Capital sigma	Π	Capital pi
Φ	Capital phi	Ψ	Capital psi

Some of the useful Greek alphabets

Chapter 1

Foundation of Arithmetic

1.1 What is a Natural Number?

We begin with axiomatic definition of the set of all *natural numbers*, known as *Peano's axioms*, also known as *Dedekind–Peano axioms*. This was originally proposed by Richard Dedekind in 1988, and was published in a simplified version as a collection of axioms in 1989 by Giuseppe Peano in his book *Arithmetices principia, nova methodo exposita* (in English: *The principles of arithmetic presented by a new method*). We define addition and multiplication of natural numbers, and briefly discuss their useful arithmetic properties (with outline of proofs) that we are familiar with from elementary mathematics courses, without possibly thinking *why and how these work?* The purpose of this section is to provide a *logical foundation of natural numbers and their arithmetic*.

Axiom 1.1.1 (Peano's axioms)**.** *There is a set* $\mathbb{N}$ *satisfying the following axioms.*

(P1) $1 \in \mathbb{N}$ *(so* $\mathbb{N} \neq \emptyset$*); the element* 1 *is called one.*

(P2) Axiom of equality: There is a relation " $=$ *" on* $\mathbb{N}$*, called the equality, satisfying the following properties.*

(i) $a = a, \forall\, a \in \mathbb{N}$,

(ii) given $a, b \in \mathbb{N}$*, we have* $a = b \;\Rightarrow\; b = a$*, and*

(iii) given $a, b, c \in \mathbb{N}$*, if* $a = b$ *and* $b = c$*, then* $a = c$*.*

In other words, the relation " $=$ *" on* $\mathbb{N}$ *is an equivalence relation on* $\mathbb{N}$*. If "*$a = b$*", we say that "*a *is equal to* b*". If "*$a = b$*" is not true, we say that "*a *is not equal to* b*", expressed symbolically as "*$a \neq b$*".*

*(***Remark:** *The axiom (P2) was included in the original list of axioms published by Peano in 1889. However, since the axiom (P2) is logically valid in first-order logic with equality, this is always accepted, and is not considered to be a part of Axiom 1.1.1 in modern treatments.)*

(P3) For each $n \in \mathbb{N}$*, there is a unique* $s(n) \in \mathbb{N}$*, called the successor of* n*.*

(P4) 1 *is not a successor of any element of* $\mathbb{N}$*.*

(P5) Given $m, n \in \mathbb{N}$ *with* $m \neq n$*, we have* $s(m) \neq s(n)$*.*

(P6) Principle of Mathematical Induction: If a subset $S \subseteq \mathbb{N}$ *has properties that*

(i) $1 \in S$*, and*

(ii) $n \in S \;\Rightarrow\; s(n) \in S$*,*

then $S = \mathbb{N}$*.*

The elements of $\mathbb{N}$ are called natural numbers, and hence $\mathbb{N}$ is called the set of all natural numbers.

Exercise 1.1.2. Verify that $s : \mathbb{N} \to \mathbb{N},\ n \mapsto s(n)$ is injective but not surjective.

Remark 1.1.3. In contrast to our naive intuition, the properties (P1)–(P5) in Peano's Axioms 1.1.1 do not guarantee that the successor function generates all natural numbers (we are familiar with) except for 1. To make our naive intuition works, we need the assumption (P6), known as the Principle of Mathematical Induction.

Lemma 1.1.4. *If $n \in \mathbb{N}$ with $n \neq 1$, then there is a unique element $p(n) \in \mathbb{N}$, called the predecessor of n, such that $s(p(n)) = n$.*

Proof. Since $s : \mathbb{N} \to \mathbb{N},\ n \mapsto s(n)$ is injective by (P5), uniqueness of $p(n)$ follows. To show existence of $p(n)$, for each $n \in \mathbb{N} \setminus \{1\}$, it is enough to show that

$$s(\mathbb{N}) := \{s(n) : n \in \mathbb{N}\} = \mathbb{N} \setminus \{1\}.$$

Since $1 \notin s(\mathbb{N}) := \{s(n) : n \in \mathbb{N}\}$ by (P4), to show that $s(\mathbb{N}) = \mathbb{N} \setminus \{1\}$, it is enough to show that

$$T := s(\mathbb{N}) \cup \{1\} = \mathbb{N}.$$

Clearly $T \subseteq \mathbb{N}$ and $1 \in T$. If $m \in T$, then $m = 1$ or $m = s(n)$, for some $n \in \mathbb{N}$, and so in both cases, $s(m) \in T$ by construction of T. Then (P6) tells us that $T = \mathbb{N}$. This completes the proof. □

Definition 1.1.5. A *binary operation* on a set S is a map $S \times S \to S$.

Definition 1.1.6. On the set $\mathbb{N}$, we define two binary operations

$$\textit{Addition} \quad + : \mathbb{N} \times \mathbb{N} \to \mathbb{N},\ (m, n) \mapsto m + n, \tag{1.1.7}$$

$$\text{and } \textit{Multiplication} \quad \cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N},\ (m, n) \mapsto m \cdot n\,. \tag{1.1.8}$$

using the following rules given by the *recurrence relations*[1]:

Rule for addition of natural numbers:

$$n + 1 := s(n),\ \forall\, n \in \mathbb{N}, \text{ and} \tag{1.1.9}$$

$$n + s(m) := s(n + m),\ \forall\, n, m \in \mathbb{N}. \tag{1.1.10}$$

Rule for multiplication of natural numbers:

$$n \cdot 1 := n,\ \forall\, n \in \mathbb{N}, \text{ and} \tag{1.1.11}$$

$$n \cdot s(m) := (n \cdot m) + n,\ \forall\, n, m \in \mathbb{N}. \tag{1.1.12}$$

Lemma 1.1.13. *The above rules (1.1.9)–(1.1.10) defines a unique binary operation on $\mathbb{N}$, called addition of natural numbers satisfying those properties.*

Proof. To check uniqueness of the binary operation $+$ satisfying the properties (1.1.9)–(1.1.10), let $\oplus : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be any binary operation on $\mathbb{N}$ satisfying the following properties:

(A') $n \oplus 1 = s(n), \forall\, n \in \mathbb{N}$, and

(B') $n \oplus s(m) = s(n \oplus m), \forall\, n, m \in \mathbb{N}$.

Let $m \in \mathbb{N}$ be arbitrary but fixed after choice. Let $A := \{n \in \mathbb{N} : m + n = m \oplus n\} \subseteq \mathbb{N}$. Since $m + 1 = s(m) = m \oplus 1$, $1 \in A$. If $n \in A$, then $m + n = m \oplus n$, and so $m + s(n) = s(m + n) =$

[1] A relation that recalls itself repeatedly to generate its complete meaning.

$s(m \oplus n) = m \oplus s(n)$. Therefore, $s(n) \in A$, and hence by principle of mathematical induction (see (P6) in Axiom 1.1.1) we have $A = \mathbb{N}$. This proves uniqueness of the binary operation $+$ on $\mathbb{N}$.

Let $n \in \mathbb{N}$ be arbitrary but fixed after choice. Let

$$T_n := \{m \in \mathbb{N} : n + m \text{ is defined}\}.$$

Clearly $T_n \subseteq \mathbb{N}$. We want to show that $T_n = \mathbb{N}$. Now $1 \in T_n$ by axiom (1.1.9). If $m \in T_n$, then $n + m$ is defined, and so by axiom 1.1.10 $n + s(m)$ is defined. So $s(m) \in T_n$. Then by principle of mathematical induction (see (P6) in Peano's Axiom 1.1.1) we have $T_n = \mathbb{N}$. □

Lemma 1.1.14. *The above rules* (1.1.11)–(1.1.12) *defines a unique binary operation on* $\mathbb{N}$*, called the multiplication of natural numbers satisfying those properties.*

Proof. Left as an exercise. □

Now you know why and how you could add and multiply any two natural numbers!

Definition 1.1.15. Let $* : S \times S \to S$ be a binary operation on a set S. We say that $*$

(i) is *associative* if $(a * b) * c = a * (b * c),\ \forall\ a, b, c \in S$;

(ii) is *commutative* if $a * b = b * a,\ \ \forall\ a, b \in S$;

(iii) *distributes* over a binary operation $\boxplus : S \times S \to S$ if for all $a, b, c \in S$ we have

$$a * (b \boxplus c) = (a * b) \boxplus (a * c),$$
$$(a \boxplus b) * c = (a * c) \boxplus (b * c).$$

The following result is well-known, however, it is strongly recommended to verify these in details purely using Peano's Axioms 1.1.1, and the axioms (or, definition) for addition and multiplication (1.1.9)–(1.1.12).

Theorem 1.1.16. *For all* $a, b, c \in \mathbb{N}$*, the following statements hold.*

(i) Associativity for addition: $(a + b) + c = a + (b + c)$.

(ii) Commutativity for addition: $a + b = b + a$.

(iii) Left distribution of multiplication over addition: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

(iv) Right distribution of multiplication over addition: $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.

(v) Commutativity for multiplication: $a \cdot b = b \cdot a$.

(vi) Associativity for multiplication: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Proof. (i) *Proof of associativity of addition:* Let $a, b \in \mathbb{N}$ be arbitrary but fixed after choices. Let

$$T_{a,b} := \{c \in \mathbb{N} : a + (b + c) = (a + b) + c\}.$$

Clearly $T_{a,b} \subseteq \mathbb{N}$. To prove associativity for addition, we need to show that $T_{a,b} = \mathbb{N}$. Since

$$\begin{aligned} a + (b + 1) &= a + s(b), \text{ by axiom (1.1.9).} \\ &= s(a + b), \text{ by axiom 1.1.10.} \\ &= (a + b) + 1, \text{ by axiom 1.1.9,} \end{aligned}$$

we conclude that $1 \in T_{a,b}$. Suppose that $c \in T_{a,b}$ be arbitrary. Then

$$\begin{aligned} a + (b + s(c)) &= a + s(b + c), \text{ by axiom (1.1.10).} \\ &= s(a + (b + c)), \text{ by axiom (1.1.10).} \\ &= s((a + b) + c), \text{ by axiom (1.1.10).} \\ &= (a + b) + s(c), \text{ by axiom (1.1.10).} \end{aligned}$$

Therefore, $s(c) \in T_{a,b}$. Then by principle of mathematical induction (see (P6) in Peano's Axiom 1.1.1) we have $T_{a,b} = \mathbb{N}$. (Now you know why $1 + (2 + 3) = (1 + 2) + 3$.)

(ii) *Proof of commutativity of addition:* For each $a \in \mathbb{N}$, let $S_a := \{b \in \mathbb{N} : a + b = b + a\} \subseteq \mathbb{N}$. We first show that $S_1 = \mathbb{N}$. Clearly $1 \in S_1$. If $b \in S_1$, then

$$\begin{aligned} s(b) + 1 &= s(s(b)), \text{ by axiom 1.1.9.} \\ &= s(b + 1), \text{ by axiom 1.1.9.} \\ &= s(1 + b), \text{ since } b \in S_1 \text{ by assumption.} \\ &= 1 + s(b), \text{ by axiom 1.1.10.} \end{aligned}$$

Therefore, $s(b) \in S_1$, and hence $S_1 = \mathbb{N}$ by (P6) in Axiom 1.1.1. Now let $a \in \mathbb{N}$ be arbitrary but fixed after choice. Since $S_1 = \mathbb{N}$, we have $1 \in S_a$. If $b \in S_a$, then $a + b = b + a$, and so we have

$$\begin{aligned} a + s(b) &= s(a + b), \quad \text{by axiom (1.1.10).} \\ &= s(b + a), \quad \text{since } b \in S_a \text{ by assumption.} \\ &= (b + a) + 1, \quad \text{by axiom (1.1.9).} \\ &= 1 + (b + a), \quad \text{since } b + a \in \mathbb{N} = S_1. \\ &= (1 + b) + a, \quad \text{using associativity of addition.} \\ &= (b + 1) + a, \quad \text{since } b \in \mathbb{N} = S_1. \\ &= s(b) + a, \quad \text{by axiom (1.1.9).} \end{aligned}$$

Then $s(b) \in S_a$, and hence by (P6) in Peano's Axiom 1.1.1 we have $S_a = \mathbb{N}$.

(iii) *Proof of left distribution of multiplication over addition:* Let $a, b \in \mathbb{N}$ be arbitrary but fixed after choices. Let

$$D_{a,b} := \{c \in \mathbb{N} : a \cdot (b + c) = (a \cdot b) + (a \cdot c)\} \subseteq \mathbb{N}.$$

We need to show that $D_{a,b} = \mathbb{N}$. Note that,

$$\begin{aligned} a \cdot (b + 1) &= a \cdot s(b), \text{ by axiom (1.1.9);} \\ &= (a \cdot b) + a, \text{ by axiom (1.1.12);} \\ &= (a \cdot b) + (a \cdot 1), \text{ by axiom (1.1.9).} \end{aligned}$$

Therefore, $1 \in D_{a,b}$. Suppose that $c \in D_{a,b}$. Then

$$\begin{aligned} a \cdot (b + s(c)) &= a \cdot s(b + c), \text{ by axiom (1.1.10);} \\ &= a \cdot (b + c) + a, \text{ by axiom (1.1.12);} \\ &= ((a \cdot b) + (a \cdot c)) + a, \text{ since } c \in D_{a,b} \text{ by assumption;} \\ &= (a \cdot b) + ((a \cdot c) + a), \text{ by associativity for addition;} \\ &= (a \cdot b) + (a \cdot s(c)), \text{ by axiom (1.1.12).} \end{aligned}$$

So $s(c) \in D_{a,b}$. Therefore, by (P6) of Axiom 1.1.1 we have $D_{a,b} = \mathbb{N}$.

(iv) *Proof of right distribution of multiplication over addition:* Left as an exercise.

(v) *Proof of commutativity of multiplication:* Given $a \in \mathbb{N}$, let

$$S_a := \{b \in \mathbb{N} : a \cdot b = b \cdot a\}.$$

We first consider the case $a = 1$. Clearly $1 \in S_1$. If $b \in S_1$, then

$$\begin{aligned} 1 \cdot s(b) &= 1 \cdot (b+1), \text{ by axiom (1.1.9).} \\ &= (1 \cdot b) + (1 \cdot 1), \text{ by left distribution of multiplication over addition.} \\ &= (b \cdot 1) + (1 \cdot 1), \text{ since } b \in S_1. \\ &= (b+1) \cdot 1, \text{ by right distribution of multiplication over addition.} \\ &= s(b) \cdot 1, \text{ by axiom (1.1.9).} \end{aligned}$$

Thus, $s(b) \in S_1$. Therefore, by principle of mathematical induction we have $S_1 = \mathbb{N}$. Now assume that $a \neq 1$. Since $S_1 = \mathbb{N}$, we have $1 \in S_a$. Suppose that $b \in S_a$. Then

$$\begin{aligned} a \cdot s(b) &= (a \cdot b) + a, \text{ by axiom (1.1.12).} \\ &= (b \cdot a) + (1 \cdot a), \text{ since } 1 \in S_a \Rightarrow 1 \cdot a = a \cdot 1 = a. \\ &= (b+1) \cdot a, \text{ by Theorem 1.1.16 (iv).} \\ &= s(b) \cdot a, \text{ by axiom 1.1.9.} \end{aligned}$$

So $s(b) \in S_a$, and hence $S_a = \mathbb{N}$ by principle of mathematical induction.

(vi) *Proof of associativity of multiplication:* Left as an exercise! Let $a, b \in \mathbb{N}$ be arbitrary but fixed after choice. Let

$$M_{a,b} := \{c \in \mathbb{N} : a \cdot (b \cdot c) = (a \cdot b) \cdot c\}.$$

Clearly $M_{a,b} \subseteq \mathbb{N}$. To prove associativity for multiplication, we need to show that $M_{a,b} = \mathbb{N}$. Since $n \cdot 1 = n$, $\forall\, n \in \mathbb{N}$ by axiom (1.1.11), we have $a \cdot (b \cdot 1) = a \cdot b = (a \cdot b) \cdot 1$. So $1 \in M_{a,b}$. Suppose that $c \in M_{a,b}$. Then

$$\begin{aligned} a \cdot (b \cdot s(c)) &= a \cdot ((b \cdot c) + b), \text{ by axiom (1.1.12).} \\ &= a \cdot (b \cdot c) + (a \cdot b), \text{ by Theorem 1.1.16 (iii).} \\ &= (a \cdot b) \cdot c + (a \cdot b), \text{ by Theorem 1.1.16 (v).} \\ &= (a \cdot b) \cdot s(c), \text{ by axiom 1.1.12.} \end{aligned}$$

Therefore, $s(c) \in M_{a,b}$, and hence by principle of mathematical induction we have $M_{a,b} = \mathbb{N}$.

□

Proposition 1.1.17. *For each $n, a \in \mathbb{N}$, we have $s^n(a) = a + n$, where $s^n : \mathbb{N} \to \mathbb{N}$ is the n-times composition of s with itself (e.g., $s^2 = s \circ s$, $s^3 = s \circ s \circ s$ etc.).*

Proof. Let $T := \{n \in \mathbb{N} : s^n(a) = a + n,\ \forall\, a \in \mathbb{N}\}$. Clearly $T \subseteq \mathbb{N}$, and $1 \in T$ by axiom 1.1.9. Assume that $n \in T$. Then $s^{s(n)}(a) = s^{n+1}(a) = s(s^n(a)) = s(a+n) = (a+n)+1 = a+(n+1) = a + s(n)$. So $s(n) \in T$. Then by principle of mathematical induction we have $T = \mathbb{N}$. □

Lemma 1.1.18. *Let $a, b, n \in \mathbb{N}$. If $a + n = b + n$, then $a = b$.*

Proof. Note that the successor map $s : \mathbb{N} \to \mathbb{N}$ is injective by (P5) in Axiom 1.1.1. Since $s^n(a) = a + n = b + n = s^n(b)$ by Proposition 1.1.17, and composition of injective maps is injective, we have $a = b$. □

Exercise 1.1.19 (Cancellation for multiplication)**.** Let $a, b, r, \ell \in \mathbb{N}$.

(i) If $\ell a = \ell b$, show that $a = b$.

(ii) If $ar = br$, show that $a = b$.

Exercise 1.1.20. Let $a \in \mathbb{N}$. Show that the equation $x + a = 1$ has no solution for x in $\mathbb{N}$.

Theorem 1.1.21 (Law of trichotomy for natural numbers)**.** *Given $a, b \in \mathbb{N}$, exactly one of the following three conditions holds:*

(i) $a = b$,

(ii) $a = b + c$, *for some* $c \in \mathbb{N}$, *or*

(iii) $b = a + d$, *for some* $d \in \mathbb{N}$.

Proof. We first show that no two conditions among (i)–(iii) can hold simultaneously. If (i) and (ii) holds simultaneously, then $b = b + c$ implies $s(b) = s(b + c) \Rightarrow b + 1 = (b + c) + 1 = b + (c + 1) \Rightarrow 1 = c + 1 = s(c)$, which contradicts axiom (P4) in Peano's Axioms 1.1.1. The same argument shows that (i) and (iii) cannot hold simultaneously. If (ii) and (iii) hold simultaneously, then we have $a = b + c = (a + c) + d = a + (c + d)$, for some $c, d \in \mathbb{N}$. Then applying successor map we see that $a + 1 = (a + (c + d)) + 1 = a + ((c + d) + 1)$. Then by Lemma 1.1.18 we have $1 = (c + d) + 1 = s(c + d)$, which contracts (P4) in Peano's Axioms 1.1.1. Therefore, no two conditions among (i)–(iii) can hold simultaneously.

We now show that at least one of (i)–(iii) holds. For each $a \in \mathbb{N}$, let

$$S_a := \{b \in \mathbb{N} : \text{ at least one of (i) or (ii) or (iii) holds}\}.$$

Consider the case $a = 1$. Clearly $1 \in S_1$. Suppose that $b \in S_1$. Then $s(b) = b + 1 = a + b$ satisfies condition (iii), and so $s(b) \in S_1$. Then by (P6) in Peano's Axioms we have $S_1 = \mathbb{N}$. Suppose that $a \in \mathbb{N} \setminus \{1\}$ be arbitrary but fixed after choice. Since $b = 1$ satisfies $a = s(p(a)) = p(a) + 1 = p(a) + b$, with $p(a) \in \mathbb{N}$, the condition (ii) holds for $b = 1$, and so $1 \in S_a$. Suppose that $b \in S_a$. Then we have the following cases:

(I) If $a = b$, then $s(b) = b + 1 = a + 1$, and so $s(b)$ satisfies condition (iii). So $s(b) \in S_a$.

(II) If $a = b + c$, for some $c \in \mathbb{N}$, then $a = s(b)$ or $a = s(b) + p(c)$ depending on whether $c = 1$ or $c \in \mathbb{N} \setminus \{1\}$, respectively. So in both cases, $s(b) \in S_a$.

(III) If $b = a + d$, for some $d \in \mathbb{N}$, then $s(b) = b + 1 = a + (d + 1)$ satisfies condition (iii), and hence $s(b) \in S_a$.

Therefore, $S_a = \mathbb{N}$ by principle of mathematical induction. □

The law of trichotomy in Theorem 1.1.21 allow us to define usual order relation " $<$ " on $\mathbb{N}$ as follow.

Definition 1.1.22. Given $a, b \in \mathbb{N}$, we define $a < b$ if $\exists\ c \in \mathbb{N}$ such that $a + c = b$. If $a < b$, we say that "*a is strictly less than b*".

Note that " $<$ " is a relation on $\mathbb{N}$ which is neither reflexive nor symmetric or anti-symmetric. We show that it is a transitive relation on $\mathbb{N}$. If $a < b$ and $b < c$, then $a + r = b$ and $b + s = c$, for some $r, s \in \mathbb{N}$, and then $a + (r + s) = (a + r) + s = b + s = c$ shows that $a < c$. If $a < b$ we say that "*a is less than b*". The relation " $<$ " is called the *usual ordering relation* on $\mathbb{N}$. Define another relation " $\leq$ " on $\mathbb{N}$ by setting

$$a \leq b \quad \text{if either } a = b \text{ or } a < b.$$

If $a \leq b$, we say that "*a is less than or equal to b*". It is easy to see that " $\leq$ " is reflexive and transitive. We show that " $\leq$ " is anti-symmetric, and hence is a partial order relation on $\mathbb{N}$.

Suppose that $a, b \in \mathbb{N}$ with $a \leq b$ and $b \leq a$. We want to show that $a = b$. Suppose on the contrary that $a \neq b$. Then we must have $a < b$ and $b < a$. Then there exist $c, d \in \mathbb{N}$ such that $a + c = b$ and $b + d = a$. Then

$$\begin{aligned}
&(b + d) + c = a + c = b \\
\Rightarrow\ & b + (d + c) = b, \text{ using associativity of addition.} \\
\Rightarrow\ & s(b + (d + c)) = s(b), \text{ applying successor map.} \\
\Rightarrow\ & (b + (d + c)) + 1 = b + 1, \text{ using axiom 1.1.10.} \\
\Rightarrow\ & b + ((d + c) + 1) = b + 1, \text{ using associativity of addition.} \\
\Rightarrow\ & (d + c) + 1 = 1, \text{ using Lemma 1.1.18.} \\
\Rightarrow\ & s(d + c) = 1.
\end{aligned}$$

This contradicts axiom (P4) in Peano's Axioms 1.1.1. Therefore, we must have $a = b$ as required.

Definition 1.1.23. A partial order relation ρ on a set S is called a *total order* if for any two elements $a, b \in S$, at least one of $a \,\rho\, b$ and $b \,\rho\, a$ holds. A non-empty set S together with a total order relation is called a *well-ordered set*.

As an immediate consequence of the law of trichotomy of natural numbers (Theorem 1.1.21) we see that " $\leq$ " is a total order relation on $\mathbb{N}$, and hence $(\mathbb{N}, \leq)$ is a well-ordered set.

Theorem 1.1.24. *The following are equivalent.*

(i) Principle of mathematical induction (regular version): Let $S \subseteq \mathbb{N}$ be such that

(a) $1 \in S$, and

(b) for each $n \in \mathbb{N}$, $n \in S$ implies $s(n) \in S$.

Then $S = \mathbb{N}$.

(ii) Principle of mathematical induction (strong version): Let $T \subseteq \mathbb{N}$ be such that

(a') $1 \in T$, and

(b') for each $n \in \mathbb{N}$, $J_n := \{k \in \mathbb{N} : k \leq n\} \subseteq T$ implies $s(n) \in T$.

Then $T = \mathbb{N}$.

Proof. (i) $\Rightarrow$ (ii): Suppose that the conditions (a') and (b') holds for $T \subseteq \mathbb{N}$. Since $1 \in T$ by (a'), to show $T = \mathbb{N}$ using the regular version of principle of mathematical induction (i), it is enough to show that for each $n \in \mathbb{N}$, the statement

$$P_n : \quad \text{"}n \in T \text{ implies } s(n) \in T\text{."}$$

holds. Consider the set

$$S := \{n \in \mathbb{N} : P_k \text{ holds, } \forall\, k \leq n\} \subseteq \mathbb{N}.$$

Since $1 \in T$ by (a'), we have $J_1 = \{1\} \subseteq T$, and hence by (b') we have $s(1) \in T$. Therefore, P_1 holds, and so $1 \in S$. Let $n \in S$ be arbitrary but fixed after choice. Then $P_1, \ldots, P_n$ hold, and hence we have $J_{s(n)} = \{k \in \mathbb{N} : k \leq s(n)\} \subseteq T$. Then by the condition (b') we have $s(s(n)) \in T$, and hence $P_{s(n)}$ holds. Therefore, P_k holds, $\forall\, k \leq s(n)$, and hence $s(n) \in S$. Then by (i) we have $S = \mathbb{N}$. Thus, $T = \mathbb{N}$.

(ii) $\Rightarrow$ (i): Let $S \subseteq \mathbb{N}$ be such that $1 \in S$, and $n \in S$ implies $s(n) \in S$. To show $S = \mathbb{N}$ using the strong version of principle of mathematical induction (ii), we just need to ensure that for each $n \in \mathbb{N}$, if $J_n \subseteq S$ then $s(n) \in S$. But this follows because $n \in J_n$ implies that $n \in S$, and so $s(n) \in S$ by (a). Then by (ii) we have $S = \mathbb{N}$. This proves (i). □

Theorem 1.1.25. *The following are equivalent.*

(i) Principle of Mathematical Induction (strong version): Let $S \subseteq \mathbb{N}$ be such that

(a) $1 \in S$, and

(b) for each $n \in \mathbb{N}$ with $n > 1$, if $\{k \in \mathbb{N} : k < n\} \subseteq S$ then $n \in S$.

Then $S = \mathbb{N}$.

(ii) Well-ordering principle of $(\mathbb{N}, \leq)$: Any non-empty subset of $\mathbb{N}$ has a least element.

Proof. (i) $\Rightarrow$ (ii): Suppose on the contrary that there is a non-empty subset $S \subseteq \mathbb{N}$ which has no least element. Let

$$T := \mathbb{N} \setminus S = \{n \in \mathbb{N} : n \notin S\}.$$

Since 1 is the least element of $\mathbb{N}$, we have $1 \notin S$; for otherwise 1 would be the least element of S. Therefore, $1 \in T$ and hence T is a non-empty subset of $\mathbb{N}$. Let $n \in \mathbb{N}$ with $n > 1$, and suppose that for any $k \in \mathbb{N}$ with $k < n$, we have $k \in T$. Then $n \notin S$, for otherwise n would be the least element of S. So $n \in T$. Then by principle of mathematical induction (strong version), we have $T = \mathbb{N}$. This contradicts our assumption that S is non-empty. So S must have a least element.

(ii) $\Rightarrow$ (i): Let $S \subseteq \mathbb{N}$ be such that

(a) $1 \in S$, and

(b) for each $n \in \mathbb{N}$ with $n > 1$, if $\{k \in \mathbb{N} : k < n\} \subseteq S$ then $n \in S$.

Assuming well-ordering principle of $(\mathbb{N}, \leq)$, we want to show that $S = \mathbb{N}$. Suppose on the contrary that $S \neq \mathbb{N}$. Then $T := \mathbb{N} \setminus S$ is a non-empty subset of $\mathbb{N}$, and so by (i) it has a least element, say $n \in T$. Since $1 \in S$ by assumption, $n > 1$. Since n is the least element of T, for any $k \in \mathbb{N}$ with $k < n$, we have $k \in \mathbb{N} \setminus T = S$. Then by property (b) of S we have $n \in S$, which is a contradiction. This completes the proof. □

1.2 Integers: Construction & Basic Operations

Let $a, b \in \mathbb{N}$. Suppose that we want to solve the equation

$$x + a = b \tag{1.2.1}$$

to find x. If $a < b$ in $\mathbb{N}$, then there is $r \in \mathbb{N}$ such that $b = r + a$. If there is another number $s \in \mathbb{N}$ such that $b = s + a$, then $r + a = s + a$ implies $r = s$. So the solution of the equation (1.2.1) exists and is unique; we denote this solution by $a - b \in \mathbb{N}$. Now the problem is if $a \leq b$, we don't have any solution of this equation in $\mathbb{N}$. This forces us to enlarge our natural number system to a bigger number system where we can find solutions to such linear equations.

Define a relation $\sim$ on the Cartesian product $\mathbb{N} \times \mathbb{N}$ by setting

$$(a, b) \sim (c, d), \quad \text{if } a + d = b + c. \tag{1.2.2}$$

It is an easy exercise to show that $\sim$ is an equivalence relation on $\mathbb{N} \times \mathbb{N}$. The $\sim$-equivalence class of $(a, b) \in \mathbb{N} \times \mathbb{N}$ is the subset

$$[(a, b)] := \{(c, d) \in \mathbb{N} \times \mathbb{N} \,\big|\, (a, b) \sim (c, d)\}. \tag{1.2.3}$$

Let $\mathbb{Z} := \{[(a, b)] : a, b \in \mathbb{N}\}$ be the associated set of all $\sim$-equivalence classes. The idea is to think of the equivalence class $[(a, b)]$ to be the solution of the equation $x + b = a$. The elements of $\mathbb{Z}$ are called *integers*, and $\mathbb{Z}$ is called the *set of all integers*.

Define a map

$$\iota : \mathbb{N} \to \mathbb{Z}$$

by

$$\iota(n) = [(s(n), 1)], \ \ \forall\, n \in \mathbb{N}.$$

Then $\iota(n) = \iota(m) \ \Rightarrow\ [(s(n), 1)] = [(s(m), 1)] \ \Rightarrow\ s(n) + 1 = s(m) + 1 \ \Rightarrow s(s(n)) = s(s(m)) \ \Rightarrow\ s(n) = s(m) \ \Rightarrow\ n = m$, since $s : \mathbb{N} \to \mathbb{N}$ is an injective map. Therefore, $\iota : \mathbb{N} \to \mathbb{Z}$ is an injective map, and hence we can use it to identify $\mathbb{N}$ as a subset of $\mathbb{Z}$. For notational simplicity, we may denote by n the element $[(s(n), 1)] \in \mathbb{Z}$, for all $n \in \mathbb{N}$.

Define a binary operation on $\mathbb{Z}$, called *addition of integers*, by

$$[(a, b)] + [(c, d)] := [(a + c, b + d)], \ \ \forall\, [(a, b)], [(c, d)] \in \mathbb{Z}. \tag{1.2.4}$$

Note that, if $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$, then $(a + c, b + d) \sim (a' + c', b' + d')$. Therefore, we have a well-defined binary operation $+$ on $\mathbb{Z}$.

Exercise 1.2.5. Show that the addition of integers is associative and commutative.

Exercise 1.2.6. Verify that,

$$\iota(m + n) = \iota(m) + \iota(n), \ \ \forall\, m, n \in \mathbb{N}.$$

Therefore, the addition operation on integers preserves the addition operation on natural numbers defined earlier.

Note that, the element $[(1, 1)] \in \mathbb{Z}$ satisfies

$$[(a, b)] + [(1, 1)] = [(a, b)] = [(1, 1)] + [(a, b)].$$

We denote by 0 (pronounced as *zero*) the element $[(1, 1)] \in \mathbb{Z}$. Since

$$[(s(n), 1)] + [(1, s(n))] = [(1, 1)] = 0, \ \ \forall\, n \in \mathbb{N},$$

for notational simplicity (for peaceful working notations), we denote by $-n$ the element $[(1, s(n))] \in \mathbb{Z}$, for all $n \in \mathbb{N}$. The element of $\mathbb{Z}$ of the form n and $-n$ are called *positive integers* and *negative integers*, respectively.

Exercise 1.2.7. The subsets $\mathbb{Z}^- := \{[(1, s(n))] : n \in \mathbb{N}\}$, $\{0\} := \{[(1, 1)]\}$ and $\mathbb{Z}^+ := \{[(s(n), 1)] : n \in \mathbb{N}\}$ are mutually disjoint, and their union is $\mathbb{Z}$. As a result, we may write the set $\mathbb{Z}$ as

$$\mathbb{Z} = \{-n : n \in \mathbb{N}\} \cup \{0\} \cup \mathbb{N}.$$

The elements of $\mathbb{Z}^-$ and $\mathbb{Z}^+$ are called the *negative integers* and the *positive integers*, respectively.

We define another binary operation on $\mathbb{Z}$, called the *product* operation, by

$$[(a, b)] \cdot [(c, d)] := [(ac + bd, ad + bc)], \ \ \forall\, [(a, b)], [(c, d)] \in \mathbb{Z}. \tag{1.2.8}$$

It is easy to check that, if $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$, then $(ac + bd, ad + bc) \sim (a'c' + b'd', a'd' + b'c')$, and hence the product operation is well-defined. One can easily check that,

(i) $[(a, b)] \cdot [(c, d)] = [(c, d)] \cdot [(a, b)]$,

(ii) $[(s(m), 1)] \cdot [(s(n), 1)] = [(s(mn), 1)]$.

Remark 1.2.9. With the above definitions and notations, one can check that the binary operations addition and multiplication of integers are associative, commutative, and multiplication distributes over addition. In other words, the following properties hold.

(i) $(a + b) + c = a + (b + c), \ \ \forall\, a, b, c \in \mathbb{Z}$;

(ii) $(ab)c = a(bc), \ \forall\, a, b, c \in \mathbb{Z}$;

(iii) $a + b = b + a, \ \forall\, a, b \in \mathbb{Z}$;

(iv) $ab = ba, \ \forall\, a, b \in \mathbb{Z}$;

(v) $a(b + c) = (ab) + (ac), \ \forall\, a, b, c \in \mathbb{Z}$;

(vi) $(a + b)c = (ac) + (bc), \ \forall\, a, b, c \in \mathbb{Z}$.

Exercise 1.2.10. Let $n \in \mathbb{Z}$. If $a + n = b + n$, for some $a, b \in \mathbb{Z}$, show that $a = b$.

We define the *usual ordering* relation " $\leq$ " on $\mathbb{Z}$ as follow: given $m, n \in \mathbb{Z}$, we define

$$m \leq n \text{ if } \exists\, r \in \mathbb{N} \cup \{0\} \text{ such that } m + r = n.$$

Exercise 1.2.11. Verify that $(\mathbb{Z}, \leq)$ is a well-ordered set.

1.3 Division Algorithm

Recall that the *well-ordering principle of natural numbers* says that any non-empty subset S of $\mathbb{N}$ has a least element. This means, there exists $n \in S$ such that $n \leq m$, for all $m \in S$. This statement is equivalent to the *principle of mathematical induction*, which says that if $S \subseteq \mathbb{N}$ is such that $1 \in S$, and for each $n \in \mathbb{N}$, $n \in S \ \Rightarrow \ n + 1 \in S$, then $S = \mathbb{N}$.

Theorem 1.3.1 (Division algorithm)**.** *Given $a, d \in \mathbb{Z}$ with $d > 0$, there exists unique $q, r \in \mathbb{Z}$ with $0 \leq r < d$ such that $a = qd + r$.*

Proof. We first show uniqueness of q and r. Suppose that we have another pair of integers $q', r' \in \mathbb{Z}$ such that $0 \leq r' < d$ and $a = q'd + r'$. Without loss of generality we may assume that $r \leq r'$. Then $qd + r = a = q'd + r'$ implies $r' - r = (q - q')d$. Since $0 \leq r \leq r' < d$, we have $0 \leq (q - q')d = r' - r < d$. Therefore, $(q - q')d$ is a non-negative integer which is strictly less than d and is a multiple of d. This is possible only if $(q - q')d = 0$. Since $d \neq 0$, we must have $q = q'$, and hence $r = r'$. This proves uniqueness part.

To show existence, consider the set

$$S := \{a - dq : q \in \mathbb{N}\} \cap \mathbb{N}.$$

Since $d > 0$, choosing q sufficiently small we can ensure that $a - dq \in \mathbb{N}$, and hence $S \neq \emptyset$. Then by well-ordering principle of $(\mathbb{N}, \leq)$, S has a least element, say r_0. Then $0 \leq r_0 = q - dq_0$, for some $q_0 \in \mathbb{Z}$. We claim that $r_0 < d$. If not, then $r_0 \geq d$ and hence $0 \leq r_0 - d = a - d(q + 1)$ implies that $r_0 - d \in S$. Since $d > 0$, it contradicts the fact that r_0 is the least element of S. Therefore, we must have $r_0 < d$. This completes the proof. □

Definition 1.3.2. The *absolute value* of $n \in \mathbb{Z}$ is the integer $|n|$ defined by

$$|n| := \begin{cases} n, & \text{if} \quad n \geq 0, \\ -n, & \text{if} \quad n < 0. \end{cases}$$

Corollary 1.3.3. *Given $a, d \in \mathbb{Z}$ with $d \neq 0$, there exists unique $q, r \in \mathbb{Z}$ with $0 \leq r < |d|$ such that $a = dq + r$.*

Proof. If $d > 0$, this is precisely Theorem 1.3.1. If $d < 0$, then $d' := -d > 0$, and so by division algorithm (Theorem 1.3.1) we find unique integers $q, r \in \mathbb{Z}$ with $0 \leq r < d'$ such that $a = d'q + r$. Then the integers $q' := -q$ and r satisfies $0 \leq r < |d|$ with $a = q'd + r$. □

Definition 1.3.4. Given $n, d \in \mathbb{Z}$, with $d \neq 0$, we say that d *divides* n, written as $d \mid n$, if there is an element $q \in \mathbb{Z}$ such that $n = qd$. Given finitely many integers $a_1, \ldots, a_n \in \mathbb{Z}$, which are not all zero, we define their *greatest common divisor* to be a positive integer $d \in \mathbb{Z}^+$ such that

(i) d divides each of the numbers $a_1, \ldots, a_n$, and

(ii) if an integer r divides a_i, for all $i = 1, \ldots, n$, then r divides d.

Remark 1.3.5. Given a finite number of integers $a_1, \ldots, a_n \in \mathbb{Z}$, if d and d' are two greatest common divisors of $a_1, \ldots, a_n$, then $d \mid d'$ and $d' \mid d$ implies $d \in \{d', -d'\}$. Since both d and d' are positive integers, we must have $d = d'$. Therefore, the greatest common divisor of $a_1, \ldots, a_n$ is unique, and we denote it by $\gcd(a_1, \ldots, a_n)$. However, it is not yet clear if $\gcd(a_1, \ldots, a_n)$ exists in $\mathbb{N}$. This requires a proof.

Lemma 1.3.6. *Given $m, n \in \mathbb{Z}$, not all zero, the greatest common divisor $\gcd(m, n)$ exists in $\mathbb{N}$. Moreover, there exist $a, b \in \mathbb{Z}$ such that $\gcd(m, n) = am + bn$.*

Proof. Let $S := \{am + bn : a, b \in \mathbb{Z}\}$. Since at least one of m and n is non-zero, there is a non-zero element, say x, in S. Then $x = am + bn$, for some $a, b \in \mathbb{Z}$. If $x < 0$, then $-x = (-a)m + (-b)n \in S \cap \mathbb{N}$. Therefore, $S \cap \mathbb{N}$ is a non-empty subset of $\mathbb{N}$. Then by well-ordering principle of $\mathbb{N}$, the non-empty subset $S \cap N$ has a least element, say d. Then $d = a_0m + b_0n$, for some $a_0, b_0 \in \mathbb{Z}$. We claim that $d = \gcd(m, n)$.

If $r \mid m$ and $r \mid n$, then $r \mid (a_0m + b_0n)$ and so $r \mid d$. Now we need to show that $d \mid m$ and $d \mid n$. Let $x \in S$ be arbitrary. Then $x = am + bn \in S$, for some $a, b \in \mathbb{Z}$. By division algorithm we can find $q, r \in \mathbb{Z}$ with $0 \leq r < d$ such that $x = qd + r$. Then $am + bn = x = qd + r = q(a_0m + b_0n) + r$ implies $r = (a - qa_0)m + (b - qb_0)n \in S$. Since $0 \leq r < d$ and d is the smallest positive integer in $S \cap \mathbb{N}$, we must have $r = 0$. Therefore, $x = qd$ and hence $d \mid x$, for all $x \in S$. In particular, choosing $(a, b) \in \{(1, 0), (0, 1)\}$, we see that $d \mid m$ and $d \mid n$. This completes the proof. □

Definition 1.3.7. Given $m, n \in \mathbb{Z}$, we say that m and n are *relatively prime* (or, *coprime*) if $\gcd(m, n) = 1$.

Corollary 1.3.8. *Two integers m and n are coprime if and only if there exists $a, b \in \mathbb{Z}$ such that $am + bn = 1$.*

Proof. If $\gcd(m, n) = 1$, then by above Lemma 1.3.6, there exists $a, b \in \mathbb{Z}$ such that $am + bn = 1$. Conversely, suppose that $am + bn = 1$, for some $a, b \in \mathbb{Z}$. If $d = \gcd(m, n)$, then $d \mid m$ and $d \mid n$ implies $d \mid 1$. Then $d \in \{1, -1\}$. Since $d > 0$, we have $d = 1$. □

Exercise 1.3.9. Given a finite number of integers $a_1, \ldots, a_n$, not all zero, show that $\gcd(a_1, \ldots, a_n)$ exists in $\mathbb{N}$.

Definition 1.3.10. An integer $p \in \mathbb{Z}$ is said to be a *prime number* if $p > 1$ and its only divisors in $\mathbb{Z}$ are $\pm 1, \pm p$.

Exercise 1.3.11 (Principle of mathematical induction)**.** Fix $n_0 \in \mathbb{N}$. Prove that the following are equivalent.

(i) *Regular version:* Let $S \subseteq \mathbb{N}$ be such that

  (a) $n_0 \in S$, and

  (b) for any $n \in \mathbb{N}$ with $n \geq n_0$, if $n \in S$ then $n + 1 \in S$.

  Then $S = \{n \in \mathbb{N} : n \geq n_0\}$.

(ii) *Strong version:* Let $T \subseteq \mathbb{N}$ be such that

  (a′) $n_0 \in T$, and

(b′) for any $n \in \mathbb{N}$ with $n \geq n_0$, if $\{k \in \mathbb{N} : n_0 \leq k \leq n\} \subseteq T$ then $n + 1 \in T$.

Then $T = \{n \in \mathbb{N} : n \geq n_0\}$.

Assuming well-ordering principle of $(\mathbb{N}, \leq)$ show that the above two versions of induction holds true.

Theorem 1.3.12 (Fundamental theorem of Arithmetic)**.** *Given a positive integer $n > 1$, there exists a unique factorization of n as a product of positive integer powers of prime numbers. More precisely, there exist finite number of unique prime numbers $p_1, \ldots, p_k \in \mathbb{N}$ with $p_1 > \cdots > p_k$ and positive integers $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$ such that $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.*

Chapter 2

Group Theory

2.1 Group

A *binary operation* on a set A is a map $* : A \times A \to A$; given $(a, b) \in A \times A$ its image under the map $*$ is denoted by $a * b$. We consider some examples of non-empty set together with a natural binary operation and study list down their common properties.

Example 2.1.1. The set of all integers

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \ldots\}$$

admits a binary operation, namely addition of integers:

$$+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}, \quad (a, b) \longmapsto a + b.$$

This binary operation has the following interesting properties:

(i) $a + (b + c) = (a + b) + c, \ \forall\, a, b, c \in \mathbb{Z}$,

(ii) there is an element $0 \in \mathbb{Z}$ such that $a + 0 = 0 + a = a, \ \forall\, a \in \mathbb{Z}$,

(iii) for each $a \in \mathbb{Z}$, there exists an element $b \in \mathbb{Z}$ (depending on a) such that $a + b = b + a = 0$; the element b is denoted by $-a$.

Example 2.1.2. A *symmetry* on a non-empty set X is a bijective map from X onto itself. The set of all symmetries of X is denoted by $S(X)$. Note that $S(X)$ admits a binary operation given by composition of maps:

$$\circ : S(X) \times S(X) \longrightarrow S(X), \ \ (f, g) \longmapsto g \circ f.$$

Note that

(i) given any $f, g, h \in S(X)$, we have $(f \circ g) \circ h = f \circ (g \circ h)$.

(ii) there is a distinguished element, the identity map $\mathrm{Id}_X \in S(X)$ such that $f \circ \mathrm{Id}_X = f = \mathrm{Id}_X \circ f$, for all $f \in S(X)$.

(iii) given any $f \in S(X)$, there is a element $g := f^{-1} \in S(X)$ such that $f \circ g = \mathrm{Id}_X = g \circ f$.

Example 2.1.3. Fix a natural number $n \geq 1$, and consider the set $\mathrm{GL}_n(\mathbb{R})$ of all invertible $n \times n$ matrices with entries from $\mathbb{R}$. Note that $\mathrm{GL}_n(\mathbb{R})$ admits a natural binary operation given by matrix multiplication:

$$\cdot : \mathrm{GL}_n(\mathbb{R}) \times \mathrm{GL}_n(\mathbb{R}) \to \mathrm{GL}_n(\mathbb{R}), \ \ (A, B) \longmapsto AB.$$

Note that

(i) given any $A, B, C \in \mathrm{GL}_n(\mathbb{R})$, we have $(AB)C = A(BC)$.

(ii) there is a distinguished element, the identity matrix $I_n \in \mathrm{GL}_n(\mathbb{R})$ such that $AI_n = I_nA = A$, for all $A \in \mathrm{GL}_n(\mathbb{R})$.

(iii) given any $A \in \mathrm{GL}_n(\mathbb{R})$, there is a element $B := A^{-1} \in \mathrm{GL}_n(\mathbb{R})$ such that $AB = BA = I_n$.

A non-empty set together with a binary operation satisfying the three properties listed in the above examples is a mathematical model for many important mathematical and physical systems; such a mathematical model is called a group. Here is a formal definition.

Definition 2.1.4. A *group* is a pair $(G, *)$ consisting of a non-empty set G together with a binary operation

$$* : G \times G \longrightarrow G, \quad (a, b) \longmapsto a * b,$$

satisfying the following conditions:

(G1) *Associativity:* $a * (b * c) = (a * b) * c$, for all $a, b, c \in G$.

(G2) *Existence of neutral element:* $\exists$ an element $e \in G$ such that $a * e = e * a = a, \ \forall\, a \in G$.

(G3) *Existence of inverse:* for each $a \in G$, there exists an element $b \in G$, depending on a, such that $a * b = e = b * a$.

A *semigroup* is a pair $(G, *)$ consisting of a non-empty set G together with an associative binary operation $* : G \times G \to G$ (i.e., the condition (G1) holds). A *monoid* is a semigroup $(G, *)$ satisfying the condition (G2) as above. For example, $(\mathbb{N}, +)$ is a semigroup but not a monoid, and $(\mathbb{Z}_{\geq 0}, +)$ is a monoid but not a group. However, we shall not deal with these two notations in this text.

Example 2.1.5. (i) *Trivial group:* A singleton set $\{e\}$ with the binary operation $e * e := e$ is a group; such a group is called a *trivial group*.

(ii) The set $G := \{e, a\}$, with the binary operation $*$ given by $a * e = e * a = a$ and $a * a = e$, is a group with two elements.

(iii) Verify that $G := \{e, a, b\}$ together with the binary operation $*$ given by the following multiplication table, is a group (with three elements).

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

TABLE 2.1: A group with 3 elements

Remark 2.1.6. For a group consisting of small number of elements, it is convenient to write down the associated binary operation explicitly using a table as above, known as the *Cayley table*.

(iv) The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ form groups with respect to usual addition.

(v) The set $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ forms a group with respect to usual multiplication.

Exercise 2.1.7. Let $(G, *)$ be a group.

(i) *Uniqueness of neutral element:* Show that the neutral element (also known as the *identity element*) $e \in G$ is unique.

(ii) *Uniqueness of inverse:* Show that, for each $a \in G$, there is a unique element $b \in G$ such that $a * b = b * a = e$. The element b is called *the inverse* of a, and denoted by the symbol a^{-1}.

(iii) *Cancellation Law:* If $a * c = b * c$, for some $a, b, c \in G$, show that $a = b$.

(iv) Let $a, b \in G$. Show that $\exists$ unique $x, y \in G$ such that $a * x = b$ and $y * a = b$.

Let $(G, *)$ be a group. We say that G is *finite* or *infinite* according as its underlying set G is finite or infinite; the cardinality of G is called the *order* of the group $(G, *)$, and we denote it by the symbol $|G|$. For notational simplicity, we write ab to mean $a * b$, for all $a, b \in G$; and for any integer $n \geq 1$, we denote by a^n the n-fold product of a with itself, i.e.,

$$a^n := \underbrace{a * \cdots * a}_{n\text{-fold product of } a}.$$

For a negative integer n, we define $a^n := (a^{-1})^{-n}$. When there is no confusion likely to arise, we simply denote a group $(G, *)$ by G without specifying the binary operation.

Exercise 2.1.8. Let G be a group.

(i) Show that $(a^{-1})^{-1} = a$, for all $a \in G$.

(ii) Show that $(ab)^{-1} = b^{-1}a^{-1}$, for all $a, b \in G$.

(iii) Show that $a^m a^n = a^{m+n}$, for all $m, n \in \mathbb{Z}$ and $a \in G$.

(iv) Show that $(a^m)^n = a^{mn}$, for all $m, n \in \mathbb{Z}$ and $a \in G$.

(v) Let $a, b \in G$ be such that $ab = ba$. Show that $(ab)^n = a^n b^n$, for all $n \in \mathbb{Z}$.

Example 2.1.9. (i) The set $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$ of non-zero complex numbers forms a group with respect to multiplication of complex numbers.

(ii) *Circle group:* The set

$$S^1 := \{z \in \mathbb{C} \,:\, |z| = 1\}$$

forms a group with respect to multiplication of complex numbers.

(iii) *Klein four-group:* Consider the set $K_4 = \{e, a, b, c\}$ together with the binary operation

$$* : K_4 \times K_4 \longrightarrow K_4$$

defined by the Cayley table 2.2 below. Verify that K_4 is a group.

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

TABLE 2.2: Klein four group

Exercise 2.1.10. Define a binary operation on $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ by

$$(x_1, y_1) + (x_2, y_2) := (x_1 + x_2, y_1 + y_2), \;\; \forall\, (x_1, y_1), (x_2, y_2) \in \mathbb{R}^2.$$

Verify that $(\mathbb{R}^2, +)$ is a commutative group. Similarly, for each $n \in \mathbb{N}$, show that the componentwise addition of real numbers:

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) := (a_1 + b_1, \ldots, a_n + b_n), \; \forall\, a_j, b_j \in \mathbb{R}, \tag{2.1.11}$$

defines a binary operation $+$ on $\mathbb{R}^n$ which makes the pair $(\mathbb{R}^n, +)$ a commutative group.

Definition 2.1.12. A map $f : A \to B$ is said to be

(i) *injective* if given any $a_1, a_2 \in A$ with $f(a_1) = f(a_2)$, we have $a_1 = a_2$,

(ii) *surjective* if given any $b \in B$, there is an element $a \in A$ such that $f(a) = b$,

(iii) *bijective* if f is both injective and surjective.

Exercise 2.1.13. Let A, B and C be three sets. Given maps $f : A \to B$ and $g : B \to C$, we define the *composition of g with f*, also called "*g composed f*", to be the map $g \circ f : A \to C$ defined by

$$(g \circ f)(a) = g(f(a)), \ \ \forall\, a \in A.$$

Prove the following.

(i) If both f and g are injective, so is $g \circ f : A \to C$.

(ii) If both f and g are surjective, so is $g \circ f : A \to C$.

(iii) If $g \circ f$ is injective, show that f is injective.

(iv) Give an example to show that $g \circ f$ could be injective without g being injective.

(v) If $g \circ f$ is surjective, show that g is surjective.

(vi) Give an example to show that $g \circ f$ could be surjective without f being surjective.

(vii) Given any set A, there is a map $\mathrm{Id}_A : A \to A$ defined by $\mathrm{Id}_A(a) = a, \forall\, a \in A$, known as the *identity map* of A. Verify that Id_A is bijective.

(viii) If $f : A \to B$ is bijective, show that there is a bijective map $\widetilde{f} : B \to A$ such that $\widetilde{f} \circ f = \mathrm{Id}_A$ and $f \circ \widetilde{f} = \mathrm{Id}_B$. The bijective map $\widetilde{f} : B \to A$, defined above, is called the *inverse of f*, and is usually denoted by f^{-1}.

Definition 2.1.14. A *permutation* on a set A is a bijective map from A onto itself.

For a non-empty set A, we denote by S_A the set of all permutations on A. Let A be a non-empty set. Define a binary operation on S_A by

$$\circ \ : \ S_A \times S_A \longrightarrow S_A, \ \ (f, g) \longmapsto g \circ f.$$

Verify that $(S_A, \circ)$ is a group. (*Hint:* Use Exercise 2.1.13).

Example 2.1.15 (Symmetric group S_3)**.** Consider an equilateral triangle $\triangle$ in a plane with its vertices labelled as $1, 2$ and 3. Consider the symmetries of $\triangle$ obtained by its rotations by angles $2n\pi/3$, for $n \in \mathbb{Z}$, around its centre, and reflections along a straight line passing through its top vertex and centre. Note that, we have only six possible symmetries of $\triangle$ as follow:

$$\sigma_0 = \begin{pmatrix} 1 & \mapsto & 1 \\ 2 & \mapsto & 2 \\ 3 & \mapsto & 3 \end{pmatrix}, \ \sigma_1 = \begin{pmatrix} 1 & \mapsto & 2 \\ 2 & \mapsto & 3 \\ 3 & \mapsto & 1 \end{pmatrix}, \ \sigma_2 = \begin{pmatrix} 1 & \mapsto & 3 \\ 2 & \mapsto & 1 \\ 3 & \mapsto & 2 \end{pmatrix},$$
$$\sigma_3 = \begin{pmatrix} 1 & \mapsto & 1 \\ 2 & \mapsto & 3 \\ 3 & \mapsto & 2 \end{pmatrix}, \ \sigma_4 = \begin{pmatrix} 1 & \mapsto & 3 \\ 2 & \mapsto & 2 \\ 3 & \mapsto & 1 \end{pmatrix}, \ \sigma_5 = \begin{pmatrix} 1 & \mapsto & 2 \\ 2 & \mapsto & 1 \\ 3 & \mapsto & 3 \end{pmatrix}.$$

Let $S_3 := \{\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$. Note that, each of symmetries are bijective maps from the set $J_3 := \{1, 2, 3\}$ onto itself, and any bijective map from J_3 onto itself is one of the symmetries in S_3. Since composition of bijective maps is bijective (see Exercise 2.1.13), we get a binary operation

$$S_3 \times S_3 \longrightarrow S_3, \ \ (\sigma_i, \sigma_j) \longmapsto \sigma_i \circ \sigma_j.$$

Exercise 2.1.16. Write down the Cayley table for this binary operation on S_3 defined by composition of maps, and show that S_3 together with this binary operation is a group. Find $\sigma_1, \sigma_2 \in S_3$ such that $\sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1$.

Definition 2.1.17. The *order* of a group G is the cardinality of its underlying set G. We denote this by $|G|$. In particular, if G is a finite set, then $|G|$ is the number of elements of the set G.

Example 2.1.18. Let S_4 be the set of all bijective maps from $J_4 := \{1, 2, 3, 4\}$ onto itself. Given any two elements $\sigma, \tau \in S_4$, note that their composition $\sigma \circ \tau \in S_4$. Thus we have a binary operation on S_4 given by sending $(\sigma, \tau) \in S_4 \times S_4$ to $\sigma \circ \tau \in S_4$. Show that the set S_4 together with this binary operation (composition of bijective maps) is a non-commutative group of order $4! = 24$.

Definition 2.1.19. Let $A \subseteq \mathbb{R}$. A map $f : A \to \mathbb{R}$ is said to be *continuous* at $a \in A$ if given any real number $\epsilon > 0$, there is a real number $\delta > 0$ (depending on both ϵ and a) such that for each $x \in A$ satisfying $|a - x| < \delta$, we have $|f(a) - f(x)| < \epsilon$. If f is continuous at each point of A, we say that f is *continuous on* A.

Exercise 2.1.20. Let $A \subseteq \mathbb{R}$, and let $C(A) := \{f : A \to \mathbb{R} \,\big|\, f \text{ is continuous}\}$. Verify that $C(A)$ is a group with respect to the binary operation defined for all $f, g \in C(A)$ by the formula

$$(f + g)(x) := f(x) + g(x), \ \forall\, x \in A.$$

Solution. Let $f_1, f_2 \in C(A)$. Let $a \in A$ be arbitrary but fixed after choice. Since both f_1 and f_2 are continuous at a, given a real number $\epsilon > 0$, there exist real numbers $\delta_1, \delta_2 > 0$ such that for each $x \in A$ satisfying $|a - x| < \delta_j$ we have $|f_j(a) - f_j(x)| < \epsilon/2$, for all $j = 1, 2$. Let $\delta := \min\{\delta_1, \delta_2\}$. Then $\delta > 0$, and for any $x \in A$ satisfying $|a - x| < \delta$, we have $|f_j(a) - f_j(x)| < \epsilon/2$, for all $j = 1, 2$. Then we have,

$$\begin{aligned}
|(f_1 + f_2)(a) - (f_1 + f_2)(x)| &= |f_1(a) + f_2(a) - f_1(x) - f_2(x)| \\
&= |\big(f_1(a) - f_1(x)\big) + \big(f_2(a) - f_2(x)\big)| \\
&\leq |f_1(a) - f_1(x)| + |f_2(a) - f_2(x)| \\
&< \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.
\end{aligned}$$

Therefore, $f_1 + f_2$ is continuous at $a \in A$. Since $a \in A$ is arbitrary, $f_1 + f_2$ is continuous at every points of A, and hence $f_1 + f_2 \in C(A)$. Since for given $f_1, f_2, f_3 \in C(A)$ and any $x \in A$, we have

$$\begin{aligned}
\big((f_1 + f_2) + f_3\big)(x) &= \big(f_1 + f_2\big)(x) + f_3(x) \\
&= \big(f_1(x) + f_2(x)\big) + f_3(x) \\
&= f_1(x) + \big(f_2(x) + f_3(x)\big) \\
&= f_1(x) + \big(f_2 + f_3\big)(x) \\
&= \big(f_1 + (f_2 + f_3)\big)(x),
\end{aligned}$$

we have $(f_1 + f_2) + f_3 = f_1 + (f_2 + f_3)$. Note that, the constant function

$$0 : A \to \mathbb{R}$$

defined by sending all points of A to $0 \in \mathbb{R}$, given by $0(a) = 0, \ \forall\, a \in A$, is continuous (*Hint:* given $\epsilon > 0$, take any $\delta > 0$), and satisfies $f + 0 = f = 0 + f$, for all $f \in A$. Given $f \in C(A)$, note that the function $-f$ defined by $(-f)(a) = -f(a)$, for all $a \in A$, is continuous on A (*Hint:* given $\epsilon > 0$, take the same $\delta > 0$ which works for f), and satisfies $f + (-f) = (-f) + f = 0$. Therefore, $\big(C(A), +\big)$ satisfies all axioms of a group, and hence is a group. □

Example 2.1.21 (Matrix groups)**.** (i) Fix two integers $m, n \geq 1$, and let $\mathrm{M}_{m\times n}(\mathbb{R})$ be the set of all $m \times n$ matrices with entries from $\mathbb{R}$. Given $A, B \in \mathrm{M}_{m\times n}(\mathbb{R})$, we define their *addition*

to be the matrix $A + B \in \mathrm{M}_{m\times n}(\mathbb{R})$ whose (i,j)-th entry is given by $a_{ij} + b_{ij}$, where a_{ij} and b_{ij} are the (i,j)-th entries of A and B, respectively. Then we have a binary operation

$$+ : \mathrm{M}_{m\times n}(\mathbb{R}) \times \mathrm{M}_{m\times n}(\mathbb{R}) \longrightarrow \mathrm{M}_{m\times n}(\mathbb{R}), \quad (A,B) \longmapsto A + B.$$

Clearly, the set $\mathrm{M}_{m\times n}(\mathbb{R})$ is non-empty, and the pair $(\mathrm{M}_{m\times n}(\mathbb{R}), +)$ satisfies the properties (G1)–(G3) in Definition 2.1.4.

(ii) *Matrix multiplication:* Fix positive integers m, n, p, and let $A \in \mathrm{M}_{m\times n}(\mathbb{R})$ and $B \in \mathrm{M}_{n\times p}(\mathbb{R})$. Define the *product of A and B* to be the $m \times p$ matrix $AB \in \mathrm{M}_{m\times p}(\mathbb{R})$, whose (i,j)-th entry is

$$c_{ij} = \sum_{k=1} a_{ik} b_{kj}, \tag{2.1.22}$$

where a_{ik} is the (i,k)-th entry of A, and b_{kj} is the (k,j)-th entry of B.

Let $A \in \mathrm{M}_{n\times n}(\mathbb{R})$. A matrix $B \in \mathrm{M}_{n\times n}(\mathbb{R})$ is said to be the *left inverse* (resp., *right inverse*) of A if $BA = I_n$ (resp., $AB = I_n$), where $I_n \in \mathrm{M}_{n\times n}(\mathbb{R})$ whose (i,j)-th entry is

$$\delta_{ij} = \begin{cases} 1, & \text{if} \quad i = j, \\ 0, & \text{if} \quad i \neq j. \end{cases}$$

Exercise 2.1.23. Show that the left inverse and the right inverse of $A \in \mathrm{M}_{n\times n}(\mathbb{R})$, when they exists, are the same. In other words, if $AB = I_n$ and $CA = I_n$, for some $B, C \in \mathrm{M}_{n\times n}(\mathbb{R})$, show that $B = C$.

A matrix $A \in \mathrm{M}_{n\times n}(\mathbb{R})$ is said to be *invertible* if there is a matrix $B \in \mathrm{M}_{n\times n}(\mathbb{R})$ such that $AB = BA = I_n$.

General linear group: Let

$$\mathrm{GL}_n(\mathbb{R}) = \{A \in \mathrm{M}_{n\times n}(\mathbb{R}) : A \text{ is invertible}\}$$

be the set of all invertible $n \times n$ matrices with real entries.

(a) Show that $\mathrm{GL}_n(\mathbb{R})$ is a group with respect to matrix multiplication.

(b) Give examples of $A, B \in \mathrm{GL}_n(\mathbb{R})$ such that $A + B \notin \mathrm{GL}_n(\mathbb{R})$.

(c) Give an example of $A \in \mathrm{M}_{n\times n}(\mathbb{R})$ such that $AB \neq I_n, \forall\, B \in \mathrm{M}_{n\times n}(\mathbb{R})$.

(d) Assuming $n \geq 2$ give examples of $A, B \in \mathrm{GL}_n(\mathbb{R})$ such that $AB \neq BA$.

The group $\mathrm{GL}_n(\mathbb{R})$ is called the *general linear group* (of degree n).

As we see in Example 2.1.21 that the relation $ab = ba$ need not hold for all $a, b \in G$, in general. We shall see later that the symmetric group S_3 in Example 2.1.9 (2.1.15) is the smallest such group; in this case, we have $\sigma_3 \circ \sigma_1 = \sigma_4$ while $\sigma_1 \circ \sigma_3 = \sigma_5$.

Definition 2.1.24. A group G is said to be *commutative* (or, *abelian*) if $ab = ba$, for all $a, b \in G$. A group which is not commutative (or, abelian) is called a *non-commutative* (or, *non-abelian*) group.

Exercise 2.1.25. (i) Verify that $\{e\}$, $\mathbb{Z}$, $\mathbb{C}^*$, S^1, K_4 are abelian groups.

(ii) Show that S_3 and $\mathrm{GL}_2(\mathbb{R})$ are non-abelian groups.

Exercise 2.1.26. Show that $\mathrm{GL}_n(\mathbb{R})$ is not abelian, for all $n \geq 2$.

Definition 2.1.27. A *relation* on a non-empty set A is a non-empty subset $\rho \subseteq A \times A$. If $(a,b) \in \rho$, sometimes we may express it as $a\,\rho\,b$, and call a *is ρ-related to b* in A. A relation ρ on A is said to be

(i) *reflexive* if $(a, a) \in \rho, \ \forall\, a \in A$;

(ii) *symmetric* if $(a, b) \in \rho$ implies $(b, a) \in \rho$;

(iii) *anti-symmetric* if $(a, b) \in \rho$ and $(b, a) \in \rho$ implies $a = b$;

(iv) *transitive* if $(a, b) \in \rho$ and $(b, c) \in \rho$ implies $(a, c) \in \rho$;

(v) *equivalence* if ρ is reflexive, symmetric and transitive; and

(vi) *partial order* if ρ is reflexive, anti-symmetric and transitive.

Let A be a non-empty set, and let ρ be an equivalence relation on A. The *ρ-equivalence class* of an element $a \in A$ is the subset

$$[a]_\rho := \{b \in A : (b, a) \in \rho\} \subseteq A.$$

Proposition 2.1.28. *With the above notations, given any $a, b \in A$, $[a]_\rho = [b]_\rho$ if and only if $(a, b) \in \rho$.*

Proof. Suppose that $(a, b) \in \rho$. Then for any $c \in [a]_\rho$, we have $(c, a) \in \rho$. Since ρ is transitive, from $(c, a), (a, b) \in \rho$ we have $(c, b) \in \rho$, and so $c \in [b]_\rho$. Therefore, $[a]_\rho \subseteq [b]_\rho$. Since ρ is symmetric, $(a, b) \in \rho$ implies $(b, a) \in \rho$. Then following above arguments, we conclude that $[b] \subseteq [a]$. Therefore, $[a]_\rho = [b]_\rho$.

Conversely, suppose that $[a]_\rho = [b]_\rho$. Since ρ is reflexive, $a \in [a]_\rho$. Then $[a]_\rho = [b]_\rho$ implies that $a \in [b]_\rho$, and so $(a, b) \in \rho$. This completes the proof. □

Proposition 2.1.29. *With the above notations, given $a, b \in A$, either $[a]_\rho \cap [b]_\rho = \emptyset$ or $[a]_\rho = [b]_\rho$.*

Proof. It is enough to show that if $[a]_\rho \cap [b]_\rho \neq \emptyset$, then $[a]_\rho = [b]_\rho$. Let $c \in [a]_\rho \cap [b]_\rho$. Then $(c, a), (c, b) \in \rho$. Since ρ is symmetric, $(c, a) \in \rho$ implies $(a, c) \in \rho$. Then $(a, c) \in \rho$ and $(c, b) \in \rho$ together implies $(a, b) \in \rho$, since ρ is transitive. Then by Proposition 2.1.28 we have $[a]_\rho = [b]_\rho$. □

Definition 2.1.30. Let A be a non-empty set. A *partition* on A is a non-empty collection $\mathcal{P} := \{A_\alpha : \alpha \in \Lambda\}$, where

(i) $A_\alpha \subseteq A$, for all $\alpha \in \Lambda$,

(ii) $A_\alpha \cap A_\beta = \emptyset$, for $\alpha \neq \beta$ in Λ, and

(iii) $A = \bigcup_{\alpha \in \Lambda} A_\alpha$.

Proposition 2.1.31. *To give an equivalence relation on a non-empty set is equivalent to give a partition on it.*

Proof. Suppose that we have given an equivalence relation ρ on A. Since ρ is reflexive, $a \in [a]_\rho$, for all $a \in A$, and hence $A = \bigcup_{a \in A} [a]_\rho$. Since ρ-equivalence classes of elements of A are either disjoint or equal (see Proposition 2.1.29), the collection $\mathcal{P}$ consisting of all distinct ρ-equivalence classes of elements of A is a partition of A.

Conversely, suppose that $\mathcal{P} = \{A_\alpha : \alpha \in \Lambda\}$ be a partition of A. Define

$$\rho = \{(a, b) \in A \times A : a, b \in A_\alpha, \text{ for some } \alpha \in \Lambda\}.$$

Note that $(a, a) \in \rho$, for all $a \in A$. If $(a, b) \in \rho$, then both a and b are in the same A_α, for some $\alpha \in \Lambda$, and so $(b, a) \in \rho$. So ρ is symmetric. If $(a, b), (b, c) \in \rho$, then $a, b \in A_\alpha$ and $b, c \in A_\beta$, for some $\alpha, \beta \in \Lambda$. Since $b \in A_\alpha \cap A_\beta$, so we must have $A_\alpha = A_\beta$. Therefore, $(a, c) \in \rho$. Thus ρ is transitive. Therefore, ρ is an equivalence relation on A. One should note that the elements of $\mathcal{P}$ are precisely the ρ-equivalence classes in A (verify!). □

Example 2.1.32 (The groups $\mathbb{Z}_n$ and U_n)**.** Fix an integer $n \geq 2$. Define a relation $\equiv_n$ on $\mathbb{Z}$ by setting

$$a \equiv_n b, \quad \text{if } a - b = nk, \text{ for some } k \in \mathbb{Z}.$$

If $a \equiv_n b$ sometimes we also express it as $a \equiv b \pmod{n}$, and say that *a is congruent to b modulo n*. Verify that $\equiv_n$ is an equivalence relation on $\mathbb{Z}$. Given any $a \in \mathbb{Z}$, let

$$[a] := \{b \in \mathbb{Z} : b \equiv_n a\} \subseteq \mathbb{Z}$$

be the $\equiv_n$-equivalence class of a in $\mathbb{Z}$. Let

$$\mathbb{Z}_n := \{[a] : a \in \mathbb{Z}\}$$

be the set of all $\equiv_n$-equivalence classes of elements of $\mathbb{Z}$. Let $a, b \in \mathbb{Z}$. If $c \in [a] \cap [b]$, then $c = a + nk_1$ and $c = b + nk_2$, for some $k_1, k_2 \in \mathbb{Z}$. Then $a - b = n(k_1 - k_2)$, and hence $a \equiv_n b$. Then $[a] = [b]$ in $\mathbb{Z}_n$. Therefore, the $\equiv_n$-equivalence classes are either disjoint or identical (c.f. Proposition 2.1.29). Use division algorithm (Theorem 1.3.1) to show that $\equiv_n$-equivalence classes $[0], [1], \ldots, [n-1]$ are all distinct, and

$$\mathbb{Z}_n = \{[k] : 0 \leq k \leq n-1\}.$$

In particular, $\mathbb{Z}_n$ is a finite set containing n elements.

We now define two binary operations on $\mathbb{Z}_n$. Suppose that $[a] = [a']$ and $[b] = [b']$ in $\mathbb{Z}_n$, for some $a, a', b, b' \in \mathbb{Z}$. Then we have

$$\begin{aligned} a - a' &= nk_1, \\ \text{and } \ b - b' &= nk_2, \end{aligned}$$

for some $k_1, k_2 \in \mathbb{Z}$. Therefore,

$$(a + b) - (a' + b') = n(k_1 - k_2),$$

and hence $[a + b] = [a' + b']$ in $\mathbb{Z}_n$. Therefore, we have a well-defined binary operation on $\mathbb{Z}_n$ (called *addition of integers modulo n*) given by

$$[a] + [b] := [a + b], \ \ \forall\, [a], [b] \in \mathbb{Z}_n.$$

Now it is easy to see that,

(i) $([a] + [b]) + [c] = [a] + ([b] + [c])$, for all $[a], [b], [c] \in \mathbb{Z}_n$.

(ii) $[a] + [0] = [a] = [0] + [a]$, for all $[a] \in \mathbb{Z}_n$.

(iii) $[a] + [-a] = [0]$, for all $[a] \in \mathbb{Z}$.

Therefore, $(\mathbb{Z}_n, +)$ is a group. Note that, for all $[a], [b] \in \mathbb{Z}_n$ we have

$$\begin{aligned} [a] + [b] = [a + b] &= [b + a], \ \text{ since addition in } \mathbb{Z} \text{ is commutative,} \\ &= [b] + [a]. \end{aligned}$$

Therefore, $(\mathbb{Z}_n, +)$ is an abelian group.

Now we define *multiplication operation on $\mathbb{Z}_n$*. Suppose that $[a] = [a']$ and $[b] = [b']$. Then $a - a' = nk_1$ and $b - b' = nk_2$, for some $k_1, k_2 \in \mathbb{Z}$. Then

$$\begin{aligned} ab - a'b' &= (a - a')b + a'(b - b') \\ &= nk_1 b + a' nk_2 \\ &= n(k_1 b + a' k_2), \end{aligned}$$

implies that $[ab] = [a'b']$. Thus we have a well-defined binary operations on $\mathbb{Z}_n$ (called the *multiplication of integers modulo* n) defined by

$$[a] \cdot [b] := [ab], \ \ \forall\, [a], [b] \in \mathbb{Z}_n.$$

Clearly the multiplication modulo n operation on $\mathbb{Z}_n$ is both associative and commutative. Note that,

$$[1] \cdot [a] = [a] = [a] \cdot [1], \ \ \forall\, [a] \in \mathbb{Z}_n.$$

Therefore, $[1] \in \mathbb{Z}_n$ is the multiplicative identity in $\mathbb{Z}_n$. Moreover, the multiplication distributes over addition from left and right on $\mathbb{Z}_n$. Indeed, we have

$$\begin{aligned} [a] \cdot ([b] + [c]) &= [a] \cdot [b] + [a] \cdot [c], \\ \text{and} \quad ([a] + [b]) \cdot [c] &= [a] \cdot [c] + [b] \cdot [c]\,. \end{aligned}$$

Such a triple $(\mathbb{Z}_n, +, \cdot)$ is called a *ring*. Since $n \geq 2$ by assumption, n does not divide 1 in $\mathbb{Z}_n$. So $[0] \neq [1]$ in $\mathbb{Z}_n$ by Proposition 2.1.28. Since for any $[a] \in \mathbb{Z}_n$, we have $[0] \cdot [a] = [0 \cdot a] = [0] \neq [1]$, we see that $[0] \in \mathbb{Z}_n$ has no multiplicative inverse in $\mathbb{Z}_n$. Therefore, $(\mathbb{Z}_n, \cdot)$ is just a commutative monoid, but not a group.

We now find out elements of $\mathbb{Z}_n$ that have multiplicative inverse in $\mathbb{Z}_n$, and use them to construct a subset of $\mathbb{Z}_n$ which forms a group with respect to the multiplication modulo n operation. Recall that given $n, k \in \mathbb{Z}$, we have $\gcd(n, k) = 1$ if and only if there exists $a, b \in \mathbb{Z}$ such that $an + bk = 1$ (see Corollary 1.3.8). Use this to verify that if $[k] = [k']$ in $\mathbb{Z}_n$, then $\gcd(n, k) = 1$ if and only if $\gcd(n, k') = 1$. Thus we get a well-defined subset

$$U_n := \{[k] \in \mathbb{Z}_n \,:\, \gcd(k, n) = 1\} \subset \mathbb{Z}_n.$$

Note that, $[0] \notin U_n$. If $[k_1], [k_2] \in U_n$, then $\gcd(k_1, n) = 1 = \gcd(k_2, n)$. Then there exists $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ such that

$$\begin{aligned} a_1 k_1 + b_1 n &= 1 \\ \text{and} \quad a_2 k_2 + b_2 n &= 1. \end{aligned}$$

Multiplying these two equations, we have

$$(a_1 a_2)(k_1 k_2) + (a_1 k_1 b_2 + a_2 k_2 b_1 + b_1 b_2) n = 1.$$

Then we have $\gcd(k_1 k_2, n) = 1$. Therefore,

$$[k_1] \cdot [k_2] = [k_1 k_2] \in U_n, \ \forall\, [k_1], [k_2] \in U_n.$$

Verify that $(U_n, \cdot)$ is an abelian group. If $p > 1$ is a prime number (see Definition 1.3.10), show that $U_p = \mathbb{Z}_p \setminus \{[0]\}$, as sets.

Exercise 2.1.33. Let X be a non-empty set. Let $\mathcal{P}(X)$ be the set of all subsets of X; called the *power set of* X. Given any two elements $A, B \in \mathcal{P}(X)$, define

$$A \triangle B := (A \setminus B) \cup (B \setminus A).$$

The set $A \triangle B$ is known as the *symmetric difference* of A and B. Show that $\big(\mathcal{P}(X), \triangle\big)$ is a commutative group. (*Hint:* The empty subset $\emptyset \subset X$ acts as the neutral element in $\mathcal{P}(X)$, and every element of $\mathcal{P}(X)$ is inverse of itself).

2.2 Subgroup

Definition 2.2.1 (Subgroup)**.** Let G be a group. A *subgroup* of G is a subset $H \subseteq G$ such that H is a group with respect to the binary operation induced from G. A subgroup H of G is said to be *proper* if $H \neq G$. A subgroup whose underlying set is singleton is called a *trivial* subgroup.

For example, $\mathbb{Z}$ is a subgroup of $\mathbb{Q}$; S^1 is a subgroup of $\mathbb{C}^*$ etc.

Exercise 2.2.2. For each integer n, let $n\mathbb{Z} := \{nk : k \in \mathbb{Z}\}$.

(i) Show that $n\mathbb{Z}$ is a proper subgroup of $\mathbb{Z}$, for all $n \in \mathbb{Z} \setminus \{1, -1\}$.

(ii) Show that any subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$, for some $n \in \mathbb{Z}$.

Exercise 2.2.3 (Group of n^{th} roots of unity)**.** Fix an integer $n \geq 1$, and let

$$\mu_n := \{\zeta \in \mathbb{C} \mid \zeta^n = 1\}.$$

Show that μ_n is a subgroup of the circle group S^1.

Exercise 2.2.4. Show that a finite subgroup of $\mathbb{C}^*$ of order n is μ_n.

Exercise 2.2.5. Show that $\{1, -1, i, -i\}$ is a subgroup of $\mathbb{C}^*$, where $i = \sqrt{-1}$.

Exercise 2.2.6. For each integer $n \geq 1$, show that there is a commutative group of order n.

Remark 2.2.7. It is easy to see that any subgroup of an abelian group is abelian. However, the converse is not true, in general. For example, one can easily check that S_3 is a non-abelian group whose all proper subgroups are abelian.

Lemma 2.2.8. *Let G be a group. A non-empty subset $H \subseteq G$ forms a subgroup of G if and only if $ab^{-1} \in H$, for all $a, b \in H$.*

Proof. Since $H \neq \emptyset$, there is an element $a \in H$. Then $e = aa^{-1} \in H$. In particular, for any $b \in H$, its inverse $b^{-1} = eb^{-1} \in H$. Then for any $a, b \in H$, their product $ab = a(b^{-1})^{-1} \in H$. Thus H is closed under the binary operation induced from G. Associativity is obvious. Thus, H is a subgroup of G. □

Exercise 2.2.9 (Special linear group)**.** Fix an integer $n \geq 1$, and let

$$\mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) : \det(A) = 1\},$$

where $\det(A)$ denotes the determinant of the matrix A. Show that $\mathrm{SL}_n(\mathbb{R})$ is a non-trivial proper subgroup of $\mathrm{GL}_n(\mathbb{R})$. Also show that $\mathrm{SL}_n(\mathbb{R})$ is non-commutative for $n \geq 2$.

Proposition 2.2.10 (Center of a group)**.** *Let G be a group. Then*

$$Z(G) := \{a \in G \,:\, ab = ba, \forall\, b \in G\}$$

is a commutative subgroup of G, called the center of G.

Proof. Clearly $e \in Z(G)$. Let $a \in Z(G)$. Then for any $c \in G$ we have

$$ac = ca \;\Rightarrow\; c = a^{-1}ca \;\Rightarrow\; ca^{-1} = a^{-1}caa^{-1} = a^{-1}c,$$

and hence $a^{-1} \in Z(G)$. Then for any $a, b \in Z(G)$, we have $c(ab^{-1})c^{-1} = cac^{-1}cb^{-1}c^{-1} = ab^{-1}$, for all $c \in G$, and hence $ab^{-1} \in Z(G)$. Therefore, $Z(G)$ is a subgroup of G. Clearly $Z(G)$ is commutative. □

Exercise 2.2.11. Show that a group G is commutative if and only if $Z(G) = G$.

Exercise 2.2.12. Find the centers of S_3, $\mathrm{GL}_n(\mathbb{R})$ and $\mathrm{SL}_n(\mathbb{R})$, where $n \in \mathbb{N}$.

Lemma 2.2.13. *Let G be a group, and let $\{H_\alpha\}_{\alpha\in\Lambda}$ be a non-empty collection of subgroups of G. Then $\bigcap_{\alpha\in\Lambda} H_\alpha$ is a subgroup of G.*

Proof. Since $e \in H_\alpha$, for all $\alpha \in \Lambda$, we have $e \in \bigcap_{\alpha\in\Lambda} H_\alpha$. Let $a, b \in \bigcap_{\alpha\in\Lambda} H_\alpha$ be arbitrary. Since $a, b \in H_\alpha$, for all $\alpha \in \Lambda$, we have $ab^{-1} \in H_\alpha$, for all $\alpha \in \Lambda$, and hence $ab^{-1} \in \bigcap_{\alpha\in\Lambda} H_\alpha$. Thus $\bigcap_{\alpha\in\Lambda} H_\alpha$ is a subgroup of G. □

Corollary 2.2.14. *Let G be a group and S a subset of G. Let $\mathscr{C}_S$ be the collection of all subgroups of G that contains S. Then $\langle S \rangle := \bigcap_{H\in\mathscr{C}_S} H$ is the smallest subgroup of G containing S.*

Proof. By Lemma 2.2.13, $\langle S \rangle := \bigcap_{H\in\mathscr{C}_S} H$ is a subgroup of G containing S. If H' is any subgroup of G containing S, then $H' \in \mathcal{C}_S$, and hence $\langle S \rangle := \bigcap_{H\in\mathcal{C}_S} H \subseteq H'$. □

Exercise 2.2.15. Recall Exercise 2.2.2, and find the subgroup $2\mathbb{Z} \cap 3\mathbb{Z}$ of $\mathbb{Z}$.

Exercise 2.2.16. Is $2\mathbb{Z} \cup 3\mathbb{Z}$ a subgroup of $\mathbb{Z}$? Justify your answer.

Definition 2.2.17. Let G be a group and $S \subseteq G$. The group $\langle S \rangle := \bigcap_{H\in\mathcal{C}_S} H$ is called the *subgroup of G generated by S*. If S is a singleton subset $S = \{a\}$ of G, we denote by $\langle a \rangle$.

Exercise 2.2.18. Let G be a group. Find the subgroup of G generated by the empty subset of G.

Proposition 2.2.19. *Let G be a group, and let S be a non-empty subset of G. Then*

$$\langle S \rangle = \{a_1^{e_1} \cdots a_n^{e_n} \mid n \in \mathbb{N}, \text{ and } a_i \in S, e_i \in \{1, -1\}, \forall\, i \in \{1, 2, \ldots, n\}\}.$$

Proof. Let

$$K := \{a_1^{e_1} \cdots a_n^{e_n} \mid n \in \mathbb{N}, \text{ and } a_i \in S, e_i \in \{1, -1\}, \forall\, i \in \{1, 2, \ldots, n\}\}.$$

Clearly $S \subset K \subseteq G$. Taking $n = 2$, $a_1 = a_2 = a \in S$, $e_1 = 1$ and $e_2 = -1$, we have $e = a\,a^{-1} \in K$. Let $a, b \in K$. Then $a = a_1^{e_1} \cdots a_n^{e_n}$ and $b = b_1^{f_1} \cdots b_m^{f_m}$, for some $a_i, b_j \in S$, $e_i, f_j \in \{1, -1\}$, $1 \le i \le n$, $1 \le j \le m$, and $m, n \in \mathbb{N}$. Then $ab^{-1} = a_1^{e_1} \cdots a_n^{e_n} \cdot (b_1^{f_1} \cdots b_m^{f_m})^{-1} = a_1^{e_1} \cdots a_n^{e_n} \cdot b_m^{-f_m} \cdots b_1^{-f_1} \in K$. Therefore, K is a subgroup of G containing S. Then by Proposition 2.2.14, we have $\langle S \rangle \subseteq K$. To see the reverse inclusion, note that if $S \subseteq H$, for some subgroup H of G, then all the elements of K lies inside H. Therefore, $K \subseteq \bigcap_{H\in\mathscr{C}_S} H = \langle S \rangle$. □

Example 2.2.20. Let G be a group. Given an element $a \in G$, the subgroup of G generated by a can be written as

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\};$$

and is called the *cyclic subgroup* of G generated by a.

Definition 2.2.21. Let G be a group. The *order* of an element $a \in G$ is the smallest positive integer n, if exists, such that $a^n = e$. If no such positive integer n exists, we say that the order of a is infinite. We denote by $\mathrm{ord}(a)$ the order of $a \in G$. In other words, if we set $S_a := \{n \in \mathbb{Z} : n \ge 1 \text{ and } a^n = e\}$, then

$$\mathrm{ord}(a) := \begin{cases} \inf S_a, & \text{if} \quad S_a \neq \emptyset, \text{ and} \\ \infty, & \text{if} \quad S_a = \emptyset. \end{cases}$$

Exercise 2.2.22. Let G be a group and $a, b \in G$ be such that $ab = ba$. Show that $(ab)^n = a^n b^n$, for all $n \in \mathbb{N}$.

Exercise 2.2.23. Let G be a group. Let $a, b \in G$ be elements of finite orders.

(i) If $a^m = e$, for some $m \in \mathbb{N}$, then show that $\mathrm{ord}(a) \mid m$.

(ii) Show that $\mathrm{ord}(a^n) = \dfrac{\mathrm{ord}(a)}{\gcd\big(n,\ \mathrm{ord}(a)\big)}$, for all $n \in \mathbb{N}$.

(iii) Show that both a and a^{-1} have the same order in G.

(iv) Show that both ab and ba have the same finite order in G.

Exercise 2.2.24. Let G be a group, and let a and b two elements of G of finite orders with $ab = ba$.

(i) Show that $\mathrm{ord}(ab)$ divides $\mathrm{lcm}(\mathrm{ord}(a), \mathrm{ord}(b))$.

(ii) If $\gcd(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$, show that $\mathrm{ord}(ab) = \mathrm{ord}(a)\,\mathrm{ord}(b)$.

Theorem 2.2.25. *Given any integers $m, n, r > 1$, there exists a finite group G with elements $a, b \in G$ such that $\mathrm{ord}(a) = m$, $\mathrm{ord}(b) = n$ and $\mathrm{ord}(ab) = r$.*

Proof. Requires structure theorem for finite abelian group and concept of finite field, so a proof of this fact may appear at the end of this course. □

Exercise 2.2.26. Find two elements σ and τ of S_3 that generates it.

Exercise 2.2.27 (Derived subgroup)**.** Let G be a group. The *commutator* of two elements $a, b \in G$ is the element $[a, b] := aba^{-1}b^{-1} \in G$. Given $a, b \in G$, show that

(i) $[a, b] = e$ if and only if $ab = ba$;

(ii) $[a, b]^{-1} = [b, a]$; and

(iii) $g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}]$, for all $g \in G$.

The subgroup $[G, G] := \langle\, [a, b] : a, b \in G \rangle$ of G generated by all commutators of elements of G is called the *derived subgroup* or the *commutator subgroup* of G. Show that $[G, G]$ is a trivial subgroup of G if and only if G is abelian.

2.3 Cyclic group

Let G be a group. For any element $a \in G$, we consider the subset

$$\langle a \rangle := \{a^n : n \in \mathbb{Z}\} \subseteq G.$$

Clearly $e \in \langle a \rangle$, and for any two elements $a^n, a^m \in \langle a \rangle$, we have $a^n \cdot (b^m)^{-1} = a^{n-m} \in \langle a \rangle$. Therefore, $\langle a \rangle$ is a subgroup of G, called the *cyclic subgroup* of G generated by a. If H is any subgroup of G with $a \in H$, then $a^{-1} \in H$, and hence $a^n \in H$, for all $n \in \mathbb{Z}$. Therefore, $\langle\, a \,\rangle \subseteq H$. Therefore, $\langle\, a \,\rangle$ is the smallest subgroup of G containing a.

Definition 2.3.1. A group G is said to be *cyclic* if there is an element $a \in G$ such that $G = \langle a \rangle$. The element a is called the *generator* of $\langle a \rangle$.

Remark 2.3.2. If G is a cyclic group generated by $a \in G$, then $\langle\, a^{-1} \,\rangle = G$. Therefore, if $a^2 \neq e$, the cyclic group $\langle\, a \,\rangle$ has at least two distinct generators, namely a and a^{-1}. We shall see later that if a cyclic group $\langle\, a \,\rangle$ has at least two distinct generators, then we must have $a^2 \neq e$.

For example, the additive group $\mathbb{Z}$ is a cyclic group generated by 1 or -1. It is clear that a cyclic group may have more than one generators. For example, $\mathbb{Z}_3$ is a cyclic group that can be generated by $[1]$ or $[2]$.

Example 2.3.3. $\mathbb{Z}_n$ is a finite cyclic group generated by $[1] \in \mathbb{Z}_n$. To see this, note that for any $[m] \in \mathbb{Z}_n$, we have $[m] = [m \cdot 1] = m[1] \in \langle\, [1] \,\rangle \subseteq \mathbb{Z}_n$. Therefore, $\mathbb{Z}_n \subseteq \langle\, [1] \,\rangle$, and hence $\mathbb{Z}_n = \langle\, [1] \,\rangle$.

Proposition 2.3.4. *Fix an integer $n \geq 2$. Then $[a] \in \mathbb{Z}_n$ is a generator of the group $\mathbb{Z}_n$ if and only if $\gcd(a, n) = 1$.*

Proof. Suppose that $\langle\, [a] \,\rangle = \mathbb{Z}_n$. Then there exists $m \in \mathbb{Z}$ such that $[1] = m[a] = [ma]$. Then $n \mid (ma - 1)$ and so $ma - 1 = nd$, for some $d \in \mathbb{Z}$. Therefore, $ma + n(-d) = 1$, and hence by Corollary 1.3.8 we have $\gcd(a, n) = 1$. Conversely, if $\gcd(a, n) = 1$, then there exists $m, q \in \mathbb{Z}$ such that $am + nq = 1$. Then $n \mid (1 - am)$ and hence $[a] = [1]$ in $\mathbb{Z}_n$. Hence the result follows. □

Corollary 2.3.5. *For a prime number $p > 0$, $\mathbb{Z}_p$ has $p - 1$ distinct generators.*

Clearly any cyclic group is abelian. However, the converse is not true in general. For example, the Klein four-group K_4 in Example 2.1.9 (iii) is abelian but not cyclic (verify).

Exercise 2.3.6. Give an example of an infinite abelian group which is not cyclic.

Proposition 2.3.7. *Subgroup of a cyclic group is cyclic.*

Proof. Let $G = \langle\, a \,\rangle$ be a cyclic group generated by $a \in G$. Let $H \subseteq G$ be a subgroup of G. If $H = \{e\}$ is the trivial subgroup of G, then $H = \langle\, e \,\rangle$. Suppose that $H \neq \{e\}$. Then there exists $b \in G$ such that $b \neq e$ and $b \in H$. Since $G = \langle\, a \,\rangle$, we have $b = a^n$, for some $n \in \mathbb{Z}$. Since H is a group and $a^n = b \in H$, we have $a^{-n} = b^{-1} \in H$. Therefore,

$$S := \{k \in \mathbb{N} : a^k \in H\} \subseteq \mathbb{N}$$

is a non-empty subset of $\mathbb{N}$. Then by well-ordering principle of $(\mathbb{N}, \leq)$ (see Theorem 1.1.25) S has a least element, say $m \in S$. We claim that $H = \langle\, a^m \,\rangle$. Clearly $\langle\, a^m \,\rangle \subseteq H$. Let $h \in H$ be arbitrary. Since $H \subseteq G = \langle\, a \,\rangle$, we have $h = a^n$, for some $n \in \mathbb{Z}$. Then by division algorithm (see Theorem 1.3.1) there exists $q, r \in \mathbb{Z}$ with $0 \leq r < m$ such that $n = mq + r$. Then $a^r = a^{n-mq} = a^n(a^m)^{-q} = h(a^m)^{-q} \in H$. Since m is the least element of S, we must have $r = 0$. Then $n = mq$, and so we have $h = a^n = a^m q \in \langle\, a^m \,\rangle$. Therefore, $H \subseteq \langle\, a^m \,\rangle$, and hence $H = \langle\, a^m \,\rangle$. □

Exercise 2.3.8. Show that any subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z} := \{nk : k \in \mathbb{Z}\}$, for some $n \in \mathbb{Z}$.

Lemma 2.3.9. *Let $G = \langle\, a \,\rangle$ be an infinite cyclic group. Then for all $m, n \in \mathbb{Z}$ with $m \neq n$, we have $a^n \neq a^m$.*

Proof. Suppose not, then there exists $m, n \in \mathbb{Z}$ with $m > n$ such that $a^m = a^n$. Then $a^{m-n} = a^m(a^n)^{-1} = e$. Since $m - n$ is a positive integer, the subset

$$S := \{k \in \mathbb{N} : a^k = e\} \subseteq \mathbb{N}$$

is non-empty. Then by well-ordering principle S has a least element, say d. We claim that $G = \{a^k : k \in \mathbb{Z} \text{ with } 0 \leq k \leq d - 1\}$. Clearly $\{a^k : k \in \mathbb{Z} \text{ with } 0 \leq k \leq d - 1\} \subseteq G$. Let $b \in G$ be arbitrary. Then $b = a^n$, for some $n \in \mathbb{Z}$. Then by division algorithm (Theorem 1.3.1), there exists $q, r \in \mathbb{Z}$ with $0 \leq r < d$ such that $n = dq + r$. Since $d \in S$, we have $a^d = e$. Then $b = a^n = a^{dq+r} = (a^d)^q a^r = a^r \in \{a^k : k \in \mathbb{Z} \text{ with } 0 \leq k \leq d - 1\}$ implies $G \subseteq \{a^k : k \in \mathbb{Z} \text{ with } 0 \leq k \leq d - 1\}$, and hence $G = \{a^k : k \in \mathbb{Z} \text{ with } 0 \leq k \leq d - 1\}$. This is not possible since G is infinite by our assumption. Hence the result follows. □

Corollary 2.3.10. *Let $G = \langle a \rangle$ be a cyclic group generated by $a \in G$. Then G is infinite if and only if $\mathrm{ord}(a)$ is infinite.*

Proof. If $G = \langle a \rangle$ is infinite, then for any non-zero integer n, we have $a^n \neq a^0 = e$ by Lemma 2.3.9. Therefore, $\mathrm{ord}(a)$ is infinite. Conversely, if $\mathrm{ord}(a)$ is infinite, then $a^n \neq e$, for all $n \in \mathbb{Z}\backslash\{0\}$. Since $a^n = a^m$ implies $a^{m-n} = e$, the map $f : \mathbb{Z} \to G$ given by $f(n) = a^n$, $\forall\, n \in \mathbb{Z}$, is injective. Therefore, since $\mathbb{Z}$ is infinite, G must be infinite. □

Corollary 2.3.11. *Let G be a finite cyclic group generated by a. Then $|G| = \mathrm{ord}(a)$.*

Proof. Since G is finite, $\mathrm{ord}(a)$ must be finite by Corollary 2.3.10. Suppose that $\mathrm{ord}(a) = n \in \mathbb{N}$. Then for any two integers $r, s \in \{k \in \mathbb{Z} : 0 \leq k \leq n-1\}$, $a^r = a^s$ implies $a^{r-s} = e$, and hence $r = s$, because $|r - s| < n = \mathrm{ord}(a)$. Then all the elements in the collection $\mathscr{C} := \{a^k : k \in \mathbb{Z} \text{ with } 0 \leq k \leq n-1\}$ are distinct, and that $\mathscr{C}$ has n elements. Clearly $\mathscr{C} \subseteq G$. Given any $b \in G = \langle a \rangle$, $b = a^m$, for some $m \in \mathbb{Z}$. Then by division algorithm (Theorem 1.3.1) there exists $q, r \in \mathbb{Z}$ with $0 \leq r < n$ such that $m = nq + r$. Then $b = a^m = a^{nq+r} = (a^n)^q a^r = a^r \in \mathscr{C}$, since $a^n = e$. Therefore, $G \subseteq \mathscr{C}$, and hence $G = \mathscr{C}$. Thus, $|G| = \mathrm{ord}(a)$. □

Corollary 2.3.12. *Let G be a finite group of order n. Then G is cyclic if and only if it contains an element of order n.*

Proof. If G is cyclic, then the result follows from Corollary 2.3.11. Conversely, if G contains an element a of order n, then it follows from the proof of Corollary 2.3.11 that the cyclic subgroup $\langle a \rangle$ of G has n elements, and hence $\langle a \rangle = G$. □

Corollary 2.3.13. *Any non-trivial subgroup of an infinite cyclic group is infinite and cyclic.*

Proof. Let G be an infinite cyclic group generated by $a \in G$. Let H be a non-trivial subgroup of G. Since H is cyclic by Proposition 2.3.7, we have $H = \langle b \rangle$, where $b = a^r$ for some $r \in \mathbb{Z} \setminus \{0\}$. Since G is an infinite cyclic group, by above Lemma 2.3.9, we have $b^m = a^{mr} \neq a^{nr} = b^n$ for $m \neq n$ in $\mathbb{Z}$. Therefore, $H = \langle b \rangle = \{b^k : k \in \mathbb{Z}\}$ is infinite. □

Proposition 2.3.14. *Let G be a finite cyclic group of order n. Then for each positive integer d such that $d \mid n$, there is a unique subgroup H of G of order d.*

Proof. Let $G = \langle a \rangle$ be a finite cyclic group of order n. Then $\mathrm{ord}(a) = n$ by Corollary 2.3.11. Since $d \mid n$, there exists $q \in \mathbb{Z}$ such that

$$n = dq.$$

Let $H := \langle a^q \rangle$ be the cyclic subgroup of G generated by a^q. Since G is finite, so is H. Since $\mathrm{ord}(a) = n$, we see that d is the least positive integer such that $(a^q)^d = a^{qd} = a^n = e$. Therefore, $\mathrm{ord}(a^q) = d$, and hence $|H| = d$ by Corollary 2.3.11.

We now show uniqueness of H in G. If $d = 1$, then the trivial subgroup $\{e\} \subseteq G$ is the only subgroup of G of order $d = 1$. Suppose that $d > 1$. Let H and K be two subgroups of G of order d, where $d \mid n$. Then by Proposition 2.3.7 we have $H = \langle a^n \rangle$ and $K = \langle a^m \rangle$, for some $m, n \in \mathbb{N}$. Since subgroup of a finite group is finite, by Corollary 2.3.10 we have $\mathrm{ord}(a^n) = d = \mathrm{ord}(a^m)$. By division algorithm (Theorem 1.3.1) there exists unique integers k, r with $0 \leq r < q$ such that $m = kq + r$. Then $dm = kdq + dr = kn + dr$ gives

$$e = (a^m)^d = a^{dm} = (a^n)^k a^{dr} = a^{dr}.$$

Since $0 \leq r < q$, we have $0 \leq dr < dq = n$. If $r \neq 0$, this contradicts the fact that $\mathrm{ord}(a) = n$. Therefore, we must have $r = 0$, and hence $a^m = a^{kq+r} = (a^k)^q \in \langle a^k \rangle = H$. Therefore, $K \subseteq H$. Since $|H| = |K| = d$, we have $H = K$. □

Proposition 2.3.15. *An infinite cyclic group has exactly two generators.*

Proof. Let $G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ be an infinite cyclic group. Let $b \in G$ be any generator of G. Then $b = a^n$, for some $n \in \mathbb{Z}$. Similarly, since $a \in G = \langle b \rangle$, we have $a = b^m$, for some $m \in \mathbb{Z}$. Then we have $a = b^m = (a^n)^m = a^{mn}$. Then by Lemma 2.3.9 we have $mn = 1$. Since both m and n are integers, we must have $m, n \in \{1, -1\}$. Therefore, $b \in \{a, a^{-1}\}$. □

Exercise 2.3.16. Let $G = \langle a \rangle$ be a finite cyclic group of order n. Given any $k \in \mathbb{N}$ with $1 \leq k \leq n-1$, show that $\langle a^k \rangle = G$ if and only if $\gcd(n, k) = 1$. Conclude that G has exactly $\phi(n)$ number of generators, where $\phi(n)$ is the number of elements in the set $\{k \in \mathbb{N} : \gcd(n, k) = 1\}$. (*Hint:* Use the idea of the proof of Proposition 2.3.4.)

Remark 2.3.17. The map $\phi : \mathbb{N} \to \mathbb{N}$ given by sending $n \in \mathbb{N}$ to the cardinality of the set

$$\{k \in \mathbb{N} : 1 \leq k \leq n \text{ and } \gcd(n, k) = 1\},$$

is called the *Euler phi function*.

Exercise 2.3.18. Give an example of a non-abelian group G such that all of its proper subgroups are cyclic.

2.4 Product of Groups

Definition 2.4.1. Let G be a group. For any two non-empty subsets H and K of G, we define their product $HK := \{hk : h \in H, k \in K\}$.

Exercise 2.4.2. Show by example that HK need not be a group in general even if both H and K are subgroups of a group.

Theorem 2.4.3. *Let H and K be two subgroups of G. Then HK is a group if and only if $HK = KH$.*

Proof. Note that, for any $h \in H$ and $k \in K$ we have $h = h \cdot e \in HK$ and $k = e \cdot k \in HK$. Therefore, $H \subseteq HK$ and $K \subseteq HK$.

Suppose that HK is a group. Then $kh \in HK$, for all $h \in H \subseteq HK$ and $k \in K \subseteq HK$, and hence $KH \subseteq HK$. Let $h \in H$ and $k \in K$. Since HK is a group, $hk \in HK$ implies $(hk)^{-1} \in HK$, and so $(hk)^{-1} = h_1 k_1$, for some $h_1 \in H$ and $k_1 \in K$. Then $hk = \left((hk)^{-1}\right)^{-1} = k_1^{-1} h_1^{-1} \in KH$. Therefore, $HK \subseteq KH$, and hence $HK = KH$.

Conversely suppose that $HK = KH$. Let $h_1 k_1, h_2 k_2 \in HK$ with $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Since $k_2^{-1} h_2^{-1} \in KH = HK$, there exists $h_3 \in H$ and $k_3 \in K$ such that $k_2^{-1} h_2^{-1} = h_3 k_3$. Again $k_1 h_3 \in KH = HK$ implies there exists $h_4 \in H$ and $k_4 \in K$ such that $k_1 h_3 = h_4 k_4$. Now

$$\begin{aligned}(h_1 k_1)(h_2 k_2)^{-1} &= h_1 k_1 k_2^{-1} h_2^{-1} \\ &= h_1 k_1 h_3 k_3 \\ &= h_1 h_4 k_4 k_3 \in HK.\end{aligned}$$

Therefore, HK is a subgroup of G. □

Corollary 2.4.4. *If H and K are subgroups of a commutative group, then HK is a group.*

Notation: For a finite set S, we denote by $|S|$ the number of elements of S.

Remark 2.4.5. The phrase "number of elements of S" is ambiguous when S is not a finite set. For example, both $\mathbb{Z}$ and $\mathbb{R}$ are infinite sets, but there are some considerable differences between "the number of elements" of them; $\mathbb{Z}$ is a countable set, while $\mathbb{R}$ is an uncountable set. So the "number of elements" (whatever that means) for $\mathbb{Z}$ and $\mathbb{R}$ should not be the same. For this reason, we need an appropriate concept of "number of elements" for an infinite set S, known as the *cardinality* of S, also denoted by $|S|$. When S is a finite set, the cardinality

of S is determined by the number of elements of S. The cardinality of $\mathbb{Z}$ is denoted by $\aleph_0$ (aleph-naught) and the cardinality of $\mathbb{R}$ is $2^{\aleph_0}$, which is also denoted by $\aleph_1$ or $\mathfrak{c}$.

Definition 2.4.6. The *order* of a group G is the cardinality $|G|$ of its underlying set G. For a finite group, its order is precisely the number of elements in it.

For example, the order of S_3 is 6, while the order of $\mathbb{Z}$ is $\aleph_0$.

Proposition 2.4.7. *If H and K are finite subgroups of a group G, then*

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

Proof. For each positive integer n, let $J_n := \{k \in \mathbb{N} : k \leq n\}$. Let $H = \{h_i : i \in J_n\}$ and $K = \{k_j : j \in J_m\}$. Then $HK = \{h_i k_j : i \in J_n,\ j \in J_m\}$. To find the number of elements of HK, for each pair $(i, j) \in J_n \times J_m$, we need to count the number of times $h_i k_j$ repeats in the collection $\mathscr{C} := \{h_i k_j : (i, j) \in J_n \times J_m\}$. Fix $(i, j) \in J_n \times J_m$. If $h_i k_j = h_p k_q$, for some $(p, q) \in J_n \times J_m$, then $t := h_p^{-1} h_i = k_q k_j^{-1} \in H \cap K$. So any element $h_p k_q \in \mathscr{C}$, which coincides with $h_i k_j$ is of the form $(h_i t^{-1})(t k_j)$, for some $t \in H \cap K$. Conversely, for any $t \in H \cap K$, we have $(h_i t^{-1})(t k_j) = h_i (t^{-1} t) k_j = h_i e k_j = h_i k_j$. Therefore, the element $h_i k_j$ appears exactly $|H \cap K|$-times in the collection $\mathscr{C}$, and hence we have

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

This completes the proof. □

Proposition 2.4.8. *Let H and K be subgroups of G. Then HK is a subgroup of G if and only if $HK = \langle H \cup K \rangle$.*

Proof. Suppose that HK is a subgroup of G. Since $H \subseteq HK$ and $K \subseteq HK$, we have $H \cup K \subseteq HK$, and hence $\langle H \cup K \rangle \subseteq HK$. Since $\langle H \cup K \rangle$ is a group containing $H \cup K$, for any $h \in H$ and $k \in K$ we have $hk \in \langle H \cup K \rangle$. Therefore, $HK \subseteq \langle H \cup K \rangle$, and hence $HK = \langle H \cup K \rangle$. Converse is obvious since $\langle H \cup K \rangle$ is a group and $HK = \langle H \cup K \rangle$ by assumption. □

2.5 Permutation Groups

Let X be a non-empty set. A *permutation* on X is a bijective map $\sigma : X \to X$. We denote by S_X the set of all permutations on X. For notational simplicity, when $|X| = n$, fixing a bijection of X with the subset $J_n := \{1, 2, 3, \ldots, n\} \subset \mathbb{N}$ we may identify S_X with S_n. An element $\sigma \in S_n$ may be described as follow.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix} \quad \text{or,} \quad \sigma = \begin{cases} 1 \mapsto \sigma(1) \\ 2 \mapsto \sigma(2) \\ \quad \vdots \\ n \mapsto \sigma(n) \end{cases}.$$

Since elements of S_n are bijective maps of J_n onto itself, composition of two elements of S_n is again an element of S_n. Thus we have a binary operation

$$\circ : S_n \times S_n \longrightarrow S_n, \ \ (\sigma, \tau) \longmapsto \tau \circ \sigma.$$

For example, consider the elements $\sigma, \tau \in S_4$ defined by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}, \ \ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}.$$

Then their composition $\tau \circ \sigma$ is the permutation

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

Clearly composition of functions $J_n \to J_n$ is associative, and for any $\sigma \in S_n$ its pre-composition and post-composition with the identity map of I_n is σ itself. Also inverse of a bijective map is again bijective. Thus for all integer $n \geq 1$, $(S_n, \circ)$ is a group, called the *Symmetric group* (or, the *permutation group*) on J_n.

Remark 2.5.1. For each integer $n \geq 0$, the symmetric group S_{n+1} can be understood as the group of symmetries of a regular n-simplex inside $\mathbb{R}^{n+1}$. The *standard n-simplex*

$$\Delta^n := \{(t_0, \ldots, t_n) \in \mathbb{R}^{n+1} : \sum_{j=1}^{n} t_j = 1,\ t_j \geq 1, \forall\, j = 0, 1, \ldots, n.\} \subset \mathbb{R}^{n+1}$$

is an example of a regular n-simplex. This has vertices the unit vectors $\{e_0, e_1, \ldots, e_n\}$ in $\mathbb{R}^{n+1}$, where

$$\begin{array}{ll} e_0 & = (1, 0, 0, \ldots, 0, 0), \\ e_1 & = (0, 1, 0, \ldots, 0, 0), \\ \vdots & \qquad\qquad \vdots \\ e_n & = (0, 0, 0, \ldots, 0, 1). \end{array}$$

For example,

- Δ^0 is a point,
- Δ^1 is the straight line segment $[-1, 1] \subset \mathbb{R} \subset \mathbb{R}^2$,
- Δ^2 is an equilateral triangle in the plane $\mathbb{R}^2$,
- Δ^3 is a regular tetrahedron in $\mathbb{R}^3$, and so on.

Exercise 2.5.2. Show that S_1 is a trivial group, and S_2 is an abelian group with two elements.

Lemma 2.5.3. *For all integer $n \geq 3$, the group S_n is non-commutative.*

Proof. Let $\sigma, \tau \in S_n$ be defined by

$$\sigma(k) = \begin{cases} 2, & \text{if} \quad k = 1 \\ 1, & \text{if} \quad k = 2 \\ k, & \text{if} \quad k \in I_n \setminus \{1, 2\} \end{cases}, \quad \text{and } \tau(k) = \begin{cases} 3, & \text{if} \quad k = 1 \\ 1, & \text{if} \quad k = 3 \\ k, & \text{if} \quad k \in I_n \setminus \{1, 3\} \end{cases}.$$

Since $\tau \circ \sigma(1) = 2$ and $\sigma \circ \tau(1) = 3$, we have $\sigma \circ \tau \neq \tau \circ \sigma$. Therefore, S_n is non-commutative. □

Let $\sigma \in S_n$. If $\sigma(k) = k$, for some $k \in J_n$, we may drop the corresponding column from its two-column notation, and rearrange its columns, if required, to get a cyclic expression like

$$\sigma = \begin{pmatrix} k_1 & k_2 & \cdots & k_{r-1} & k_r \\ k_2 & k_3 & \cdots & k_r & k_1 \end{pmatrix},$$

where $k_1, \ldots, k_r$ are all distinct, to denote the permutation $\sigma \in S_n$ defined by

$$\sigma(k_j) = \begin{cases} k_{j+1}, & \text{if} \quad j \in \{1, \ldots, r-1\}, \\ k_1, & \text{if} \quad j = r, \text{ and} \\ k_j, & \text{if} \quad k_j \in J_n \setminus \{k_1, \ldots, k_r\}. \end{cases} \tag{2.5.4}$$

We may further simplify this expression and write it in cyclic notation as

$$\sigma = \begin{pmatrix} k_1 & k_2 & \cdots & k_{r-1} & k_r \\ k_2 & k_3 & \cdots & k_r & k_1 \end{pmatrix} = (k_1\ k_2\ k_3\ \cdots\ k_r). \tag{2.5.5}$$

An element $\sigma \in S_n$ is said to be an *r-cycle* if it can be expressed in a cyclic form $(k_1\ k_2\ k_3\ \cdots\ k_r)$ as in (2.5.5). The integer r is called the length of the cycle σ. A 2-cycle is called a *transposition*.

Remark 2.5.6. Transpositions are of particular interests. We shall see later that any $\sigma \in S_n$ can be written as product of either even number of transpositions or odd number of transpositions, and accordingly we call $\sigma \in S_n$ an even permutation or an odd permutation.

Example 2.5.7. Using cycle notation, the group S_3 can be written as

$$S_3 = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\},$$

where $(1\ 2)$, $(1\ 3)$ and $(2\ 3)$ are transpositions. However, we can write 3-cycles as product of 2-cycles as $(1\ 2\ 3) = (2\ 3) \circ (1\ 3)$ and $(1\ 3\ 2) = (2\ 3) \circ (1\ 2)$. Also, the identity element e can be written as $e = (1\ 2) \circ (1\ 2)$ or $e = (1\ 3) \circ (1\ 3)$ etc. So the decomposition of $\sigma \in S_n$ as a product of transpositions is not unique.

Proposition 2.5.8. *Let $\sigma \in S_n$ be a cycle. Then σ is a r cycle if and only if* $\mathrm{ord}(\sigma) = r$.

Outline of proof. Let $\sigma = (k_1\ k_2\ \cdots\ k_r)$, for some $k_1, \ldots, k_r \in J_n$. It follows from the definition of the cyclic expression of σ given in (2.5.4) that $\sigma^r(j) = j$, for all $j \in J_n$. In other words, $\sigma^r = e$, where e is the identity element in S_n. Since $\sigma^s(k_1) = k_{s+1}$, for all $s \in \{1, \ldots, r-1\}$ (see (2.5.4)), we conclude that r is the smallest positive integer such that $\sigma^r = e$ in S_n. Therefore, $\mathrm{ord}(\sigma) = r$. The converse is also similar. Details are left as an exercise. □

Proposition 2.5.9. *The number of distinct r cycles in S_n is* $\dfrac{n!}{r(n-r)!}$.

Proof. Note that, we can choose a r cycle from S_n in

$${}^nC_r = \binom{n}{r} = \frac{n!}{r!(n-r)!}$$

ways. Fix a r-cycle $\sigma = (k_1\ k_2\ \cdots\ k_r) \in S_n$. Note that, the cycles

$$(k_1\ k_2\ \cdots\ k_r) \quad \text{and} \quad (k_2\ k_3\ \cdots\ k_r\ k_1)$$

represents the same element $\sigma \in S_n$. Note that, given any two permutations (bijective maps)

$$\phi, \psi : \{2, 3, \ldots, r\} \to \{2, 3, \ldots, r\},$$

two r cycles (note that k_1 is fixed!)

$$(k_1\ k_{\phi(2)}\ \cdots\ k_{\phi(r)}) \text{ and } (k_1\ k_{\psi(2)}\ \cdots\ k_{\psi(r)})$$

represents the same element of S_n if and only if $\phi = \psi$. Since there are $(r-1)!$ number of distinct bijective maps $\{2, 3, \ldots, r\} \to \{2, 3, \ldots, r\}$ (verify!), fixing k_1 in one choice of r cycle $(k_1\ k_2\ \cdots\ k_r)$ in S_n, considering all permutations of the remaining $(r-1)$ entries $k_2, \ldots, k_r$, we get $(r-1)!$ number of distinct r cycles in S_n. Therefore, the total number of distinct r cycles in S_n is precisely

$$(r-1)! \cdot \frac{n!}{r!(n-r)!} = \frac{n!}{r(n-r)!}.$$

This completes the proof. □

Definition 2.5.10. Two cycles $\sigma = (i_1 \ \ i_2 \cdots \ i_k)$ and $\tau = (j_1 \ \ j_2 \ \cdots \ j_\ell)$ in S_n are said to be *disjoint* if $\{i_1, i_2, \ldots, i_k\} \cap \{j_1, j_2, \cdots, j_\ell\} = \emptyset$.

Exercise 2.5.11. If σ and τ are disjoint cycles in S_n, show that $\sigma \circ \tau = \tau \circ \sigma$.

Theorem 2.5.12. *For $n \geq 2$, any non-identity element of S_n can be written as a product of disjoint cycles of length at least 2. This expression is unique up to ordering of factors.*

Theorem 2.5.13. *For $n \geq 2$, every element of S_n can be written as a finite product of transpositions. This expression is not unique. However, the number of transpositions appearing in such a product expression for $\sigma \in S_n$ is either odd or even, but cannot be both.*

Definition 2.5.14. A permutation $\sigma \in S_n$ is called *even* (respectively, *odd*) if σ can be written as a product of even (respectively, odd) number of disjoint transpositions in S_n.

Exercise 2.5.15. Express the following permutations as product of disjoint cycles, and then express them as a product of transpositions. Determine if they are even or odd permutations.

(i) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 8 & 5 & 6 & 4 & 7 & 1 \end{pmatrix} \in S_8$.

Answer: Note that,

$$\begin{aligned} \sigma &= (1 \ \ 2 \ \ 3 \ \ 8) \circ (4 \ \ 5 \ \ 6) \\ &= (1 \ \ 8) \circ (1 \ \ 3) \circ (1 \ \ 2) \circ (4 \ \ 6) \circ (4 \ \ 5). \end{aligned}$$

Therefore, σ is odd.

(ii) $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 4 & 2 & 3 & 6 \end{pmatrix} \in S_6$.

(iii) $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 6 & 1 & 3 & 7 & 5 \end{pmatrix} \in S_7$.

Proposition 2.5.16. *Let $A_n = \{\sigma \in S_n : \sigma \text{ is even}\}$ be the set of all even permutations in S_n. Then A_n is a subgroup of S_n, known as the alternating group on J_n.*

Proof. Since $e = (1 \ \ 2) \circ (1 \ \ 2)$, we see that $e \in A_n$. Thus A_n is a non-empty subset of S_n. Let $\sigma, \tau \in A_n$ be arbitrary. Suppose that $\tau = \tau_1 \circ \cdots \circ \tau_{2r}$, where $\tau_1, \ldots, \tau_{2r}$ are transpositions in S_n. Since transpositions are elements of order 2 (see Proposition 2.5.8), they are self inverse in S_n. Now it follows from Exercise 2.1.8 (ii) that

$$\tau^{-1} = \tau_{2r} \circ \cdots \circ \tau_1.$$

Therefore, τ^{-1} is also an even permutation. Since σ and τ^{-1} are even, their product $\sigma \circ \tau^{-1} \in A_n$. Therefore, A_n is a subgroup of S_n by Lemma 2.2.8. □

Remark 2.5.17. Assume that $n \geq 3$. Note that, any transposition $(i \ \ j) \in S_n$, with $i \neq 1$ and $j \neq 1$, can be written as

$$(i \ \ j) = (1 \ \ i) \circ (1 \ \ j) \circ (1 \ \ i).$$

Again $(1 \ \ i) \circ (1 \ \ j) = (1 \ \ j \ \ i)$. Since each element of A_n are product of even number of transpositions, using above two observations, one can write each element of A_n as product of 3 cycles in S_n.

Exercise 2.5.18. Show that $|A_n| = n!/2$.

Exercise 2.5.19. Determine the groups A_3 and A_4.

Exercise 2.5.20. Given $\sigma, \tau \in S_n$, show that $[\sigma, \tau] := \sigma \circ \tau \circ \sigma^{-1} \circ \tau^{-1} \in A_n$. The element $[\sigma, \tau]$ is called the *commutator of σ and τ* in S_n.

Example 2.5.21 (Dihedral group D_n)**.** Consider a regular n-gon in the plane $\mathbb{R}^2$ whose vertices are labelled as $1, 2, 3, \ldots, n$ in clockwise order. Let D_n be the set of all symmetries of this regular n-gon given by the following operations and their finite compositions:

$a :=$ The rotations about its centre through the angles $2\pi/n$, and

$b :=$ The reflections along the vertical straight line passing through the centre of the regular n-gon.

Note that $\mathrm{ord}(a) = n$, $\mathrm{ord}(b) = 2$ and that $a^{n-1}b = ba$. Therefore, the group generated by all such symmetries of the regular n-gon can be expressed in terms of generators and relations as

$$D_n := \langle\, a, b \mid \mathrm{ord}(a) = n, \mathrm{ord}(b) = 2, \text{ and } a^{n-1}b = ba \,\rangle.$$

This group is called the *dihedral group* of degree n. Note that D_n is a non-commutative finite group of order $2n$ and its elements can be expressed as

$$D_n = \{e, a, a^2, a^3, \ldots, a^{n-1}, b, ba, ba^2, ba^3, \ldots, ba^{n-1}\}.$$

Note that each element of D_n is given by a bijection of the set $J_n := \{1, 2, \ldots, n\}$ onto itself, and hence is a permutation on J_n. However, not all permutations of the set J_n corresponds to a symmetry of a regular n-gon as described above (see Exercise 2.5.22 below). We can define a binary operation on D_n by composition of bijective maps. Then it is easy to check using Lemma 2.2.8 that D_n is a subgroup of S_n. The group D_n is called the *Dihedral group* of degree n. It is a finite group of order $2n$ which is non-commutative for $n \geq 3$.

Exercise 2.5.22. Show that $D_3 = S_3$, and D_n is a proper subgroup of S_n, for all $n \geq 4$.

Exercise 2.5.23. Let G be the subgroup of S_4 generated by the cycles

$$a := (1\ \ 2\ \ 3\ \ 4) \text{ and } b := (2\ \ 4)$$

in S_4. Show that G is a dihedral group of degree 4.

2.6 Coset, Normal Subgroup & Quotient Group

Let G be a group, and H a subgroup of G. Define a relation $\rho_L \subseteq G \times G$ on G by setting

$$(a, b) \in \rho_L \text{ if } a^{-1}b \in H. \tag{2.6.1}$$

Clearly ρ_L is reflexive because $a^{-1}a = e \in H$, $\forall\ a \in G$. If $(a, b) \in \rho_L$, then $a^{-1}b \in H$, and so $b^{-1}a = (a^{-1}b)^{-1} \in H$, which gives $(b, a) \in \rho_L$. Therefore, ρ_L is symmetric. Suppose that $(a, b), (b, c) \in \rho_L$. Then $a^{-1}b, b^{-1}c \in H$, and so $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$. Therefore, $(a, c) \in \rho_L$. Thus, ρ_L is transitive. Therefore, ρ_L is an equivalence relation on G. Then by Proposition 2.1.31 we can write G as a disjoint union of ρ_L-equivalence classes of its elements.

Note that, the ρ_L-equivalence class of $a \in G$ is the subset

$$\begin{aligned}[a]_{\rho_L} &= \{b \in G : a^{-1}b \in H\} \\ &= \{ah : h \in H\},\end{aligned}$$

which, for notational simplicity, we denote by aH, and call it the *left coset* of H in G represented by $a \in G$. Given $a, b \in G$, it follows from Proposition 2.1.29 that either $aH = bH$ or $aH \cap bH = \emptyset$.

Proposition 2.6.2. *For each $a \in G$, the map $\varphi_a : H \to aH$ defined by $\varphi_a(h) = ah$, for all $h \in H$, is bijective. Consequently, $|aH| = |bH|$, for all $a, b \in H$.*

Proof. Since every element of aH is of the form ah, for some $h \in H$, we see that $\varphi_a(h) = ah$, and hence φ_a is surjective. Since $ah = ah'$ implies that $h = (a^{-1}a)h = a^{-1}(ah) = a^{-1}(ah') = (a^{-1}a)h' = h'$, we see that φ_a is injective. Therefore, φ_a is bijective. Thus, both H and aH have the same cardinality. □

Let $G/H = \{aH : a \in G\}$ be the set of all distinct left cosets of H in G.

Theorem 2.6.3 (Lagrange's Theorem)**.** *Let G be a finite group, and H a subgroup of G. Then $|H|$ divides $|G|$.*

Proof. Since ρ_L is an equivalence relation on G, it follows from Proposition 2.1.31 that G is a disjoint union of distinct left cosets of H in G. Since G is finite, there can be at most finitely many distinct left cosets of H in G. Since $|aH| = |bH|$, for all $a, b \in G$ (see Proposition 2.6.2), it follows that

$$|G| = |G/H| \cdot |H|,$$

where $|G/H|$ is the cardinality of the set G/H, i.e., the number of distinct left cosets of H in G. This completes the proof. □

Corollary 2.6.4. *Let G be a finite group of order n. Then for any $a \in G$, $\mathrm{ord}(a)$ divides n. In particular, $a^n = e, \ \forall\, a \in G$.*

Proof. Let H be the cyclic subgroup of G generated by a. Since G is a finite group, so is H. Then by Lagrange's theorem 2.6.3, $|H|$ divides $|G| = n$. Since $|H| = \mathrm{ord}(a)$, the result follows. To see the second part, note that if $\mathrm{ord}(a) = k$, then $n = km$, for some $m \in \mathbb{N}$, and so $a^n = (a^k)^m = e^m = e$. □

Corollary 2.6.5. *Any group of prime order is cyclic.*

Proof. Let G be a finite group of order p, where p is a prime number. If $p = 2$, then clearly G is cyclic. Suppose that $p > 2$. Then there is an element $a \in G$ such that $a \neq e$. Since the cyclic subgroup $\in H_a := \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ contains both a and e, we have $|H_a| \geq 2$. Since $|H_a|$ divides $|G| = p$ by Lagrange's theorem, we must have $|H_a| = p$, because p is prime. Then we must have $G = H_a$, and hence G is cyclic. □

Corollary 2.6.6. *Let $n \geq 2$ be an integer. Then for any positive integer a with $\gcd(a, n) = 1$, we have $a^{\phi(n)} \equiv 1$ (mod n), where $\phi(n)$ is the number of elements in the set $\{k \in \mathbb{N} : 1 \leq k < n$ and $\gcd(k, n) = 1\}$.*

Proof. Note that, $U_n := \{[a] \in \mathbb{Z}_n : \gcd(a, n) = 1\}$ is a finite subset of $\mathbb{Z}_n$ containing $\phi(n)$ elements. Since U_n is a group with respect to the multiplication operation modulo n, for any $[a] \in U_n$ we have $[a]^{\phi(n)} = [1]$. In other words, $a^{\phi(n)} \equiv 1 \pmod{n}$. □

Corollary 2.6.7 (Fermat's little theorem)**.** *If $p > 0$ is a prime number, then for any positive integer a with $\gcd(a, p) = 1$, we have $a^{p-1} \equiv 1$ (mod p).*

Proof. Since $\phi(p) = |U_p| = p - 1$, the result follows from the Corollary 2.6.6. □

Exercise 2.6.8. Show that $2^{6000} - 1$ is divisible by 7.

Solution. Since $\gcd(2, 7) = 1$, by Fermat's little theorem we have $2^{7-1} \equiv 1 \pmod 7$. So $[2^6] = [1]$ in $\mathbb{Z}_7$. Then $[2^6]^{1000} = [1]^{1000} = [1^{1000}] = [1]$ in $\mathbb{Z}_7$. Therefore, $2^{6000} \equiv 1 \pmod 7$, and hence $2^{6000} - 1$ is divisible by 7. □

Exercise 2.6.9. Define a relation ρ_R on G by setting

$$(a, b) \in \rho_R \ \text{ if } \ ab^{-1} \in H.$$

(i) Show that ρ_R is an equivalence relation on G.

(ii) Show that the ρ_R-equivalence class of $a \in G$ in G is the subset of G defined by

$$[a]_{\rho_R} := \{b \in G : a^{-1}b \in H\} = \{ha : h \in H\} =: Ha.$$

The subset $Ha \subseteq G$ is called the *right coset* of H in G represented by a.

(iii) Show that if G is abelian then $aH = Ha$, for all $a \in G$.

(iv) Give an example of a group G, two subgroups H and K of G, and an element $b \in G$ such that that $bK \neq Kb$, while $aH = Ha$ holds, for all $a \in G$. (*Hint:* Take $G = S_3$, and

$$H := \{e, (1\ 2\ 3), (1\ 3\ 2)\} \subset S_3 \text{ and } K := \{e, (2\ 3)\} \subset S_3.$$

Note that both H and K are subgroups of S_3. Verify that $aH = Ha$, $\forall\ a \in S_3$, while for $b = (1\ 3\ 2) \in S_3$ we have $bK \neq Kb$.)

(v) Show that H and Ha have the same cardinality, for all $a \in G$.

The set of all distinct right cosets of H in G is denoted by

$$H\backslash G = \{Ha : a \in G\}.$$

Proposition 2.6.10. *Let H be a subgroup of a group G. Then there is a one-to-one correspondence between the set of all left cosets of H in G and the set of all right cosets of H in G. In other words, there is a bijective map $\varphi : G/H \longrightarrow H\backslash G$. Therefore, both the sets G/H and $H\backslash G$ have the same cardinality.*

Proof. Define a map $\varphi : \{aH : a \in G\} \longrightarrow \{Hb : b \in G\}$ by sending $\varphi(aH) = Ha^{-1}$, for all $a \in G$. Note that, $aH = bH$ if and only if $a^{-1}b \in H$ if and only if $a^{-1}(b^{-1})^{-1} \in H$ if and only if $Ha^{-1} = Hb^{-1}$. Therefore, φ is well-defined and injective. To show φ bijective, note that given any $Hb \in \{Hb : b \in G\}$ we have $\varphi(b^{-1}H) = Hb$. Thus, φ is surjective, and hence is a bijective map. □

Definition 2.6.11. Let H be a subgroup of a group G. We define the *index of H in G*, denoted as $[G : H]$, to be the cardinality $|G/H| = |H\backslash G|$. In case, this is a finite number, the index $[G : H]$ is the number of distinct left (and right) cosets of H in G.

Example 2.6.12. The index of $n\mathbb{Z}$ in $\mathbb{Z}$ is n. Indeed, given any two elements $a, b \in \mathbb{Z}$, we have $a - b \in n\mathbb{Z}$ if and only if $a \equiv b \pmod{n}$. Therefore, the left coset of $n\mathbb{Z}$ represented by $a \in \mathbb{Z}$ is precisely the equivalence class

$$[a] := \{b \in \mathbb{Z} : a \equiv b \pmod{n}\}.$$

Since there are exactly n such distinct equivalence classes (see Example 2.1.32), we conclude that the index of $n\mathbb{Z}$ in $\mathbb{Z}$ is $[\mathbb{Z} : n\mathbb{Z}] = n$. We shall explain it later using group homomorphism and quotient group.

Exercise 2.6.13. Let G be a group and H a subgroup of G. Show that the following are equivalent.

(i) $aH = Ha$, for all $a \in G$.

(ii) $aHa^{-1} = H$, for all $a \in G$.

(iii) $aHa^{-1} \subseteq H$, for all $a \in G$.

(iv) $aha^{-1} \in H$, for all $a \in G$ and $h \in H$.

Definition 2.6.14. Let G be a group. A subgroup H of G is said to be *normal* if H satisfy any one (and hence all) of the equivalent conditions in Exercise 2.6.13.

Example 2.6.15. If a group is abelian then all of its subgroups are normal. Indeed, if G is abelian, then for any subgroup H of G, we have $aha^{-1} = aa^{-1}h = eh = h$, for all $h \in H$ and $a \in G$. However, the converse need not be true. For example, all subgroups of the Quaternion group Q_8 are normal but Q_8 is not abelian (verify!).

Remark 2.6.16. Normal subgroup of a normal subgroup need not be normal. To elaborate it, there exists a group G together with a normal subgroup H of G such that H has a subgroup K which is normal subgroup of H, but not a normal subgroup of G.

Let G be a group. Let H be a normal subgroup of G. Then $aH = Ha$, $\forall\ a \in G$, and hence the set of all left cosets of H in G coincides with the set of all right cosets of H in G. Define a binary operation on $G/H = \{gH : g \in G\}$ by

$$(aH, bH) \in G/H \times G/H \longmapsto (ab)H \in G/H. \tag{2.6.17}$$

We now show that this is well-defined. Let $a_1, a_2, b_1, b_2 \in G$ be such that $a_1H = a_2H$ and $b_1H = b_2H$. Then $a_1^{-1}a_2 = h_1$ and $b_1^{-1}b_2 = h_2$, for some $h_1, h_2 \in H$. We want to show that $(a_1b_1)H = (a_2b_2)H$ in G/H. Note that,

$$\begin{aligned}(a_1b_1)^{-1}(a_2b_2) &= b_1^{-1}(a_1^{-1}a_2)b_2 \\ &= b_1^{-1}h_1b_2, \quad \text{for some } h_1 \in H, \\ &= b_1^{-1}b_2h_3, \quad \text{for some } h_3 \in H, \text{ since } Hb_2 = b_2H. \\ &= h_2h_3 \in H, \quad \text{since } b_1^{-1}b_2 = h_2.\end{aligned}$$

Therefore, $(a_1b_1)H = (a_2b_2)H$. Now we show that the set G/H together with the binary operation defined above, is a group. Given any $a, b, c \in G$, we have $(aH \cdot bH) \cdot cH = (ab)H \cdot cH = ((ab)c)H = (a(bc))H = aH \cdot (bc)H = aH \cdot (bH \cdot cH)$. Therefore, the binary operation on G/H is associative. Given any $aH \in G/H$, we have

$$\begin{aligned} aH \cdot eH = (ae)H = aH \\ \text{and} \quad eH \cdot aH = (ea)H = aH.\end{aligned}$$

Therefore, $eH = H \in G/H$ is neutral element for the binary operation on G/H. Given any $aH \in G/H$, note that

$$\begin{aligned} aH \cdot a^{-1}H = (aa^{-1})H = eH \\ \text{and} \quad a^{-1}H \cdot aH = (a^{-1}a)H = eH.\end{aligned}$$

Therefore, G/H is a group, known as the *quotient group of G by H*.

2.7 Group homomorphism

Definition 2.7.1. Let G and H be two groups. A *group homomorphism* from $(G, *)$ into $(H, \star)$ is a map $f : G \to H$ satisfying $f(a * b) = f(a) \star f(b)$, for all $a, b \in G$.

Example 2.7.2. (i) For any group G, the constant map $e : G \to G$, which sends all points of G to the neutral element $e \in G$, is a group homomorphism, called the *trivial group homomorphism* of G.

(ii) Let H be a subgroup of a group G. Then the set theoretic inclusion map $H \hookrightarrow G$ is a group homomorphism. In particular, for any group G, the identity map

$$\mathrm{Id}_G : G \to G, \ \ a \mapsto a$$

is a group homomorphism.

(iii) Fix an integer m, and define a function

$$\varphi_m : \mathbb{Z} \longrightarrow \mathbb{Z}, \;\; n \longmapsto mn, \; \forall\, n \in \mathbb{Z}.$$

Then $\varphi_m(n_1 + n_2) = m(n_1 + n_2) = mn_1 + mn_2 = \varphi_m(n_1) + \varphi_m(n_2)$, for all $n_1, n_2 \in \mathbb{Z}$. Therefore, φ_m is a group homomorphism. Note that, φ_m is always injective, and it is surjective only for $m \in \{1, -1\}$.

(iv) Let $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$, and consider the exponential map

$$f : \mathbb{R} \longrightarrow \mathbb{R}^*, \;\; x \longmapsto e^x, \;\; \forall\, x \in \mathbb{R}.$$

Since $f(a + b) = e^{a+b} = e^a \cdot e^b = f(a) \cdot f(b)$, for all $a, b \in \mathbb{R}$, the map f is a group homomorphism from $(\mathbb{R}, +)$ into $(\mathbb{R}^*, \cdot)$. Verify that f is injective.

(v) Let

$$\phi : \mathbb{R} \longrightarrow \mathrm{SL}_2(\mathbb{R}), \;\; a \longmapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \;\; \forall\, a \in \mathbb{R}.$$

Verify that ϕ is an injective group homomorphism from the additive group $\mathbb{R}$ into the multiplicative group $\mathrm{SL}_2(\mathbb{R})$.

(vi) Fix an integer $n \geq 2$, and consider the map

$$\psi : \mathbb{Z} \longrightarrow \mathbb{Z}_n, \;\; a \longmapsto [a], \;\; \forall\, a \in \mathbb{Z}.$$

Verify that ψ is a surjective group homomorphism.

Exercise 2.7.3. For each integer $n \geq 1$, let $J_n := \{k \in \mathbb{Z} : 1 \leq k \leq n\}$. For each $\sigma \in S_n$, consider the map $\widetilde{\sigma} : J_{n+1} \to J_{n+1}$ defined by

$$\widetilde{\sigma}(k) = \begin{cases} \sigma(k), & \text{if} \quad 1 \leq k \leq n, \\ n+1, & \text{if} \quad k = n+1. \end{cases}$$

Note that, $\widetilde{\sigma}$ is a bijective map, and hence is an element of S_{n+1}. Show that the map

$$f : S_n \to S_{n+1}, \;\; \sigma \mapsto \widetilde{\sigma},$$

is an injective group homomorphism. Thus, we can identify S_n as a subgroup of S_{n+1}.

Proposition 2.7.4. *Let $f : G \to H$ be a group homomorphism. Let $e_G \in G$ and $e_H \in H$ be the neutral elements of G and H, respectively. Then we have the following.*

(i) $f(e_G) = e_H$.

(ii) $f(a^{-1}) = (f(a))^{-1}$, *for all* $a \in G$.

(iii) If $\mathrm{ord}(a) < \infty$, *then* $\mathrm{ord}(f(a)) \mid \mathrm{ord}(a)$.

Proof. (i) Since $f(e_G)f(e_G) = f(e_G \cdot e_G) = f(e_G) = f(e_G) \cdot e_H$, applying cancellation law we have $f(e_G) = e_H$. The second statement follows immediately.

(ii) Since f is a group homomorphism, for any $a \in G$, we have

$$\begin{aligned} f(a)f(a^{-1}) = f(a \cdot a^{-1}) = f(e_G) = e_H \\ \text{and } f(a^{-1})f(a) = f(a^{-1} \cdot a) = f(e_G) = e_H\,, \end{aligned}$$

and hence $f(a^{-1}) = (f(a))^{-1}$.

(iii) Let $n := \mathrm{ord}(a) < \infty$. Since $f(a)^n = f(a^n) = f(e_G) = e_H$, it follows from Exercise 2.2.23 (i) that $\mathrm{ord}(f(a)) \mid n$.

□

Exercise 2.7.5. Let G and H be two groups. Show that there is a unique constant group homomorphism from G to H.

Proposition 2.7.6. *Let $f : G \to H$ be a group homomorphism.*

(i) For any subgroup G' of G, its image $f(G') := \{f(a) : a \in G'\}$ is a subgroup of H. Moreover, if G' is commutative, so is $f(G')$.

(ii) For any subgroup H' of H, its inverse image $f^{-1}(H') := \{a \in G : f(a) \in H'\}$ is a subgroup of G. Moreover, if H' is a normal subgroup, so is $f^{-1}(H')$.

Proof. (i) Clearly, $f(G') \neq \emptyset$ as $e \in G'$. For $h_1, h_2 \in f(G')$, we have $h_1 = f(a_1)$ and $h_2 = f(a_2)$, for some $a_1, a_2 \in G'$. Since $a_1 a_2^{-1} \in G'$, we have $h_1 h_2^{-1} = f(a_1)f(a_2)^{-1} = f(a_1 a_2^{-1}) \in f(G')$. If G' is commutative, we have $f(a)f(b) = f(ab) = f(ba) = f(b)f(a)$, for all $a, b \in G'$. Hence the result follows.

(ii) Let $e_G \in G$ and $e_H \in H$ be the neutral elements of G and H, respectively. Since $f(e_G) = e_H$ by Proposition 2.7.4 (i), we have $e_G \in f^{-1}(H')$. Since H' is a subgroup of H, for any $a, b \in f^{-1}(H')$ we have $f(ab^{-1}) = f(a)f(b)^{-1} \in H'$, and hence $ab^{-1} \in f^{-1}(H')$. Thus $f^{-1}(H')$ is a subgroup of G. Suppose that H' is normal. Then for any $a \in G$ and $b \in f^{-1}(H')$, we have $f(aba^{-1}) = f(a)f(b)f(a)^{-1} \in H'$, and hence $aba^{-1} \in f^{-1}(H')$.

□

Proposition 2.7.7. *Composition of group homomorphisms is a group homomorphism.*

Proof. Let $f : G_1 \to G_2$ and $g : G_2 \to G_3$ be two group homomorphisms. Since $(g \circ f)(ab) = g(f(ab)) = g(f(a)f(b)) = g(f(a))g(f(b)) = (g \circ f)(a)(g \circ f)(b)$, for all $a, b \in G_1$, the result follows. □

Definition 2.7.8. Let $f : G \to H$ be a group homomorphism. We say that

(i) f is *trivial* if $f(a) = e_H$, for all $a \in G$.

(ii) f is a *monomorphism* if f is injective.

(iii) f is an *epimorphism* if f is surjective, and

(iv) f is an *isomorphism* if f is bijective. In that case, we say that G and *isomorphic* to H, and express it as $G \cong H$.

The next two exercises reflects abstract properties of monomorphisms and epimorphisms.

Exercise 2.7.9. Let $f : G \to H$ be a group homomorphism. Then the following are equivalent.

(i) f is a monomorphism.

(ii) There is a group homomorphism $g : H \to G$ such that $g \circ f = \mathrm{Id}_G$.

(iii) Given any group K and group homomorphisms $\phi, \psi : K \to G$ with $f \circ \phi = f \circ \psi$, we have $\phi = \psi$.

(iv) Given any group K and a group homomorphisms $\phi : K \to G$, if $f \circ \phi = f$ then ϕ is trivial.

Exercise 2.7.10. Let $f : G \to H$ be a group homomorphism. Then the following are equivalent.

(i) f is an epimorphism.

(ii) There is a group homomorphism $h : G \to H$ such that $f \circ h = \mathrm{Id}_H$.

(iii) Given any group Q and group homomorphisms $\phi, \psi : H \to Q$ with $\phi \circ f = \psi \circ f$, we have $\phi = \psi$.

(iv) Given any group Q and a group homomorphism $\phi : H \to Q$ with $\phi \circ f = f$, we have ϕ is trivial.

Corollary 2.7.11. *Being isomorphic groups is an equivalence relation.*

Proof. Given any group G, the identity map $\mathrm{Id}_G : G \to G$ given by $\mathrm{Id}_G(a) = a$, for all $a \in G$, is an isomorphism of groups. Therefore, being isomorphic is a reflexive relation. If $f : G \to H$ is an isomorphism of groups, then its inverse map $f^{-1} : H \to G$ is also a group homomorphism, and hence is an isomorphism because it is bijective. Therefore, being isomorphic groups is a symmetric relation. If $f : G \to H$ and $g : H \to K$ be isomorphism of groups. Then the composite map $g \circ f : G \to K$ is a group homomorphism, which is an isomorphism of groups. Therefore, being isomorphic groups is a transitive relation. Hence the result follows. □

The *kernel* of a group homomorphism $f : G \to H$ is the subset

$$\mathrm{Ker}(f) := \{a \in G \,:\, f(a) = e_H\} \subseteq G.$$

Since $f(e_G) = e_H$ by Proposition 2.7.4 (i), we have $e_G \in \mathrm{Ker}(f)$. Therefore, $\mathrm{Ker}(f)$ is a non-empty subset of G. Given any two elements $a, b \in \mathrm{Ker}(f)$ we have $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = e_H \cdot e_H^{-1} = e_H$. Therefore, $\mathrm{Ker}(f)$ is a subgroup of G.

Example 2.7.12. (i) Fix an integer n and consider the homomorphism

$$f : \mathbb{Z} \to \mathbb{Z}_n, \;\; a \mapsto [a].$$

Then $\mathrm{Ker}(f) = \{a \in \mathbb{Z} : n \text{ divides } a\} = n\mathbb{Z}$.

(ii) Let $S^1 := \{z \in \mathbb{C} : |z| = 1\}$. Consider the homomorphism

$$f : \mathbb{R} \longrightarrow S^1, \;\; t \mapsto e^{2\pi\sqrt{-1}\,t}.$$

Then $\mathrm{Ker}(f) = \{t \in \mathbb{R} : e^{2\pi\sqrt{-1}\,t} = 1\} = \mathbb{Z}$.

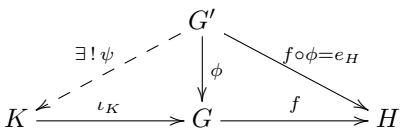
The following lemma shows that the kernel of a group homomorphism can be uniquely determined purely using its universal property. Interesting fact to note is that this description of kernel of a group homomorphism use only arrows and not any points.

Proposition 2.7.13. *Let $f : G \to H$ be a group homomorphism. Then there is a unique subgroup K of G satisfying the following properties.*

(K1) $f \circ \iota_K$ is trivial, where $\iota_K : K \hookrightarrow G$ is the inclusion map, and

(K2) given any group homomorphism $\phi : G' \to G$ with $f \circ \phi$ trivial, there is a unique group homomorphism $\psi : G' \to K$ such that $\iota_K \circ \psi = \phi$.

(2.7.14)



Proof. We first show the uniqueness of K. Let $\iota_{K'} : K' \hookrightarrow G$ be any subgroup of G satisfying (K1) and (K2). Since the homomorphism $f \circ \iota_{K'}$ is trivial, applying (K2) for K we have a unique group homomorphism $\eta : K' \to K$ such that $\iota_{K'} = \iota_K \circ \eta$. Similarly replacing (K, ι_K) with $(K', \iota_{K'})$, and (G', ϕ) with (K, ι_K) in the above diagram (2.7.14), we get a unique group homomorphism $\eta' : K \to K'$ such that $\iota_K = \iota_{K'} \circ \eta'$. Now replace (G', ϕ) with (K, ι_K) in the above diagram 2.7.14. Since both the group homomorphisms $\mathrm{Id}_K : K \to K$ and $\eta \circ \eta' : K \to K$ satisfies $\iota_K \circ (\eta \circ \eta') = \iota_K$ and $\iota_K \circ \mathrm{Id}_K = \iota_K$, by uniqueness assumption in (K2), we have $\eta \circ \eta' = \mathrm{Id}_K$. Similarly, we have $\eta' \circ \eta = \mathrm{Id}_{K'}$. Therefore, both $\eta' : K \to K'$ and $\eta : K' \to K$ are isomorphisms. Since both $\iota_K : K \hookrightarrow G$ and $\iota_{K'} : K' \hookrightarrow G$ are inclusion maps, and $\iota_K \circ \eta' = \iota_{K'}$, we must have η' is an inclusion map, and hence $K \subseteq K'$. Similarly, we have $K' \subseteq K$, and hence $K = K'$.

To prove existence, take $K = \mathrm{Ker}(f)$ and $\iota_K : K \hookrightarrow G$ the inclusion map. Clearly, $f \circ \iota_K$ is trivial. For any group homomorphism $\phi : G' \to G$ with $f \circ \phi$ trivial, we have $\phi(a) \in K$, for all $a \in G'$. Thus the image of ϕ lands inside K and hence we have a group homomorphism

$$\psi : G' \to K, \;\; a \mapsto \phi(a)$$

such that $\iota_K \circ \psi = \phi$ as required. □

Proposition 2.7.15. *A group homomorphism $f : G \to H$ is injective if and only if $\mathrm{Ker}(f)$ is trivial.*

Proof. If $\mathrm{Ker}(f) \neq \{e\}$, clearly f is not injective. Conversely, suppose that $\mathrm{Ker}(f) = \{e\}$. If $f(a) = f(b)$, for some $a, b \in G$ with $a \neq b$, then $ab^{-1} \neq e$ and $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = e_H$, which contradicts our assumption that $\mathrm{Ker}(f) = \{e\}$. This completes the proof. □

Proposition 2.7.16. *For any group homomorphism $f : G \to H$, its kernel $\mathrm{Ker}(f)$ is a normal subgroup of G.*

Proof. For any $a \in G$ and $b \in \mathrm{Ker}(f)$, we have $f(aba^{-1}) = f(a)f(b)f(a^{-1}) = f(a)e_H f(a)^{-1} = e_H$, and hence $aba^{-1} \in \mathrm{Ker}(f)$. Therefore, $\mathrm{Ker}(f)$ is a normal subgroup of G. □

Let G be a group and let H be a normal subgroup of G. Let G/H be the quotient group of G by H. Then there is a natural surjective map

$$\pi : G \to G/H$$

defined by

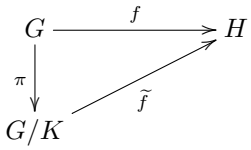
$$\pi(a) = aH, \;\; \forall\, a \in G.$$

Clearly π is surjective, and given any $a, b \in G$, we have

$$\pi(ab) = (ab)H = aH \cdot bH = \pi(a)\pi(b).$$

Therefore, π is a surjective group homomorphism.

Theorem 2.7.17. *Let $f : G \to H$ be a group homomorphism. Let K be a normal subgroup of G such that $K \subseteq \mathrm{Ker}(f)$. Then there is a unique group homomorphism $\widetilde{f} : G/K \longrightarrow H$ such that $\widetilde{f} \circ \pi = f$, where $\pi : G \to G/K$ is the quotient homomorphism.*



Furthermore, $\widetilde{f}$ is injective if and only if $K = \mathrm{Ker}(f)$.

Proof. Define a map $\widetilde{f} : G/K \to H$ by

$$\widetilde{f}(gK) = f(g), \ \ \forall\, g \in G.$$

If $g_1K = g_2K$, for some $g_1, g_2 \in G$, then $g_1^{-1}g_2 \in K \subseteq \mathrm{Ker}(f)$, and so

$$f(g_1)[f(g_2)]^{-1} = f(g_1)f(g_2^{-1}) = f(g_1^{-1}g_2) = e_H.$$

Therefore, $f(g_1) = f(g_2)$, and hence $\widetilde{f}$ is well-defined. Since for any $g_1, g_2 \in G$, we have

$$\begin{aligned}\widetilde{f}(g_1K \cdot g_2K) &= \widetilde{f}\big((g_1g_2)K\big)\\ &= f(g_1g_2) = f(g_1)f(g_2)\\ &= \widetilde{f}(g_1K)\widetilde{f}(g_2K),\end{aligned}$$

$\widetilde{f}$ is a group homomorphism. Clearly $(\widetilde{f} \circ \pi)(a) = \widetilde{f}(aK) = f(a), \ \ \forall\, a \in G$, and so $\widetilde{f} \circ \pi = f$.

Since $\mathrm{Ker}(\widetilde{f}) = \{gK : f(g) = e_H\} = \{gK : g \in \mathrm{Ker}(f)\}$, we see that $\mathrm{Ker}(\widetilde{f})$ is trivial (meaning that, it is a trivial subgroup) if and only if $gK = K, \ \forall\, g \in \mathrm{Ker}(f)$. This is equivalent to say that, $g \in K, \ \forall\, g \in \mathrm{Ker}(f)$, i.e., $\mathrm{Ker}(f) \subseteq K$. Since $K \subseteq \mathrm{Ker}(f)$ by assumption, it follows from Proposition 2.7.15 that $\widetilde{f}$ is injective if and only if $K = \mathrm{Ker}(f)$. □

As an immediate corollary, we have the following.

Corollary 2.7.18 (First Isomorphism Theorem)**.** *Let $f : G \to H$ be a surjective homomorphism of groups. Then f induces a natural isomorphism of groups $\widetilde{f} : G/\mathrm{Ker}(f) \to H$.*

Proof. Note that $\mathrm{Ker}(f)$ is a normal subgroup of G. It follows from Theorem 2.7.17 that the group homomorphism $\widetilde{f} : G/\mathrm{Ker}(f) \to H$ induced by f is injective. Since f is surjective and $\widetilde{f} \circ \pi = f$, where $\pi : G \to G/\mathrm{Ker}(f)$ is the natural surjective homomorphism, it follows that $\widetilde{f}$ is surjective. Therefore, $\widetilde{f}$ is a bijective group homomorphism, and hence is an isomorphism of groups. □

Proposition 2.7.19. *Any infinite cyclic group is isomorphic to $\mathbb{Z}$.*

Proof. Let $G = \langle a \rangle$ be an infinite cyclic group. Define a map $f : Z \to G$ by $f(n) = a^n$, for all $n \in \mathbb{Z}$. Since $f(n+m) = a^{n+m} = a^n a^m = f(n)f(m)$, for all $m, n \in \mathbb{Z}$, f is a group homomorphism. Since G is infinite, we have $a^n \neq e$, for all $n \in \mathbb{Z}\backslash\{0\}$. Therefore, $\mathrm{Ker}(f) = \{e\}$, and so f is injective. Clearly f is surjective, and hence is an isomorphism. □

Proposition 2.7.20. *The group $\mathbb{Z}_n$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.*

Proof. Let $f : \mathbb{Z} \to \mathbb{Z}_n$ be the map defined by

$$f(k) = [k], \ \forall\, k \in \mathbb{Z}.$$

Since

$$f(k_1 + k_2) = [k_1 + k_2] = [k_1] + [k_2] = f(k_1) + f(k_2), \ \forall\, k_1, k_2 \in \mathbb{Z},$$

we see that f is a group homomorphism. Clearly f is surjective (verify!). Note that $\mathrm{Ker}(f) = \{k \in \mathbb{Z} : [k] = [0]\} = n\mathbb{Z}$. Then by first isomorphism theorem we have $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. □

Proposition 2.7.21. *Any finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$.*

Proof. Let G be a finite cyclic group of order n. Then there exists $a \in G$ such that $\langle a \rangle = \{a^k : k \in \mathbb{Z}\} = G$. Define a map $f : \mathbb{Z} \to G$ by

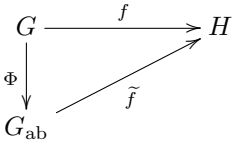
$$f(k) = a^k, \ \forall\, k \in \mathbb{Z}.$$

Since

$$f(k_1+k_2)=a^{k_1+k_2}=a^{k_1}a^{k_2}=f(k_1)f(k_2),\ \ \forall\, k_1,k_2\in\mathbb{Z},$$

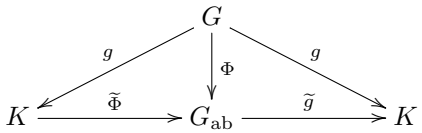
f is a group homomorphism. Clearly f is surjective because every element of G is of the form a^k, for some $k\in\mathbb{Z}$. Then by first isomorphism theorem G is isomorphic to $\mathbb{Z}/\mathrm{Ker}(f)$. Note that, $\mathrm{Ker}(f)=\{k\in\mathbb{Z}: a^k=e\}$. Since G is a cyclic group of order n generated by a, we have $\mathrm{ord}(a)=n$ (see Corollary 2.3.11). Then we have $\mathrm{Ker}(f)=\{k\in\mathbb{Z}: a^k=e\}=n\mathbb{Z}$. Therefore, $G\cong\mathbb{Z}/n\mathbb{Z}$. Since $\mathbb{Z}/n\mathbb{Z}\cong\mathbb{Z}_n$ by Theorem 2.7.20, we have $G\cong\mathbb{Z}_n$. □

Theorem 2.7.22 (Abelianization)**.** *Let G be a group. Then upto isomorphism there exists a unique pair (G_{ab},Φ) consisting of an abelian group G_{ab} and a surjective group homomorphism $\Phi: G\to G_{\mathrm{ab}}$ satisfying the following universal property: given any abelain group H and a group homomorphism $f: G\to H$, there exists a unique group homomorphism $\widetilde{f}: G_{\mathrm{ab}}\to H$ such that $\widetilde{f}\circ\Phi=f$.*



The group G_{ab} is known as the maximal abelian quotient or the abelianization of G.

Proof. Uniqueness: First we prove uniqueness of the pair (G_{ab},Φ) upto unique isomorphism of groups. Suppose that (K,g) be another such pair consisting of an abelian group K and a surjective group homomorphism $g: G\to K$ such that the pair (K,g) satisfies the above universal property. Taking $(H,f)=(G_{\mathrm{ab}},\Phi)$ we find a unique group homomorphism $\widetilde{\Phi}: K\to G_{\mathrm{ab}}$ such that $\widetilde{\Phi}\circ g=\Phi$.



Applying universal property of (G_{ab},Φ) with $(H,f)=(K,g)$, we have a unique group homomorphism $\widetilde{g}: G_{\mathrm{ab}}\to K$ such that $\widetilde{g}\circ\Phi=g$. Since the composite map $\widetilde{g}\circ\widetilde{\Phi}: K\to K$ is a group homomorphism, by the universal property of the pair (K,g) we have $\widetilde{g}\circ\widetilde{\Phi}=\mathrm{Id}_K$, where $\mathrm{Id}_K: K\to K$ is the identity map of K. Similarly, we have $\widetilde{\Phi}\circ\widetilde{g}=\mathrm{Id}_{G_{\mathrm{ab}}}$. Therefore, both $\widetilde{g}: K\to G_{\mathrm{ab}}$ and $\widetilde{\Phi}: G_{\mathrm{ab}}\to K$ are isomorphism of groups. Since both $\widetilde{\Phi}$ and $\widetilde{g}$ are unique and $\widetilde{\Phi}\circ g=\Phi$ and $\widetilde{g}\circ\Phi=g$, we conclude that the pair (K,g) is uniquely isomorphic to (G_{ab},Φ).

Existence: To prove existence of the pair (G_{ab},Φ), consider the elements of G of the form

$$[a,b]:=aba^{-1}b^{-1},$$

where $a,b\in G$, called *commutators* in G. Clearly $[a,b]=e$ if G is abelian. Let

$$[G,G]:=\langle aba^{-1}b^{-1}: a,b\in G\rangle$$

be the subgroup of G generated by all commutators of elements of G. The subgroup $[G,G]$ is known as the *commutator subgroup* or the *derived subgroup* of G. Since

$$ghg^{-1}=ghg^{-1}h^{-1}h=[g,h]h,\ \ \forall\, g,h\in G,$$

taking $h\in[G,G]$ we see that $[G,G]$ is a normal subgroup of G. Let $G_{\mathrm{ab}}:=G/[G,G]$ be the associated quotient group, and let $\Phi: G\to G_{\mathrm{ab}}$ be the natural quotient map which sends $a\in G$ to the coset $a[G,G]\in G/[G,G]=G_{\mathrm{ab}}$. Let us denote by $\overline{a}$ the image of $a\in G$ in $G/[G,G]$ under

the quotient map $\Phi : G \to G/[G,G]$. Since

$$(ab)(ba)^{-1} = aba^{-1}b^{-1} \in [G,G], \ \ \forall\, a, b \in G,$$

we have $\overline{a}\overline{b} = \overline{b}\overline{a}$ in $G/[G,G]$. Therefore, $G/[G,G]$ is commutative. If $f : G \to H$ is a group homomorphism, then

$$f([a,b]) = f(aba^{-1}b^{-1}) = [f(a), f(b)], \ \forall\, a, b \in G.$$

Now suppose that H is abelian. Then for any $a, b \in G$, we have $[f(a), f(b)] = e$, and so $[a,b] \in \mathrm{Ker}(f)$. Therefore, $[G,G] \subseteq \mathrm{Ker}(f)$. Consequently, there is a unique homomorphism $\widetilde{f} : G/[G,G] \to H$ such that $\widetilde{f} \circ \Phi = f$. This completes the proof of existence part. □

Proposition 2.7.23. *Let A be a finite set containing n elements. Fix an indexing $\alpha : J_n \to A$ of A. Then the natural map $\Phi : S_A \to S_{J_n}$ defined by sending a permutation $\sigma \in S_A$ to $\Phi(\sigma) := \alpha^{-1} \circ \sigma \circ \alpha : J_n \to J_n$ is an isomorphism of groups.*

Proof. Given a permutation $\sigma : A \to A$ on A, the composite map $\widetilde{\sigma} := \alpha^{-1} \circ \sigma \circ \alpha$,

$$J_n \xrightarrow{\alpha} A \xrightarrow{\sigma} A \xrightarrow{\alpha^{-1}} J_n,$$

is bijective by Exercise 2.1.13, and hence is a permutation on J_n.

For any set A, we denote by S_A the set of all permutations of A. If A is a finite set containing n elements, the above construction gives a map

$$\Phi : S_A \to S_{J_n}$$

defined by $\Phi(\sigma) = \widetilde{\sigma}$, for all $\sigma \in S_A$. If $\Phi(\sigma) = \Phi(\tau)$, for some $\sigma, \tau \in S_A$, then $\alpha^{-1} \circ \sigma \circ \alpha = \alpha^{-1} \circ \tau \circ \alpha$. Composing α from the left and α^{-1} from the right, we find that $\sigma = \tau$. So the map Φ is injective. To see Φ is surjective, note that given any $\tau \in S_{J_n}$, the composite map

$$\widehat{\tau} : A \xrightarrow{\alpha^{-1}} J_n \xrightarrow{\tau} J_n \xrightarrow{\alpha} A$$

is a permutation on A by Exercise 2.1.13, and hence $\widehat{\tau} := \alpha \circ \tau \circ \alpha^{-1} \in S_A$. Then $\Phi(\widehat{\tau}) = \alpha^{-1} \circ (\alpha \circ \tau \circ \alpha^{-1}) \circ \alpha = \tau$, and hence Φ is surjective. Therefore, Φ is a bijective map. Furthermore, given any $\sigma_1, \sigma_2 \in S_A$, we have

$$\begin{aligned}
\Phi(\sigma_1 \circ \sigma_2) &= \alpha^{-1} \circ (\sigma_1 \circ \sigma_2) \circ \alpha \\
&= \alpha^{-1} \circ \big(\sigma_1 \circ (\alpha \circ \alpha^{-1}) \circ \sigma_2\big) \circ \alpha \\
&= (\alpha^{-1} \circ \sigma_1 \circ \alpha) \circ (\alpha^{-1} \circ \sigma_2 \circ \alpha) \\
&= \Phi(\sigma_1) \circ \Phi(\sigma_2)
\end{aligned}$$

Therefore, Φ is a group homomorphism, and so is a group isomorphism. □

Remark 2.7.24. Study of permutation on a finite set containing n elements is the same as study of permutations on J_n.

Theorem 2.7.25 (Second Isomorphism Theorem)**.** *Let*

2.8 Group Action

Let G be a group.

Definition 2.8.1. A *G-action* on a non-empty set X is a map

$$\sigma : G \times X \to X$$

satisfying the following conditions:

(i) $\sigma(e, x) = x, \ \forall\, x \in X$, and

(ii) $\sigma(b, \sigma(a, x)) = \sigma(ba, x), \ \forall\, a, b \in G, \ x \in X.$

2.8.1 Conjugacy classes

2.8.2 Orbits and stabilizers

2.8.3 Class equations

2.9 Simple Groups

2.9.1 Simplicity of A_n, $n \geq 5$

2.10 Sylow's Theorems

2.10.1 Finitely Generated Abelian Groups