Algebra I: Group Theory

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: September 11, 2023 at 1:16pm (IST).
Available at: https://arjunpaul29.github.io/home/notes/Algebra-I.pdf

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. $\square$

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

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

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 $a \le b$ and $b \le a$. 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 " $\le$ " is a total order relation on $\mathbb{N}$, and hence $(\mathbb{N}, \le)$ 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 $n \in \mathbb{N}$, $J_n := \{k \in \mathbb{N} : k \le n\} \subseteq T$ 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

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

holds. Consider the set

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

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 $J_{s(n)} = \{k \in \mathbb{N} : k \le s(n)\} \subseteq T$. Then by the condition (b') we have $s(s(n)) \in T$, and hence $P_{s(n)}$ holds. Therefore, P_k holds, $\forall\, k \le s(n)$, 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. $\square$

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

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

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 $d = a_0 m + b_0 n$, 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 $r \mid (a_0 m + b_0 n)$ 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 $am + bn = x = qd + r = q(a_0 m + b_0 n) + r$ 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:

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

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:

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

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 component-wise 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:

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

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 $C(A) := \{f : A \to \mathbb{R} \mid f \text{ is continuous}\}$. 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

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

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

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

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) $A = \bigcup\limits_{\alpha \in \Lambda} A_\alpha$.

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 $A = \bigcup\limits_{a \in A} [a]_\rho$. 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

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

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

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

The set $A \bigtriangleup B$ is known as the *symmetric difference* of A and B. Show that $\big(\mathcal{P}(X), \bigtriangleup\big)$ 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).

Exercise 2.1.34 (Direct product of two groups)**.** Let $(A, *)$ and $(B, \star)$ be two groups. Show that the Cartesian product $G_1 \times G_2$ is a group with respect to the binary operation on it defined by

$$(a_1, b_1)(a_2, b_2) := (a_1 * a_2,\ b_1 \star b_2),\ \forall\, (a_1, b_1), (a_2, b_2) \in A \times B.$$

The group $A \times B$ defined above is called the *direct product* of A with B.

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. $\square$

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. $\square$

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 $n \in \mathbb{N}$.

Exercise 2.2.13 (Centralizer)**.** Let G be a group. Given an element $a \in G$ show that the subset

$$C_G(a) := \{b \in G : ab = ba\}$$

is a subgroup of G, called the *centralizer of* a in G. Show that $Z(G) = \bigcap_{a\in G} C_G(a)$.

Lemma 2.2.14. *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 2.2.15. *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 2.2.14, $\langle S \rangle := \bigcap_{H\in\mathscr{C}_S} H$ 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 2.2.16. Recall Exercise 2.2.2, and find the subgroup $2\mathbb{Z} \cap 3\mathbb{Z}$ of $\mathbb{Z}$.

Exercise 2.2.17. Is $2\mathbb{Z} \cup 3\mathbb{Z}$ a subgroup of $\mathbb{Z}$? Justify your answer.

Exercise 2.2.18. Show that a group cannot be written as a union of its two proper subgroups.

Definition 2.2.19. 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 2.2.20. Let G be a group. Find the subgroup of G generated by the empty subset of G.

Proposition 2.2.21. *Let G be a group, and let S be a non-empty subset of G. Then*

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

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 $a_i, b_j \in S$, $e_i, f_j \in \{1, -1\}$, $1 \leq i \leq n$, $1 \leq j \leq m$, 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 2.2.15, 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, $K \subseteq \bigcap_{H\in\mathscr{C}_S} H = \langle S \rangle$. □

Definition 2.2.22. A group G is said to be *finitely generated* if there exists a finite subset $S \subseteq G$ such that the subgroup generated by S is equal to G, i.e., $\langle G \rangle = G$.

Example 2.2.23. (i) Any finite group is finitely generated.

(ii) The additive group $(\mathbb{Z}, +)$ is finitely generated.

Exercise 2.2.24. Let G and H be finitely generated groups. Verify if the direct product $G \times H$ of G and H, as defined in Exercise 2.1.34, is finitely generated.

Example 2.2.25. 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 2.2.26. 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 $S_a := \{n \in \mathbb{Z} : n \geq 1 \text{ and } a^n = e\}$, 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 2.2.27. 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 2.2.28. 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 $\mathrm{ord}(a) \,|\, m$.

(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 2.2.29. 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 $\mathrm{ord}(ab) = \mathrm{ord}(a)\,\mathrm{ord}(b)$.

Remark 2.2.30. If we remove the assumption that $ab = ba$ from the above Exercise 2.2.29 we can say absolutely nothing about the order of the product ab. In fact, 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 $\mathrm{ord}(ab) = r$. The proof of this surprising fact requires some advanced techniques, and may appear at the end of this course.

Exercise 2.2.31. Let G be an abelian group. Let $H := \{a \in G : \mathrm{ord}(a) \text{ is finite}\}$. Show that H is a subgroup of G.

Exercise 2.2.32. Show that $(\mathbb{Q}, +)$ is not a finitely generated group.

Exercise 2.2.33. Find two elements σ and τ of S_3 that generates it.

Exercise 2.2.34 (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. $\square$

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 $H = \langle\, a^m \,\rangle$. $\square$

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 $n \in \mathbb{Z}\setminus\{0\}$. 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.

Exercise 2.3.19. Show that a non-commutative group always has a non-trivial proper subgroup.

Exercise 2.3.20. Show that a group having at most two non-trivial subgroups is cyclic.

Exercise 2.3.21. Let G be a finite group having exactly one non-trivial subgroup. Show that $|G| = p^2$, for some prime number p.

Exercise 2.3.22. Give examples of infinite abelian groups having

(i) exactly one element of finite order;

(ii) all of its non-trivial elements have order 2.

2.4 Product of subgroups

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 $(hk)^{-1} = h_1k_1$, 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 $h_1k_1, h_2k_2 \in HK$ 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 $k_2^{-1}h_2^{-1} = h_3k_3$. Again $k_1h_3 \in KH = HK$ implies there exists $h_4 \in H$ and $k_4 \in K$ such that $k_1h_3 = h_4k_4$. Now

$$\begin{aligned}
(h_1k_1)(h_2k_2)^{-1} &= h_1k_1k_2^{-1}h_2^{-1} \\
&= h_1k_1h_3k_3 \\
&= h_1h_4k_4k_3 \in HK.
\end{aligned}$$

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 $\aleph_0$.

Lemma 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 $HK = \{h_ik_j : i \in J_n,\ j \in J_m\}$. 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_ik_j repeats in the collection $\mathscr{C} := \{h_ik_j : (i, j) \in J_n \times J_m\}$. Fix $(i, j) \in J_n \times J_m$. If $h_ik_j = h_pk_q$, for some $(p, q) \in J_n \times J_m$, then $t := h_p^{-1}h_i = k_qk_j^{-1} \in H \cap K$. So any element $h_pk_q \in \mathscr{C}$, which coincides with h_ik_j is of the form $(h_it^{-1})(tk_j)$, for some $t \in H \cap K$. Conversely, for any $t \in H \cap K$, we have $(h_it^{-1})(tk_j) = h_i(t^{-1}t)k_j = h_iek_j = h_ik_j$. Therefore, the element h_ik_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

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

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

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

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

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

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

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

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 an expression of the form

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

where $k_1, \ldots, k_r$ are all distinct. By re-indexing, if required, we can find a partition of $\{k_1, \ldots, k_r\}$ into disjoint subsets, say

$$\{k_1, \ldots, k_r\} = \bigcup_{i=1}^{m} \{k_{i,1}, \ldots, k_{i,r_i}\}$$

with $m \geq 1$, $2 \leq r_i \leq r$, for all $i \in \{1, \ldots, m\}$, and $r_1 + \cdots + r_m = r$, such that for all $i \in \{1, \ldots, m\}$ we have

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

Then σ can be expressed as

$$\sigma = \begin{pmatrix} k_{1,1} & \cdots & k_{1,r_1-1} & k_{1,r_1} & \cdots\cdots & k_{m,1} & \cdots & k_{m,r_m} & k_{m,r_m-1} \\ k_{1,2} & \cdots & k_{1,r_1} & k_{1,1} & \cdots\cdots & k_{m,2} & \cdots & k_{m,r_m} & k_{m,1} \end{pmatrix}.$$

When $m = 1$ in the above notation, σ can be expressed as

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

Such a permutation is called a cycle.

Definition 2.5.6. An element $\sigma \in S_n$ is called a *r-cycle* or a *cycle of length r* if there exists distinct r elements, say $k_1, \ldots, k_r \in J_n := \{1, \ldots, n\}$ such that $\sigma(k) = k$, for all $k \in J_n \setminus \{k_1, \ldots, k_r\}$ and

$$\sigma(k_i) = \begin{cases} k_{i+1} & \text{if} \quad i \in \{1, \ldots, r-1\}, \\ k_1 & \text{if} \quad i = r. \end{cases}$$

In this case, σ is expressed as $\sigma = (k_1 \ k_2 \ \cdots \ k_r)$. A 2-cycle is called a *transposition*.

Remark 2.5.7. 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 2.5.8. 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 2.5.9. *Let $\sigma = (k_1\ \ k_2\ \ \cdots\ \ k_r) \in S_n$ be a r-cycle. Then for any $\tau \in S_n$ we have*

$$\tau\sigma\tau^{-1} = (\tau(k_1)\ \ \tau(k_2)\ \ \cdots\ \ \tau(k_r)).$$

Proof. Note that we have

$$\begin{aligned} &(\tau\sigma\tau^{-1})(\tau(k_i)) = \tau(\sigma(k_i)) = \tau(k_{i+1}),\ \ \forall\, i \in \{1, \ldots, r-1\}, \\ \text{and}\quad &(\tau\sigma\tau^{-1})(\tau(k_r)) = \tau(\sigma(k_r)) = \tau(k_1)\,. \end{aligned}$$

It remains to show that $(\tau\sigma\tau^{-1})(k) = k,\ \ \forall\, k \in J_n \setminus \{\tau(k_1), \ldots, \tau(k_r)\}$. For this, note that $\tau^{-1}(k) \in J_n \setminus \{k_1, \ldots, k_r\}$, and so $\sigma(\tau^{-1}(k)) = \tau^{-1}(k)$. Therefore, we have $(\tau\sigma\tau^{-1})(k) = \tau(\sigma(\tau^{-1}(k))) = \tau(\tau^{-1}(k)) = k$. This completes the proof. □

Proposition 2.5.10. *Let $\sigma \in S_n$ be a cycle. Then σ is a r cycle if and only if $\mathrm{ord}(\sigma) = r$.*

Proof. Let $\sigma = (k_1\ \ k_2\ \ \cdots\ k_r)$, for some distinct elements $k_1, \ldots, k_r \in J_n$. Then for any $k \in J_n \setminus \{k_1, \ldots, k_r\}$ we have $\sigma(k) = k$. It follows from the definition of the cyclic expression of σ given in (2.5.4) that $\sigma^i(k_1) = k_{i+1}$, for all $i \in \{1, \ldots, k-1\}$ and $\sigma^r(k_1) = k_1$. In general, for any k_i with $1 \leq i \leq r$ we have $\sigma^{r-i}(k_i) = k_r$ and so $\sigma^{r-i+1}(k_i) = k_1$. Therefore, $\sigma^{r-i+\ell}(k_i) = k_\ell$ for all $\ell \in \{1, \ldots, r-1\}$, and hence $\sigma^r(k_i) = k_i$, for all $i \in \{1, \ldots, r\}$. Combining all these, we have $\sigma^r(k) = k$, for all $k \in J_n$. 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, $\mathrm{ord}(\sigma) = r$. Conversely, suppose that σ is a t cycle with $\mathrm{ord}(\sigma) = r$. But then as shown above $\mathrm{ord}(\sigma) = t$, and hence $t = r$. □

Exercise 2.5.11. Show that the number of distinct r cycles in S_n is $\dfrac{n!}{r(n-r)!}$.

Solution: 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 2.5.12. Two cycles $\sigma = (i_1 \;\; i_2 \cdots \;\; i_r)$ and $\tau = (j_1 \;\; j_2 \;\; \cdots \;\; j_s)$ in S_n are said to be *disjoint* if $\{i_1, i_2, \ldots, i_r\} \cap \{j_1, j_2, \cdots, j_s\} = \emptyset$.

Proposition 2.5.13. *If σ and τ are disjoint cycles in S_n, show that $\sigma \circ \tau = \tau \circ \sigma$.*

Proof. Let $\sigma = (i_1 \;\; i_2 \cdots \;\; i_r)$ and $\tau = (j_1 \;\; j_2 \;\; \cdots \;\; j_s)$ be two disjoint cycles in S_n. Let $k \in J_n$ be arbitrary. If $k \notin \{i_1, \ldots, i_r\} \cup \{j_1, \ldots, j_s\}$, then $\sigma(k) = k = \tau(k)$ and hence $(\sigma\tau)(k) = (\tau\sigma)(k)$ in this case. Suppose that $k \in \{i_1, \ldots, i_r\}$. Then $\sigma(k) \in \{i_1, \ldots, i_r\}$ and $k \notin \{j_1, \ldots, j_s\}$ together gives $\tau\sigma(k) = \sigma(k) = \sigma\tau(k)$. Interchanging the roles of σ and τ we see that $\tau\sigma(k) = \sigma(k) = \sigma\tau(k)$ holds for the case $k \in \{j_1, \ldots, j_s\}$. Therefore, $\sigma\tau = \tau\sigma$. □

Lemma 2.5.14. *For $n \geq 2$, any non-identity element of S_n can be uniquely written as a product of disjoint cycles of length at least 2. This expression is unique up to ordering of factors.*

Proof. For $n = 2$, S_2 has only one non-identity element, which is a 2-cycle $(1 \;\; 2)$. Assume that $n \geq 3$ and the result is true for any non-identity element of S_r for $2 \leq r < n$. Let $\sigma \in S_n$ be a non-identity element. Since $\{\sigma^i(1) : i \in \mathbb{N}\} \subseteq J_n$ and J_n is a finite set, there exists distinct integers $i, j \in \mathbb{N}$ such that $\sigma^i(1) = \sigma^j(1)$. Without loss of generality we may assume that $i - j \geq 1$. Then $\sigma^{i-j}(1) = 1$. Then

$$\{i \in \mathbb{N} : \sigma^i(1) = 1\}$$

is a non-empty subset of $\mathbb{N}$, and hence it has a least element, say r. Then all the elements in

$$A := \{1, \sigma(1), \sigma^2(1), \ldots, \sigma^{r-1}(1)\}$$

are all distinct, and defines an r-cycle

$$\tau := (1 \;\; \sigma(1) \;\; \sigma^2(1) \;\; \cdots \;\; \sigma^{r-1}(1))$$

in S_n. Let $B := J_n \setminus A$. In cases $\sigma\big|_B$ is the identity map of B onto itself or $B = \emptyset$, we have $\tau = \sigma$ and so σ is a cycle in S_n. Assume that $B \neq \emptyset$ and $\pi := \sigma\big|_B$ is not the identity map. Then π is a non-identity element of S_k, where $2 \leq k := |B| < n$. Then by induction hypothesis $\pi = \pi_1 \cdots \pi_\ell$ is a finite product of disjoint cycles $\pi_1, \ldots, \pi_\ell$ of lengths at least 2 in S_k. Then for each $i \in \{1, \ldots, \ell\}$ we define $\sigma_i \in S_n$ by setting

$$\sigma_i(a) = \begin{cases} \pi_i(a), & \text{if} \quad a \in B, \\ a, & \text{if} \quad a \in J_n \setminus B. \end{cases}$$

Then $\sigma_1, \ldots, \sigma_\ell, \tau$ are pairwise disjoint cycles in S_n and that $\sigma = \sigma_1 \cdots \sigma_\ell \tau$.

For the uniqueness part, let $\sigma = \sigma_1 \cdots \sigma_r = \tau_1 \cdots \tau_s$ be two decomposition of σ into product of disjoint cycles of lengths ≥ 2 in S_n. We need to show that $r = s$, and there is a permutation $\delta \in S_r$ such that $\sigma_i = \tau_{\delta(i)}$, for all $i \in \{1, \ldots, r\}$. Suppose that $\sigma_i = (k_1 \;\; k_2 \;\; \cdots \;\; k_t)$ with $t \geq 2$. Then $\sigma(k_1) \neq k_1$. Since $\tau_1, \ldots, \tau_r$ are pairwise disjoint cycles of lengths ≥ 2 in S_n, there is a unique element, say $\delta(i) \in \{1, \ldots, r\}$ such that $\tau_{\delta(i)}(k_1) \neq k_1$. By reordering, if required, we may write $\tau_{\delta(i)} = (k_1 \;\; v_2 \;\; \cdots \;\; v_u)$. Then we have

$$\begin{array}{ccccccccccc} k_2 & = & \sigma_i(k_1) & = & \sigma(k_1) & = & \tau_{\delta(i)}(k_1) & = & v_2, & & \\ k_3 & = & \sigma_i(k_2) & = & \sigma(k_2) & = & \sigma(v_2) & = & \tau_{\delta(i)}(v_2) & = & v_3, \\ \vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots \\ k_t & = & \sigma_i(k_{r-1}) & = & \sigma(k_{r-1}) & = & \sigma(v_{r-1}) & = & \tau_{\delta(i)}(v_{r-1}) & = & v_t\,. \end{array}$$

If $t < u$, then $k_1 = \sigma_i(k_t) = \sigma(k_t) = \sigma(v_t) = v_{t+1}$, which is a contradiction. Therefore, $t = u$ and hence $\sigma_i = \tau_{\delta(i)}$. Hence the result follows by induction on r. $\square$

Corollary 2.5.15. *For $n \geq 2$, every element of S_n can be written as a finite product of transpositions.*

Proof. In view of above Lemma 2.5.14 it suffices to show that every cycle of S_n is a product of transpositions. Clearly the identity element $e \in S_n$ can be written as $e = (1 \;\; 2)(1 \;\; 2)$. If $\sigma = (k_1 \;\; k_2 \;\; \cdots \;\; k_r)$ is an r-cycle, $r \geq 2$, in S_n, then we can rewrite it as

$$\sigma = (k_1 \;\; k_2 \;\; \cdots \;\; k_r) = (k_1 \;\; k_r)(k_1 \;\; k_{r-1}) \cdots (k_1 \;\; k_2).$$

Hence the result follows. $\square$

Note that decompositions of $\sigma \in S_n$ into a finite product of transpositions is not unique. For example, when $n \geq 3$ we have $e = (1 \;\; 2)(1 \;\; 2) = (1 \;\; 3)(1 \;\; 3)$. However, we shall see shortly that the number of transpositions appearing in such a product expression for $\sigma \in S_n$ is either odd or even, but cannot be both in two such decompositions.

Lemma 2.5.16. *Fix an integer $n \geq 2$, and consider the action of a permutation $\sigma \in S_n$ on the formal product $\chi := \prod\limits_{1 \leq i < j \leq n} (x_i - x_j)$ given by*

$$\sigma(\chi) := \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

If $\sigma \in S_n$ is a 2-cycle (transposition), then $\sigma(\chi) = -\chi$.

Proof. Since $\sigma \in S_n$ is a 2-cycle, there exists a unique subset $\{p, q\} \subseteq J_n$ with $p < q$ such that $\sigma = (p \;\; q)$. Then $\sigma(k) = k$, $\forall\, k \in J_n \setminus \{p, q\}$. Consider the factor $(x_i - x_j)$ of χ with $1 \leq i < j \leq n$. We have the following situations:

(a) If $\{i, j\} = \{p, q\}$, then $\sigma(x_i - x_j) = x_{\sigma(i)} - x_{\sigma(j)} = -(x_i - x_j)$.

(b) If $\{i, j\} \cap \{p, q\} = \emptyset$, then $\sigma(x_i - x_j) = x_{\sigma(i)} - x_{\sigma(j)} = (x_i - x_j)$.

(c) If $\{i, j\} \cap \{p, q\}$ is singleton set, then we have the following subcases.

  I. If $t < p < q$, then $\sigma((x_t - x_p)(x_t - x_q)) = (x_{\sigma(t)} - x_{\sigma(p)})(x_{\sigma(t)} - x_{\sigma(q)}) = (x_t - x_q)(x_t - x_p)$.

  II. If $p < t < q$, then $\sigma((x_p - x_t)(x_t - x_q)) = (x_{\sigma(p)} - x_{\sigma(t)})(x_{\sigma(t)} - x_{\sigma(q)}) = (x_q - x_t)(x_p - x_t)$.

  III. If $p < q < t$, then $\sigma((x_p - x_t)(x_q - x_t)) = (x_{\sigma(p)} - x_{\sigma(t)})(x_{\sigma(q)} - x_{\sigma(t)}) = (x_q - x_t)(x_p - x_t)$.

  Therefore, in the above three subcases the product $(x_t - x_p)(x_t - x_q)$ remains fixed under the action of σ.

From these it immediately follows that $\sigma(\chi) = -\chi$, for all 2-cycle $\sigma \in S_n$. $\square$

Corollary 2.5.17. *Fix an integer $n \geq 2$, and let $\sigma \in S_n$. If $\sigma = \sigma_1 \cdots \sigma_r = \tau_1 \cdots \tau_s$, where σ_i, τ_j are all transpositions in S_n, then both r and s are either even or odd.*

Proof. Consider the formal product $\chi := \prod_{1 \leq i < j \leq n} (x_i - x_j)$. Then $\sigma(\chi) = (\sigma_1 \circ \cdots \circ \sigma_r)(\chi) = (-1)^r \chi$ and $\sigma(\chi) = (\tau_1 \circ \cdots \circ \tau_s)(\chi) = (-1)^s \chi$ together implies that $(-1)^r = (-1)^s$, and hence both r and s are either even or odd. $\square$

Definition 2.5.18. 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 transpositions in S_n.

Note that given a permutation $\sigma \in S_n$, if $\sigma = \sigma_1 \circ \cdots \circ \sigma_r$, where $\sigma_1, \ldots, \sigma_r$ are 2-cycles in S_n, then by Corollary 2.5.17 we see that σ is even if and only if $(-1)^r = 1$. Thus we have a well-defined map $\mathrm{sgn} : S_n \to \{1, -1\}$ given by sending $\sigma \in S_n$ to $(-1)^r$, where r is a number of 2-cycles appearing in the decomposition of σ into a product of 2-cycles in S_n. In other words,

$$\mathrm{sgn}(\sigma) = \begin{cases} -1, & \text{if } \sigma \text{ is odd}, \\ 1, & \text{if } \sigma \text{ is even}, \end{cases} \tag{2.5.19}$$

The number $\mathrm{sgn}(\sigma)$ is called the *signature* of the permutation $\sigma \in S_n$.

Proposition 2.5.20. *An r-cycle $\sigma \in S_n$ is even if and only if r is odd.*

Proof. Let $\sigma = (k_1 \ k_2 \ \cdots \ k_r)$ be an r-cycle in S_n. Then we can write it as a product $\sigma = (k_1 \ k_2 \ \cdots \ k_r) = (k_1 \ k_r)(k_1 \ k_{r-1}) \cdots (k_1 \ k_2)$ of $r - 1$ number of transpositions in S_n. Hence the result follows. $\square$

Exercise 2.5.21. 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,

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

Since σ is a product of 5 transpositions in S_8, we conclude that 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 2.5.22. *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 2.5.10), 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. $\square$

Remark 2.5.23. 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 2.5.24. For all $n \geq 3$, show that A_n is generated by 3-cycles.

Solution: Note that any 3-cycle is an even permutation by Proposition 2.5.20, and hence is in A_n. Therefore, the subgroup of S_n generated by all 3-cycles is a subgroup of A_n. For the converse part, we show that any even permutation can be written as product of 3-cycles. Note that any element of A_n is a product of even number of 2-cycles in S_n. Let $\sigma = (i\ \ j)$ and $\tau = (k\ \ \ell)$ be two 2-cycles in S_n. If σ and τ are not disjoint, then we may assume that $j = k$. Then $\sigma \circ \tau = (i\ \ j)(j\ \ \ell) = (i\ \ j\ \ \ell)$ is a 3-cycle. If σ and τ are disjoint, then

$$\begin{aligned} \sigma \circ \tau &= (i\ \ j)(k\ \ \ell) \\ &= (i\ \ j)(j\ \ k)(j\ \ k)(k\ \ \ell) \\ &= (i\ \ j\ \ k)(j\ \ k\ \ \ell), \end{aligned}$$

where the last equality is due to the first case. Hence the result follows. □

Exercise 2.5.25. Show that $|A_n| = n!/2$.

Solution: Let $\{\sigma_1, \ldots, \sigma_r\}$ and $\{\tau_1, \ldots, \tau_s\}$ be the set of all even permutations and the set of all odd permutations in S_n, respectively. Since $r + s = n!$, it suffices to show that $r = s$. Fix a transposition $\pi \in S_n$. Then $\pi\sigma_1, \ldots, \pi\sigma_r$ are all distinct (verify) odd permutations in S_n, and hence $r \leq s$. Similarly $s \leq r$, and hence $r = s$, as required. □

Exercise 2.5.26. Determine the groups A_3 and A_4.

Exercise 2.5.27. 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 2.5.28 (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 2.5.29 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 2.5.29. Show that $D_3 = S_3$, and D_n is a proper subgroup of S_n, for all $n \geq 4$.

Exercise 2.5.30. 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 Group homomorphism

A group homomorphism is a map from a group G into another group H that respects the binary operations on them. Here is a formal definition.

Definition 2.6.1. 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 2.6.2. (i) For any group G, the constant map $c_e : G \to G$, 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) The map $f : \mathbb{R} \to S^1 := \{z \in \mathbb{C}^* : |z| = 1\}$ defined by $f(t) = e^{2\pi i t}$, $\forall\, t \in \mathbb{R}$ is a surjective group homomorphism. Is it injective?

(vi) 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 $\mathrm{SL}_2(\mathbb{R})$.

(vii) 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.

(viii) Fix a prime number $p > 0$, and let $\mathbf{F} : \mathbb{Z}_p \to \mathbb{Z}_p$ be the map defined by $\mathbf{F}(a) = a^p$, for all $a \in \mathbb{Z}_p$. Since any multiple of p is 0 in $\mathbb{Z}_p$, using binomial expansion we have

$$\mathbf{F}(a+b) = (a+b)^p = \sum_{j=0}^{p} \binom{p}{j} a^{p-j} b^j = a^p + b^p.$$

Therefore, $\mathbf{F}$ is a group homomorphism.

(ix) Fix an integer $n \geq 1$, and let $f : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ be the map defined by

$$f(A) = \det(A),\ \forall\, A \in \mathrm{GL}_n(\mathbb{R}).$$

Verify that f is a group homomorphism.

(x) Let $m, n > 1$ be integers such that $n \mid m$ in $\mathbb{Z}$. Verify that the map $\varphi : \mathbb{Z}_m \to \mathbb{Z}_n$ defined by sending $[a] \in \mathbb{Z}_m$ to $[a] \in \mathbb{Z}_n$ is a well-defined map that is a group homomorphism.

(xi) Let G be a group. For each $a \in G$, the map $\varphi_a : G \to G$ defined by $\varphi_a(b) = aba^{-1}$, $\forall\, b \in G$, is a group homomorphism.

Exercise 2.6.3. 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}.

Lemma 2.6.4. *Let $n \geq 2$ be an integer. Then the map $\mathrm{sgn} : S_n \to \{1, -1\}$ defined by sending $\sigma \in S_n$ to*

$$\mathrm{sgn}(\sigma) = \begin{cases} -1, & \text{if } \sigma \text{ is odd}, \\ 1, & \text{if } \sigma \text{ is even}, \end{cases}$$

is a group homomorphism, called the signature homomorphism for S_n.

Proof. Let $\sigma, \tau \in S_n$ be arbitrary. Let $\sigma = \sigma_1 \circ \cdots \circ \sigma_r$ and $\tau = \tau_1 \circ \cdots \circ \tau_s$, where σ_i, τ_j are all 2-cycles in S_n. Then $\sigma \circ \tau = \sigma_1 \circ \cdots \circ \sigma_r \circ \tau_1 \circ \cdots \circ \tau_s$, and hence $\mathrm{sgn}(\sigma \circ \tau) = (-1)^{r+s} = (-1)^r(-1)^s = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau)$. □

Proposition 2.6.5. *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 2.2.28 (i) that $\mathrm{ord}(f(a)) \mid n$.

□

Exercise 2.6.6. Let G and H be two groups. Show that there is a unique constant group homomorphism from G to H.

Proposition 2.6.7. *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.

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 2.6.5 (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.

□

Proposition 2.6.8. *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 2.6.9. 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 (c.f. Proposition 2.6.22),

(iii) f is an *epimorphism* if f is surjective (c.f. Proposition 2.6.23), and

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

Corollary 2.6.10. *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. □

Proposition 2.6.11. *Given a group G, the set $\mathrm{Aut}(G)$ consisting of all group isomorphisms from G onto itself is a group with respect to the binary operation given by composition of maps; the group $\mathrm{Aut}(G)$ is known as the automorphism group of G.*

Proof. Since composition of two bijective group homomorphisms is bijective and a group homomorphism, we see that the map

$$G \times G \to G, \;\; (f, g) \longmapsto f \circ g,$$

is a binary operation on $\mathrm{Aut}(G)$. Clearly composition of maps is associative. The identity map $\mathrm{Id}_G : G \to G$ plays the role of a neutral element in a group. Given $f \in \mathrm{Aut}(G)$, its inverse $f^{-1} : G \to G$ is again a group homomorphism. Indeed, given $a, b \in G$ there exists unique $x, y \in G$ such that $f(x) = a$ and $f(y) = b$. Then we have $f^{-1}(ab) = f^{-1}(f(x)f(y)) = f^{-1}(f(xy)) = xy = f^{-1}(a)f^{-1}(y)$, and hence $f^{-1} \in \mathrm{Aut}(G)$. This proves that $\mathrm{Aut}(G)$ is a group. $\square$

Example 2.6.12. The complex conjugation map $z \mapsto \overline{z}$ from the additive group $\mathbb{C}$ into itself is an automorphism of $\mathbb{C}$.

Exercise 2.6.13. Show that $\mathrm{Aut}(K_4)$ is isomorphic to S_3. (*Hint:* Note that $K_4 = \{e, a, b, c\}$, where $a^2 = b^2 = c^2 = e$ and $ab = ba = c, bc = cb = a, ac = ca = b$. If $f \in \mathrm{Aut}(K_4)$, then $f(e) = e$ and hence $f\big|_{\{a,b,c\}}$ is a bijection of the subset $\{a, b, c\} \subset K_4$ onto itself, producing an element of S_3. Thus we get a map $\varphi : \mathrm{Aut}(K_4) \to S_3$. Verify that φ is a group isomorphism.)

Definition 2.6.14. 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 2.6.5 (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 2.6.15. (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 2.6.16 (Universal Property of Kernel). *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 $\iota_K \circ \psi = \phi$.

(2.6.17)
$$\begin{tikzcd}
 & G' \arrow[dl, dashed, "\exists\,!\,\psi"'] \arrow[d, "\phi"] \arrow[dr, "f\circ\phi=e_H"] & \\
K \arrow[r, "\iota_K"] & G \arrow[r, "f"] & H
\end{tikzcd}$$

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 (2.6.17), 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 2.6.17. 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 2.6.18. *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 2.6.19. *Any infinite cyclic group is isomorphic to $\mathbb{Z}$.*

Proof. Let $G = \langle a \rangle$ be an infinite cyclic group. Define a map $f : \mathbb{Z} \to G$ by $f(n) = a^n$, for all $n \in \mathbb{Z}$. Since

$$f(n+m) = a^{n+m} = a^n a^m = f(n)f(m), \; \forall\, m, n \in \mathbb{Z},$$

the map f is a group homomorphism. Since G is infinite, we have $a^n \neq e$, $\forall\, n \in \mathbb{Z} \setminus \{0\}$. Therefore, $\mathrm{Ker}(f) = \{e\}$, and so f is injective. Clearly f is surjective, and hence is an isomorphism. □

Proposition 2.6.20. *Let G be a cyclic group generated by $a \in G$. A homomorphism $f : G \to G$ is an automorphism of G if and only if $f(a)$ is a generator of G.*

Proof. Let $f : G \to G$ be an automorphism of G. Let $b = f(a)$. Let $x \in G$ be arbitrary. Since f is surjective, there exists $y \in G$ such that $f(y) = x$. Since $G = \langle a \rangle$, we have $y = a^n$, for some $n \in \mathbb{Z}$. Then $x = f(y) = f(a^n) = [f(a)]^n = b^n \in \langle b \rangle$. This shows that $G = \langle b \rangle$, and hence b is a generator of G. Conversely if $f : G \to G$ is a homomorphism such that $f(a)$ generates G, then f is surjective. If $|G|$ is finite, we must have f is bijective. If G is not finite, then G has only two generators, namely a and a^{-1} by Proposition 2.3.15, and hence f must be either Id_G or the map given by sending $b \in G$ to b^{-1}. In both cases, f is injective, and hence is in $\mathrm{Aut}(G)$. □

Theorem 2.6.21 (Cayley)**.** *Every group is a subgroup of a symmetric group.*

Proof. Let G be a group. Let $S(G)$ be the symmetric group on G; its elements are all bijective maps from G onto itself and the group operation is given by composition of bijective maps. Define a map

$$\varphi : G \longrightarrow S(G)$$

by sending an element $a \in G$ to the map

$$\varphi_a : G \to G, \;\; g \mapsto ag,$$

which is bijective (verify!), and hence is an element of $S(G)$. Then given any $g \in G$ we have

$$\begin{aligned}\varphi(ab)(g) &= \varphi_{ab}(g)\\ &= (ab)g = a(bg)\\ &= (\varphi_a \circ \varphi_b)(g)\\ &= (\varphi(a) \circ \varphi(b))(g),\end{aligned}$$

and hence φ is a group homomorphism. Note that $\varphi_a = \mathrm{Id}_G$ if and only if $a = e$ in G (verify!). Therefore, φ is an injective group homomorphism, and hence we can identify G with the subgroup $\varphi(G)$ of the symmetric group $S(G)$. □

We end this section with the following two results which justify the terminologies introduced in Definition 2.6.9 in the light of category theory.

Proposition 2.6.22. *Let $f : G \to H$ be a group homomorphism. Then the following are equivalent.*

(i) f is injective.

(ii) Given a group T and group homomorphisms $\phi, \psi : T \to G$ with $f \circ \phi = f \circ \psi$, we have $\phi = \psi$. In other words, f is a **monomorphism** *in the category of groups.*

(iii) Given a group T and a group homomorphism $\phi : T \to G$ with $f \circ \phi$ trivial, we have ϕ is trivial.

Proof. (i) $\Rightarrow$ (ii) is Clear. To show (ii) $\Rightarrow$ (iii), take $\psi : T \to G$ to be the trivial group homomorphism. Then both $f \circ \phi$ and $f \circ \psi$ are trivial, and hence ϕ is trivial by (ii). To show (iii) $\Rightarrow$ (i), take $T = \mathrm{Ker}(f)$ and $\phi : T \to G$ the inclusion map of $\mathrm{Ker}(f)$ into G. Then $f \circ \phi$ is trivial, and hence the inclusion map $\phi : \mathrm{Ker}(f) \hookrightarrow G$ is a trivial group homomorphism by (iii). This forces $\mathrm{Ker}(f) = \{e\}$, and hence f is injective. □

Proposition 2.6.23. *Let $f : G \to H$ be a group homomorphism. Then the following are equivalent.*

(i) f is surjective.

(ii) Given a group T and group homomorphisms $\phi, \psi : H \to T$ with $\phi \circ f = \psi \circ f$, we have $\phi = \psi$. In other words, f is an **epimorphism** *in the category of groups.*

(iii) Given a group T and a group homomorphism $\phi : H \to T$ with $\phi \circ f$ trivial, we have ϕ is trivial.

Proof. (i) $\Rightarrow$ (ii): Let $\phi, \psi : H \to T$ be group homomorphisms with $\phi \circ f = \psi \circ f$. Since f is surjective, given $h \in H$ there exists $g \in G$ such that $f(g) = h$. Then $(\phi \circ f)(g) = (\psi \circ f)(g)$ gives $\phi(h) = \psi(h)$. Since $h \in H$ is arbitrary, we have $\phi = \psi$.

(ii) $\Rightarrow$ (iii): Take $\psi : H \to T$ to be the trivial group homomorphism.

(iii) $\Rightarrow$ (i): We use the notion of coset of a subgroup. See Proposition 2.7.18 for a proof. □

2.7 Notion of Quotient & Cosets

Let G be a group, and H a subgroup of G. In this section we introduce the notion of a quotient group of G by H and prove its uniqueness. In the process of construction of quotient, we identify a class of subsets of G, known as *cosets* of H in G, and discuss their basic properties with some applications. An explicit construction of quotient group will appear in the next section.

Definition 2.7.1 (Quotient Group)**.** Let H be a subgroup of a group G. The *quotient* of G by H is a pair (Q, π), where Q is a group and $\pi : G \to Q$ is a surjective group homomorphism such that

(QG1) $\pi(h) = e_Q$, the neutral element of Q, for all $h \in H$, and

(QG2) *Universal property of quotient:* given a group T and a group homomorphism $t : G \to T$ satisfying $H \subseteq \mathrm{Ker}(t)$, there exists a **unique** group homomorphism $\widetilde{t} : Q \to T$ such that $\widetilde{t} \circ \pi = t$; i.e., the following diagram commutes.

(2.7.2)
$$\begin{tikzcd} G \arrow[r, "t"] \arrow[d, "\pi"'] & T \\ Q \arrow[ur, dashed, "\exists!\widetilde{t}"'] & \end{tikzcd}$$

Interesting point is that, without knowing existence of such a pair (Q, q), it follows immediately from the properties (QG1) and (QG2) that such a pair (Q, q), if it exists, must be unique up to a unique isomorphism of groups in the following sense.

Proposition 2.7.3 (Uniqueness of Quotient)**.** *With the above notations, if (Q, π) and (Q', π') are two quotients of G by H, then there exists a unique group isomorphism $\varphi : Q \to Q'$ such that $\varphi \circ \pi = \pi'$.*

Proof. Taking $(T, t) = (Q', \pi')$ by universal property of quotient (Q, π) we have a unique group homomorphism $\widetilde{\pi'} : Q \to Q'$ such that $\widetilde{\pi'} \circ \pi = \pi'$. Similarly, taking $(T, t) = (Q, \pi)$ by universal property of quotient (Q', π') we have a unique group homomorphism $\widetilde{\pi} : Q' \to Q$ such that $\widetilde{\pi} \circ \pi' = \pi$. Since both $\widetilde{\pi} \circ \widetilde{\pi'}$ and Id_Q are group homomorphisms from Q into itself making the following diagram commutative,

$$\begin{tikzcd} & G \arrow[dl, "\pi"'] \arrow[d, "\pi'"] \arrow[dr, "\pi"] & \\ Q \arrow[r, "\widetilde{\pi'}"] \arrow[rr, bend right, "\mathrm{Id}_Q"'] & Q' \arrow[r, "\widetilde{\pi}"] & Q \end{tikzcd}$$

it follows that $\widetilde{\pi} \circ \widetilde{\pi'} = \mathrm{Id}_Q$. Similarly $\widetilde{\pi'} \circ \widetilde{\pi} = \mathrm{Id}_{Q'}$. Therefore, $\widetilde{\pi'} : Q \to Q'$ is the unique group isomorphisms such that $\widetilde{\pi'} \circ \pi = \pi'$. This completes the proof. □

Now question is about existence of quotient. We shall see shortly that we need to impose an additional hypothesis on H (namely H should be a normal subgroup of G) for existence of quotient. The condition (QG1) says that $\pi(H) = \{e_Q\}$. Since $\pi : G \to Q$ is a group homomorphism by assumption, given any two elements $a, b \in G$ with $a^{-1}b \in H$ we have $\pi(a^{-1}b) = e_Q$, and hence $\pi(a) = \pi(b)$. In other words, two elements $a, b \in G$ are in the same fiber of the map $\pi : G \to Q$ if $a^{-1}b \in H$. Since the set of all fibers of any set map $f : G \to Q$ gives a partition of G, and hence an equivalence relation on G, the condition (QG1) suggests us to define a relation ρ_L on G by setting
$$(a, b) \in \rho_L \quad \text{if} \quad a^{-1}b \in H.$$
It is easy to check that ρ_L is an equivalence relation on G (verify!). The ρ_L-equivalence class of an element $a \in G$ is the subset

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

which we denote by aH; the subset aH is called the **left coset** of H in G represented by a. Note that (verify!), given $a, b \in G$,

(i) either $aH \cap bH = \emptyset$ or $aH = bH$,

(ii) $aH = bH$ if and only if $a^{-1}b \in H$, and

(iii) $G = \bigcup_{a \in G} aH$.

Proposition 2.7.4. *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 2.7.5 (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 2.7.4), 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. □

Exercise 2.7.6. Let G be a finite group of order mn having subgroups H and K of orders m and n, respectively. If $\gcd(m, n) = 1$ show that $HK := \{hk \in G : h \in H,\ k \in K\}$ is a group.

Corollary 2.7.7. *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 2.7.5, $|H|$ 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 2.7.8. *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 2.7.9 (Euler's Theorem)**.** *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 $\{k \in \mathbb{N} : 1 \leq k < n \text{ and } \gcd(k, n) = 1\}$.*

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 2.7.10 (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 2.7.9. □

Exercise 2.7.11. 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 2.7.12. Show that $15^{1000} - 1$ and $105^{1200} - 1$ are divisible by 8.

Exercise 2.7.13. 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

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

Lemma 2.7.14. *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 2.7.15. 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.

Exercise 2.7.16. Let H and K be two subgroups of G of finite indices. Show that $H \cap K$ is a subgroup of G of finite index.

Example 2.7.17. 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

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

Since there are exactly n such distinct equivalence classes by division algorithm, namely

$$a + n\mathbb{Z}, \text{ where } 0 \leq a \leq n - 1;$$

(c.f. 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.

Proposition 2.7.18 (Epimorphism of groups is surjective). *Let $f : G \to H$ be a group homomorphism satisfying the following property:*

- *Given a group T and a group homomorphism $\phi : H \to T$ with $\phi \circ f$ trivial, we have ϕ is trivial.*

Then f is surjective.

Proof. Note that $A := f(G)$ is a subgroup of H, and so we can consider the set

$$A\backslash H = \{Ah : h \in H\}$$

consisting of all distinct right cosets of A in H. Let A' be a subset of H which is not a right coset of A in H, and let $S = \{A'\} \cup H/A$. Let $T = \mathrm{Aut}(S)$ be the symmetric group on S; its elements are bijective maps from S onto itself and the group operation is given by composition of maps. Note that, given $h \in H$, consider the map

$$\varphi_h : A\backslash H \to A\backslash H$$

that sends $Ah' \in A\backslash H$ to $A(h'h) \in A\backslash H$. Since $(h'h)(h''h)^{-1} = h'hh^{-1}h''^{-1} = h'h''^{-1}$, it follows that φ_h is well-defined and injective. Since $\varphi_{h^{-1}} \circ \varphi_h = \mathrm{Id}_{A\backslash H} = \varphi_h \circ \varphi_{h^{-1}}$, the map φ_h is bijective.

Let $\varphi : H \to T := \mathrm{Aut}(S)$ be the map given by sending $h \in H$ to the permutation $\varphi(h) \in \mathrm{Aut}(S)$ which is defined by

$$\varphi(h)(A') = A' \quad \text{and} \quad \varphi(h)\big|_{A\backslash H} = \varphi_h.$$

It is easy to verify that φ is a group homomorphism. Let $\sigma \in T = \mathrm{Aut}(S)$ be the permutation that interchanges A and A', and keeps everything else fixed; i.e., σ is the 2-cycle $\sigma = (A \;\; A')$. Then the map

$$\psi : H \to T, \quad h \mapsto \sigma^{-1}\varphi(h)\sigma, \tag{2.7.19}$$

is a group homomorphism (verify!).

If $a \in A$, then $\varphi(a)(A) = Aa = A$ and $\varphi(a)(A') = A'$. Then $\varphi(a) \in T$ is disjoint from the 2-cycle $\sigma = (A \;\; A')$, and hence they commute to give $\psi(a) = \sigma^{-1}\varphi(a)\sigma = \varphi(a)$. Therefore, $\varphi\big|_A = \psi\big|_A$ and hence $\varphi \circ f = \psi \circ f$. Since f is an epimorphism, we have $\varphi = \psi$. Then $\varphi(h) = \sigma^{-1}\varphi(h)\sigma$, for all $h \in H$. Since $\sigma = (A \;\; A')$ and $\varphi(h)(A') = A'$, we have $\varphi(h)(A) = (\sigma^{-1}\varphi(h)\sigma)(A) = \sigma^{-1}\varphi(h)(A') = \sigma^{-1}(A') = A$. Since $\varphi(h)(A) = Ah$ by definition, we have $Ah = A$, and hence $h \in A$. Since $h \in H$ is arbitrary, we have $A = H$, as required. ☐

Exercise 2.7.20. (i) Does there exists a group isomorphism from $(\mathbb{Q}, +)$ onto $(\mathbb{Q}^*, \cdot)$?

(ii) Does there exists a surjective group homomorphism from $(\mathbb{Q}, +)$ onto $(\mathbb{Q}^+, \cdot)$?

(iii) Does there exists a non-trivial group homomorphism from $\mathbb{Q}$ into $\mathbb{Z}$?

2.8 Normal Subgroup & Quotient Group

In this section we introduce the notion of normal subgroup and give a construction of quotient of a group by its normal subgroup. Recall that the condition (QG1) in Definition 2.7.1 of quotient group suggests us to consider the set

$$G/H := \{gH : g \in G\}$$

consisting of all left cosets of H in G as a possible candidate for the set Q. Now question is what should be the appropriate group structure on it? Take any group homomorphism $f : G \to T$ such that $H \subseteq \mathrm{Ker}(f)$. Then we have $f(a) = f(b)$ if $a^{-1}b \in H$. The commutativity of the diagram (2.7.2) tells us to send $aH \in Q$ to $f(a) \in T$ to define the map $\widetilde{f} : Q \to T$ which needs to be a group homomorphism. Then we should have

$$\widetilde{f}((aH)(bH)) = f(ab) = \widetilde{f}((ab)H), \ \forall\, a, b \in G. \tag{2.8.1}$$

This suggests us to define a binary operation on the set $G/H = \{gH : g \in G\}$ by

$$(aH)(bH) := (ab)H, \ \ \forall\, a, b \in G. \tag{2.8.2}$$

Proposition 2.8.3. *The map $G/H \times G/H \to G/H$ defined by sending (aH, bH) to $(ab)H$ is well-defined if and only if*

$$g^{-1}hg \in H, \ \ \forall\, g \in G \text{ and } h \in H. \tag{2.8.4}$$

Proof. Suppose the the above map is well-defined. Let $h \in H$ and $g \in G$ be arbitrary. Then $hH = H$, and hence $(hH) \cdot (gH) = H \cdot (gH)$. Since the above defined binary operation on G/H is well-defined, we have $(hg)H = gH$ and hence $g^{-1}hg \in H$.

Conversely, suppose that $g^{-1}hg \in H$, for all $g \in G$ and $h \in H$. Let $a_1H = a_2H$ and $b_1H = b_2H$, for some $a_1, a_2, b_1, b_2 \in G$. Then $h := a_1^{-1}a_2 \in H$ and $b_1^{-1}b_2 \in H$. Then

$$\begin{aligned}(a_1b_1)^{-1}(a_2b_2) &= b_1^{-1}a_1^{-1}a_2b_2 \\ &= b_1^{-1}hb_2, \ \text{ since } h := a_1^{-1}a_2. \\ &= (b_1^{-1}hb_1)(b_1^{-1}b_2) \in H,\end{aligned}$$

since H is a group and both $b_1^{-1}hb_1$ and $b_1^{-1}b_2$ are in H. Therefore, $(a_1b_1)H = (a_2b_2)H$, as required. $\square$

Proposition 2.8.3 suggests us to reserve a terminology for those subgroups H of G that satisfies the property (2.8.4).

Definition 2.8.5 (Normal Subgroup)**.** A subgroup H of a group G is said to be *normal* in G if $g^{-1}hg \in H, \ \forall\, g \in G, \ h \in H$.

Exercise 2.8.6. Let G be a group and H a subgroup of G. Given $a \in G$, let

$$Ha := \{ha : h \in H\} \subseteq G.$$

Show that the following are equivalent.

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

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

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

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

Proposition 2.8.7. *Any subgroup of index 2 is normal.*

Proof. Let H be a subgroup of G such that $[G : H] = 2$. Then H has only two left (resp., right) cosets, namely H and aH (resp., H and Ha), where $a \in G \setminus H$. Since $G = H \sqcup aH = H \sqcup Ha$, for any $a \in G \setminus H$, we see that $aH = Ha$, for all $a \in G$, and hence $aHa^{-1} = H$, for all $a \in G$. This completes the proof. $\square$

Corollary 2.8.8. *For all $n \geq 3$, A_n is a normal subgroup of S_n.*

Exercise 2.8.9. (i) Show that any subgroups of an abelian group G is normal in G.

(ii) Let $H = \langle (1\ \ 2\ \ 3) \rangle$ be the cyclic subgroup of S_3 generated by the 3-cycle $(1\ \ 2\ \ 3) \in S_3$. Show that H is a normal subgroup of S_3.

(iii) Verify if the subgroup $K := \langle (1\ \ 2) \rangle$ of S_3 is normal or not.

(iv) Determine all normal subgroups of S_3.

(v) Show that $\mathrm{SL}_n(\mathbb{R})$ is a normal subgroup of $\mathrm{GL}_n(\mathbb{R})$, for all $n \in \mathbb{N}$.

Exercise 2.8.10. Let H be a subgroup of G. Let $\rho = \{(a, b) \in G \times G : a^{-1}b \in H\} \subseteq G \times G$. Note that ρ is an equivalence relation on G. Show that H is a normal subgroup of G if and only if ρ is a subgroup of the direct product group $G \times G$ (see Exercise 2.1.34).

Lemma 2.8.11. *The kernel of a group homomorphism $f : G \to H$ 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. □

Exercise 2.8.12. For $n \geq 2$, show that A_n is a normal subgroup of S_n by constructing a group homomorphism $\varphi : S_n \to \mu_2 = \{1, -1\}$ such that $\mathrm{Ker}(\varphi) = A_n$.

Exercise 2.8.13. For $n \geq 1$, show that $\mathrm{SL}_n(\mathbb{R})$ is a normal subgroup of $\mathrm{GL}_n(\mathbb{R})$ by constructing a group homomorphism $\varphi : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ such that $\mathrm{Ker}(\varphi) = \mathrm{SL}_n(\mathbb{R})$.

Lemma 2.8.14. *Let $f : G \to H$ be a group homomorphism. If K is a normal subgroup of H, then $f^{-1}(K)$ is a normal subgroup of G.*

Proof. Suppose that K is a normal subgroup of H. Then for any $a \in G$ and $b \in f^{-1}(K)$, we have $f(aba^{-1}) = f(a)f(b)f(a)^{-1} \in K$, and hence $aba^{-1} \in f^{-1}(K)$. □

Exercise 2.8.15. Show that $N := \{A \in \mathrm{GL}_n(\mathbb{C}) : |\det(A)| = 1\}$ is a normal subgroup of $\mathrm{GL}_n(\mathbb{C})$.

Remark 2.8.16. 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 normal subgroup K which is not a normal subgroup of G. Can you give such an example?

Theorem 2.8.17 (Existence of Quotient Group)**.** *Let H be a normal subgroup of a group G. Then the quotient group (Q, π) of G by H exists and is unique in the sense that if (Q, π) and (Q', π') are two quotients of G by H, then there exists a unique isomorphism of groups $\varphi : Q \to Q'$ such that $\varphi \circ \pi' = \pi$. We denote Q by G/H.*

Proof. Since H is a normal subgroup of G,

$$(aH)(bH) := (ab)H, \ \forall\, a, b \in G,$$

is a well-defined binary operation on the set $G/H := \{aH : a \in G\}$; see Proposition 2.8.3. 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. Set $Q := G/H$ and consider the map

(2.8.18) $$\pi : G \longrightarrow Q \ \text{ defined by } \ \pi(a) = aH, \ \forall\, a \in G.$$

Clearly π is surjective and given $a, b \in G$ we have $\pi(ab) = (ab)H = (aH)(bH) = \pi(a)\pi(b)$. Therefore, π is a group homomorphism. Since for any $h \in H$, we have $\pi(h) = hH = eH = H$, the neutral element of the group G/H, we see that $H \subseteq \operatorname{Ker}(\pi)$. Let T be any group and $t : G \to T$ be a group homomorphism satisfying $t(h) = e_T$, the neutral element of T, for all $t \in T$. Since $aH = bH$ if and only if $a^{-1}b \in H$, applying π on $a^{-1}b$ we see that $\pi(a) = \pi(b)$. Therefore, the map

(2.8.19) $$\widetilde{t} : G/H \to T, \ \ aH \longmapsto t(a),$$

is well-defined. Since

$$\widetilde{t}((aH)(bH)) = \widetilde{t}((ab)H) = f(ab) = f(a)f(b) = \widetilde{t}(aH)\widetilde{t}(bH),$$

we conclude that $\widetilde{t}$ is a group homomorphism. Since $(\widetilde{t} \circ \pi)(a) = \widetilde{t}(aH) = f(a)$, $\forall\, a \in G$, we have $\widetilde{t} \circ \pi = f$. If $\xi : G/H \to T$ is any group homomorphism satisfying $\xi \circ \pi = t$, then for any $a \in G$ we have $\widetilde{t}(aH) = (\widetilde{t} \circ \pi)(a) = t(a) = (\xi \circ \pi)(a) = \xi(aH)$, and hence $\widetilde{t} = \xi$. Therefore, the pair $(G/H, \pi)$ satisfy the properties (QG1) and (QG2), and hence is a quotient of G by H. Uniqueness is already shown in Proposition 2.7.3. □

Corollary 2.8.20. *Let H be a normal subgroup of a group G, and let $(G/H, \pi)$ be the associated quotient of G by H. Then $\operatorname{Ker}(\pi) = H$.*

Proof. Since the group operation on the quotient group $G/H := \{aH : a \in G\}$ is given by $(aH)(bH) := (ab)H$, $\forall\, aH, bH \in G/H$, we have

$$\begin{aligned} \operatorname{Ker}(\pi) &= \{a \in G : \pi(a) = H\} \\ &= \{a \in G : aH = H\} \\ &= \{a \in G : a \in H\} = H. \end{aligned}$$

This completes the proof. □

Exercise 2.8.21. Let G be a group such that $G/Z(G)$ is cyclic. Show that G is abelian.

2.9 Isomorphism Theorems

Let G be a group. Given a normal subgroup K of G, let $(G/K, \pi)$ be the associated quotient group of G by K, where

$$\pi : G \to G/K = \{aK : a \in G\}$$

is the natural quotient homomorphism given by

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

Theorem 2.9.1. *Let $f : G \to H$ be a group homomorphism. Let K be a normal subgroup of G such that $K \subseteq \operatorname{Ker}(f)$. 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.*

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[d, "\pi"'] & & H \\ G/K \arrow[urr, "\widetilde{f}"'] & & \end{tikzcd}$$

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

Proof. Since K is a normal subgroup of G, the quotient group G/K exists with the natural surjective group homomorphism $\pi : G \to G/K$ defined by $\pi(a) = aK$, $\forall\, a \in G$. Since $K \subseteq \mathrm{Ker}(f)$, by universal property of quotient (see Definition 2.7.1) we have a unique group homomorphism $\widetilde{f} : G/K \to H$ such that $\widetilde{f} \circ \pi = f$. The fact that $\widetilde{f}$ is a well-defined group homomorphism can also be directly checked by observing that

$$\widetilde{f}(aK) = (\widetilde{f} \circ \pi)(a) = f(a),\ \forall\, a \in G.$$

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 2.6.18 that $\widetilde{f}$ is injective if and only if $K = \mathrm{Ker}(f)$. □

As an immediate corollary, we have the following.

Corollary 2.9.2 (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 2.9.1 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. □

Let G be a group. Note that given a normal subgroup N of G, the quotient group G/N of G by N comes with a natural surjective group homomorphism $\pi_N : G \to G/N$ such that $\mathrm{Ker}(\pi_N) = N$ (see Definition 2.7.1 and Corollary 2.8.20). On the other hand, given a group Q and a surjective group homomorphism $\pi : G \to Q$, its kernel $\mathrm{Ker}(\pi)$ is a normal subgroup of G such that $G/\mathrm{Ker}(\pi) \cong Q$ by the First isomorphism theorem (Corollary 2.9.2) for groups. This motivates us to define the following (c.f. Definition 2.7.1).

Definition 2.9.3. A *quotient group* of G is a pair (Q, π), where Q is a group and $\pi : G \to Q$ is a surjective group homomorphism.

As an immediate consequence, we have the following.

Corollary 2.9.4. *Given a group G, there is a one-to-one correspondence between the following two sets:*

(i) $\mathcal{N}_G$:= the set of all normal subgroups of G, and

(ii) $\mathcal{Q}_G$:= the set of all quotient groups of G.

Proof. Define a map $\Phi : \mathcal{N}_G \to \mathcal{Q}_G$ by sending a normal subgroup N of G to the associated quotient group $(G/N, \pi_N) \in \mathcal{Q}_G$. Since π_N is a surjective group homomorphism with $\mathrm{Ker}(\pi_N) = N$, the map Φ admits an inverse, namely $\Psi : \mathcal{Q}_G \to \mathcal{N}_G$ given by sending a quotient group (Q, π) of G to the kernel $N := \operatorname{Ker}(\pi) \in \mathcal{N}_G$. Since the pairs $(G/N, \pi_N)$ and (Q, π) are uniquely isomorphic, we conclude that Φ and Ψ are inverse to each other. This completes the proof. $\square$

Proposition 2.9.5. *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 $\operatorname{Ker}(f) = \{k \in \mathbb{Z} : [k] = [0]\} = n\mathbb{Z}$. Then by first isomorphism theorem we have $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. $\square$

Proposition 2.9.6. *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 $\mathbb{Z}/\operatorname{Ker}(f)$. Note that, $\operatorname{Ker}(f) = \{k \in \mathbb{Z} : a^k = e\}$. Since G is a cyclic group of order n generated by a, we have $\operatorname{ord}(a) = n$ (see Corollary 2.3.11). Then we have $\operatorname{Ker}(f) = \{k \in \mathbb{Z} : a^k = e\} = n\mathbb{Z}$. Therefore, $G \cong \mathbb{Z}/n\mathbb{Z}$. Since $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ by Theorem 2.9.5, we have $G \cong \mathbb{Z}_n$. $\square$

Let G be a group. Given $a \in G$, the map $\varphi_a : G \to G$ defined by

$$\varphi_a(b) = aba^{-1}, \ \forall\, b \in G,$$

is a group homomorphism. Indeed,

$$\varphi_a(bc) = a(bc)a^{-1} = (aba^{-1})(aca^{-1}) = \varphi_a(b)\varphi_a(c), \ \forall\, b, c \in G.$$

Since $\operatorname{Ker}(\varphi_a) = \{b \in G : aba^{-1} = e\} = \{e\}$, φ_a is injective. Given $c \in G$, note that $\varphi_a(a^{-1}ca) = a(a^{-1}ca)a^{-1} = c$, and so φ_a is surjective. Therefore, φ_a is an isomorphism.

Definition 2.9.7. An automorphism $\varphi \in \operatorname{Aut}(G)$ is said to be an *inner automorphism of G* if there exists $a \in G$ such that $\varphi(b) = aba^{-1}$, for all $b \in G$.

Proposition 2.9.8. *Let G be a group. Let $\operatorname{Inn}(G)$ be the set of all inner autormorphisms of G. Then $\operatorname{Inn}(G)$ is a subgroup of $\operatorname{Aut}(G)$.*

Proof. Note that the identity map $\operatorname{Id}_G : G \to G$ is in $\operatorname{Inn}(G)$. Given $f, g \in \operatorname{Inn}(G)$, there exists $a, b \in G$ such that f and $g(x) = bxb^{-1}$, for all $x \in G$. Then $f^{-1} = \varphi_{a^{-1}}$, and that $(\varphi_a^{-1} \circ \varphi_b)(x) = a^{-1}bxb^{-1}a = (a^{-1}b)x(a^{-1}b)^{-1} = \varphi_{a^{-1}b}(x)$, for all $x \in G$. Therefore, $\operatorname{Inn}(G)$ is a subgroup of $\operatorname{Aut}(G)$. $\square$

Proposition 2.9.9. *The map $\varphi : G \to \operatorname{Inn}(G)$ that sends $a \in G$ to the map $\varphi_a : G \to G$ defined by*

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

is a surjective group homomorphism with kernel $Z(G)$. Consequently, $G/Z(G) \cong \operatorname{Inn}(G)$.

Proof. Let $a, b \in G$ be given. Then for any $x \in G$ we have $\varphi(ab)(x) = (ab)x(ab)^{-1} = a(bxb^{-1})a^{-1} = a(\varphi_b(x))a^{-1} = (\varphi_a \circ \varphi_b)(x)$, and hence $\varphi(ab) = \varphi(a) \circ \varphi(b)$. Therefore, φ is a group homomorphism. Since every element of $\mathrm{Inn}(G)$ is of the form φ_a, for some $a \in G$, the map φ is surjective. Since $\mathrm{Ker}(\varphi) = \{a \in G : \varphi(a) = \mathrm{Id}_G\} = \{a \in G : aba^{-1} = b, \ \forall\, b \in G\} = Z(G)$, by the first isomorphism theorem for groups we have $G/Z(G) \cong \mathrm{Inn}(G)$. □

Exercise 2.9.10. Let G be a group such that $G/Z(G)$ is cyclic. Show that $\mathrm{Inn}(G)$ is a trivial subgroup of $\mathrm{Aut}(G)$.

Theorem 2.9.11 (Second Isomorphism Theorem)**.** *Let G be a group. Let H and K be subgroups of G with K normal in G. Then*

(i) HK is a subgroup of G,

(ii) K is a normal subgroup of HK, and

(iii) $H/(H \cap K) \cong HK/K$.

Proof. (i) Let $h \in H$ and $k \in K$ be arbitrary. Since K is a normal subgroup of G, we have $hk = (hkh^{-1})h \in KH$ and so $HK \subseteq KH$. Similarly, $kh = h(h^{-1}kh) \in HK$ shows that $KH \subseteq HK$. Thus $HK = KH$ and hence HK is a subgroup of G by Theorem 2.4.3.

(ii) Clearly K is a subgroup of HK. Since K is normal in G, given any $a \in HK \subseteq G$ and $k \in K$ we have $aka^{-1} \in K$, and hence K is a normal subgroup of HK.

(iii) Define a map $\varphi : H \to HK/K$ by $\varphi(a) = aK$, for all $a \in H$. Since $\varphi(ab) = (ab)K = (aK)(bK) = \varphi(a)\varphi(b)$, for all $a, b \in H$, φ is a group homomorphism. Since $K \in HK/K$ is the neutral element, given any $h \in H$ and $k \in K$ we have $(hk)K = (hK)(kK) = hK = \varphi(h)$, and so φ is surjective. Since

$$\mathrm{Ker}(\varphi) = \{h \in H : hK = K\} = \{h \in H : h \in K\} = H \cap K,$$

by first isomorphism theorem (see Corollary 2.9.2) we have $H/(H \cap K) \cong HK/K$. □

Example 2.9.12. Let $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$. Consider the subgroups $H = m\mathbb{Z}$ and $K = n\mathbb{Z}$ of $(\mathbb{Z}, +)$. Since $\mathbb{Z}$ is abelian, K is a normal subgroup of $\mathbb{Z}$. Since $\gcd(m, n) = 1$, there exists $a, b \in \mathbb{Z}$ such that $am + bn = 1$, and so $1 \in H + K$. Since $\gcd(m, n) = 1$, we have $\mathrm{lcm}(m, n) = mn$, and so $H \cap K = mn\mathbb{Z}$. Then by the second isomorphism theorem we have $m\mathbb{Z}/mn\mathbb{Z} = H/(H \cap K) \cong (H + K)/K = \mathbb{Z}/n\mathbb{Z}$. Generalize this to the case when m and n are not necessarily coprime.

Exercise 2.9.13. Use the second isomorphism theorem for groups to prove the following.

(i) $3\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z}$, and

(ii) $6\mathbb{Z}/30\mathbb{Z} \cong 2\mathbb{Z}/10\mathbb{Z}$. (*Hint:* Take $H = 6\mathbb{Z}$ and $K = 10\mathbb{Z}$).

Theorem 2.9.14 (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 $\widetilde{f} \circ \Phi = f$.*

$$\begin{tikzcd}
G \arrow[r, "f"] \arrow[d, "\Phi"'] & H \\
G_{\mathrm{ab}} \arrow[ur, "\widetilde{f}"'] &
\end{tikzcd}$$

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 $\widetilde{\Phi} \circ g = \Phi$.

$$\begin{tikzcd}
 & G \arrow[dl, "g"'] \arrow[d, "\Phi"] \arrow[dr, "g"] & \\
K \arrow[r, "\widetilde{\Phi}"] & G_{\mathrm{ab}} \arrow[r, "\widetilde{g}"] & K
\end{tikzcd}$$

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, by universal property of quotient (see Definition 2.7.1) 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 2.9.15. *The commutator subgroup of S_n is A_n, for all $n \geq 3$.*

Proof. Since the signature map $\mathrm{sgn} : S_n \to \mu_2 = \{1, -1\}$ defined by

$$\mathrm{sgn}(\sigma) = \begin{cases} 1, & \text{if } \sigma \text{ is even,} \\ -1, & \text{if } \sigma \text{ is odd,} \end{cases}$$

is a group homomorphism (see Lemma 2.6.4), we have $\operatorname{sgn}(\sigma)^{-1} = \operatorname{sgn}(\sigma)$, for all $\sigma \in S_n$. Therefore, given $\sigma, \tau \in S_n$ we have

$$\operatorname{sgn}([\sigma,\tau]) = \operatorname{sgn}(\sigma \circ \tau \circ \sigma^{-1}\tau^{-1}) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)\operatorname{sgn}(\sigma)^{-1}\operatorname{sgn}(\tau)^{-1} = 1.$$

Therefore, $[\sigma, \tau] \in A_n$, for all $\sigma, \tau \in S_n$, and hence $[S_n, S_n] \subseteq A_n$. To show the reverse inclusion, note that A_n is generated by 3-cycles, for all $n \geq 3$ (see Exercise 2.5.24), and any 3-cycle $(i\ \ j\ \ k)$ in S_n can be written as

$$(i\ \ j\ \ k) = (i\ \ j) \circ (i\ \ k) \circ (i\ \ j)^{-1} \circ (i\ \ k)^{-1},$$

which is an element of $[S_n, S_n]$. Thus $A_n \subseteq [S_n, S_n]$. This completes the proof. □

Exercise 2.9.16. Show that the abelianization of S_n is μ_2, for all $n \geq 3$.

Theorem 2.9.17 (Third Isomorphism Theorem)**.** *Let H and K be normal subgroups of G with $K \subseteq H$. Then we have an isomorphism of groups $(G/K)/(H/K) \cong G/H$.*

Proof. Since H and K are normal subgroups of G and $K \subseteq H$, that K is a normal subgroup of H, and the associated quotient groups

(i) $\phi : G \to G/H$,

(ii) $\psi : G \to G/K$, and

(iii) $\eta : H \to H/K$

exist. Let $\iota_H : H \hookrightarrow G$ be the inclusion of H into G. Then the composite map

$$H \overset{\iota_H}{\hookrightarrow} G \xrightarrow{\psi} G/K$$

is a group homomorphism with kernel K, and hence we get an injective group homomorphism

$$H/K \hookrightarrow G/K.$$

Given $h \in H$ and $a \in G$, we have $aha^{-1} \in H$, and so $(aK)(hK)(aK)^{-1} = (ah)K \cdot a^{-1}K = (aha^{-1})K \in H/K$. Therefore, H/K is a normal subgroup of G/K, and hence the associated quotient group $\pi : G/K \to (G/K)/(H/K)$ exists. Consider the diagram

$$\begin{tikzcd} G \arrow[r, "\psi"] \arrow[d, "\phi"'] & G/K \arrow[d, "\pi"] \\ G/H \arrow[r, "\widetilde{\pi \circ \psi}"] & (G/K)/(H/K) \end{tikzcd}$$

Note that $H/K \in (G/K)/(H/K)$ is the neutral element of the group $(G/K)/(H/K)$. Moreover, the composite map $\pi \circ \psi$ is a surjective group homomorphism with kernel

$$\begin{aligned} \operatorname{Ker}(\pi \circ \psi) &= \{a \in G : \pi(\psi(a)) = e\} \\ &= \{a \in G : \pi(aK) = e\} \\ &= \{a \in G : aK(H/K) = H/K\} \\ &= \{a \in G : aK \in H/K\} \\ &= \{a \in G : a \in H\}, \quad \text{since the map } H/K \hookrightarrow G/K \text{ is injective.} \\ &= H \end{aligned}$$

Then by first isomorphism theorem (Corollary 2.9.2) applied to the group homomorphism $\pi \circ \psi$ we have the required isomorphism $G/H \cong (G/K)/(H/K)$ of groups. □

Corollary 2.9.18 (Correspondence Theorem)**.** *Let $f : G \to H$ be a surjective group homomorphism. Consider the following two sets:*

(i) $\mathcal{A}$:= the set of a subgroups of G containing $\mathrm{Ker}(f)$, and

(ii) $\mathcal{B}$:= the set of all subgroups of H.

Then there is an inclusion preserving bijective map

$$\Phi : \mathcal{A} \to \mathcal{B}$$

such that a subgroup $N \in \mathcal{A}$ of G is normal in G if and only if $\Phi(N)$ is normal in H.

Proof. Define a map $\Phi : \mathcal{A} \to \mathcal{B}$ by sending a subgroup N of G containing $\mathrm{Ker}(f)$ to its image $f(N)$. Note that $f(N)$ is a subgroup of H by Proposition 2.6.7 (i), and hence is an element of $\mathcal{B}$. Conversely, given a subgroup K of H, its preimage $f^{-1}(K)$ is a subgroup of G by Proposition 2.6.7 (ii). Since $e_H \in K$ we have $\mathrm{Ker}(f) = f^{-1}(e) \subseteq f^{-1}(K)$. Thus, $f^{-1}(K) \in \mathcal{A}$. This gives a map

$$\Psi : \mathcal{B} \to \mathcal{A},\ \ K \mapsto f^{-1}(K).$$

It remains to show that Φ and Ψ are inverse to each other. Given $N \in \mathcal{A}$, we have $(\Psi \circ \Phi)(N) = f^{-1}(f(N)) \supseteq N$. If $a \in f^{-1}(f(N))$, then $f(a) = f(b)$, for some $b \in N$. Then $f(ab^{-1}) = f(a)f(b)^{-1} = e_H$ implies $ab^{-1} \in \mathrm{Ker}(f) \subseteq N$, and so $a = (ab^{-1})b \in N$. Therefore, $(\Psi \circ \Phi)(N) = f^{-1}(f(N)) = N$, for all $N \in \mathcal{A}$, and hence $\Psi \circ \Phi = \mathrm{Id}_{\mathcal{A}}$. Conversely, given $K \in \mathcal{B}$, we have $(\Phi \circ \Psi)(K) = f(f^{-1}(K)) = K$, since f is surjective. Thus $\Phi \circ \Psi = \mathrm{Id}_{\mathcal{B}}$. This completes the proof. □

Exercise 2.9.19. Let H be a normal subgroup of a group G. Show that every subgroup of G/H is of the form K/H, for some subgroup K of G containing H.

2.10 Direct Product & Direct Sum of Groups

Definition 2.10.1. The *direct product* of a family of groups $\{G_\alpha : \alpha \in \Lambda\}$ is a pair $(G, \{\pi_\alpha\}_{\alpha \in \Lambda})$, where G is a group and $\{\pi_\alpha : G \to G_\alpha\}_{\alpha \in \Lambda}$ is a family of group homomorphisms such that given any group H and a family of group homomorphisms $\{f_\alpha : H \to G_\alpha\}_{\alpha \in \Lambda}$ there exists a **unique** group homomorphism $f : H \to G$ such that $\pi_\alpha \circ f = f_\alpha$, for all $\alpha \in \Lambda$.

Theorem 2.10.2 (Existence & Uniqueness of Product of Groups)**.** *The direct product of a family of groups exists and is unique upto a unique isomorphism in the sense that if $(G, \{g_\alpha : G \to G_\alpha\}_{\alpha \in \Lambda})$ and $(H, \{h_\alpha : H \to G_\alpha\}_{\alpha \in \Lambda})$ are direct products of the family of groups $\{G_\alpha : \alpha \in \Lambda\}$, then there exists a unique isomorphism of groups $\phi : G \to H$ such that $h_\alpha \circ \phi = g_\alpha$, for all $\alpha \in \Lambda$. We denote by $\prod\limits_{\alpha \in \Lambda} G_\alpha$ the underlying group of the direct product of the family of groups $\{G_\alpha : \alpha \in \Lambda\}$.*

Proof. Since $(G, \{g_\alpha\}_{\alpha \in \Lambda})$ is a direct product by assumption, for the test object $(H, \{h_\beta : H \to G_\beta\}_{\beta \in \Lambda})$ we have a group homomorphism $\varphi : G \to H$ such that $\pi_\alpha \circ \varphi = h_\alpha,\ \forall\, \alpha \in \Lambda$. Interchanging the roles of $(G, \{g_\alpha\}_{\alpha \in \Lambda})$ and $(H, \{h_\alpha\}_{\alpha \in \Lambda})$ we have a group homomorphism $\psi : H \to G$ such that $\pi_\alpha \circ \psi = g_\alpha,\ \forall\, \alpha \in \Lambda$. Since both $\psi \circ \varphi : G \to G$ and $\mathrm{Id}_G : G \to G$ are group homomorphisms satisfying

$$f_\alpha \circ (\psi \circ \varphi) = f_\alpha \ \text{ and } \ f_\alpha \circ \mathrm{Id}_G = f_\alpha,\ \ \forall\, \alpha \in \Lambda,$$

it follows that $\psi \circ \varphi = \mathrm{Id}_G$. Similarly, $\varphi \circ \psi = \mathrm{Id}_H$, and hence $\varphi : G \to H$ is the unique isomorphism such that $h_\alpha \circ \varphi = g_\alpha,\ \forall\, \alpha \in \Lambda$.

For a construction, let

$$\prod_{\alpha\in\Lambda} G_\alpha := \{f : \Lambda \to \coprod_{\alpha\in\Lambda} G_\alpha \mid f(\alpha) \in G_\alpha,\ \forall\, \alpha \in \Lambda\}.$$

Given $f, g \in \prod_{\alpha\in\Lambda} G_\alpha$ we define

$$fg : \Lambda \to \coprod_{\alpha\in\Lambda} G_\alpha$$

by

$$(fg)(\alpha) := f(\alpha)g(\alpha),\ \ \forall\, \alpha \in \Lambda.$$

Clearly $fg \in \prod_{\alpha\in\Lambda} G_\alpha$, and $(fg)h = f(gh)$, $\forall\, f, g, h \in \prod_{\alpha\in\Lambda} G_\alpha$. Let $e_\alpha \in G_\alpha$ be the neutral element, for all $\alpha \in \Lambda$. Then the map $e : \Lambda \to \prod_{\alpha\in\Lambda} G_\alpha$ given by $e(\alpha) = e_\alpha$, $\forall\, \alpha \in \Lambda$ satisfies $ef = fe = f$, $\forall\, f \in \prod_{\alpha\in\Lambda} G_\alpha$. Given $f \in \prod_{\alpha\in\Lambda} G_\alpha$ we define $f^{-1} \in \prod_{\alpha\in\Lambda} G_\alpha$ by $f^{-1}(\alpha) = (f_\alpha)^{-1} \in G_\alpha$, $\forall\, \alpha \in \Lambda$. Then $ff^{-1} = e = f^{-1}f$. Therefore, $\prod_{\alpha\in\Lambda} G_\alpha$ is a group. For each $\beta \in \Lambda$, we define a map $\pi_\beta : \prod_{\alpha\in\Lambda} G_\alpha \to G_\beta$ by $\pi_\beta(f) = f(\beta)$. Then π_β is a group homomorphism. Given a group H and a family $\{h_\alpha : H \to G_\alpha\}_{\alpha\in\Lambda}$ of group homomorphisms, we define a map $\psi : H \to \prod_{\alpha\in\Lambda} G_\alpha$ that sends $a \in H$ to the function $\psi_a : \Lambda \to \coprod_{\alpha\in\Lambda} G_\alpha$ defined by $\psi_a(\alpha) = h_\alpha(a)$, $\forall\, \alpha \in \Lambda$. Then it is straight forward to verify that ψ is a group homomorphism satisfying $\pi_\alpha \circ \psi = h_\alpha$, $\forall\, \alpha \in \Lambda$. $\square$

Example 2.10.3 (**External Direct Product of $G_1, \ldots, G_n$**). Let $G_1, \ldots, G_n$ be a finite family of groups, not necessarily distinct. Define a binary operation on the Cartesian product $G := G_1 \times \cdots \times G_n$ by

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) := (a_1b_1, \ldots, a_nb_n), \tag{2.10.4}$$

where $a_i, b_i \in G_i$, for all $i = 1, \ldots, n$. Given $a_i, b_i, c_i \in G_i$, for each $i \in \{1, \ldots, n\}$, we have

$$\begin{aligned}\big((a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n)\big) \cdot (c_1, \ldots, c_n) &= (a_1b_1, \ldots, a_nb_n) \cdot (c_1, \ldots, c_n)\\ &= \big((a_1b_1)c_1, \ldots, (a_nb_n)c_n\big)\\ &= \big(a_1(b_1c_1), \ldots, a_n(b_nc_n)\big)\\ &= (a_1, \ldots, a_n) \cdot \big((b_1, \ldots, b_n) \cdot (c_1, \ldots, c_n)\big)\end{aligned}$$

Therefore, the above defined binary operation on the set G is associative. Let $e_i \in G_i$ be the neutral element of G_i, for all $i \in \{1, \ldots, n\}$. Then given any $a_i \in G_i$, for each i, we have

$$(a_1, \ldots, a_n) \cdot (e_1, \ldots, e_n) = (a_1, \ldots, a_n) = (e_1, \ldots, e_n) \cdot (a_1, \ldots, a_n).$$

Since

$$(a_1, \ldots, a_n) \cdot (a_1^{-1}, \ldots, a_n^{-1}) = (e_1, \ldots, e_n) = (a_1^{-1}, \ldots, a_n^{-1}) \cdot (a_1, \ldots, a_n),$$

we conclude that $(a_1, \ldots, a_n)^{-1} = (a_1^{-1}, \ldots, a_n^{-1}) \in G$. Therefore, $G = G_1 \times \cdots \times G_n$ is a group with respect to the binary operation defined in (2.10.4).

For each $i \in \{1, \ldots, n\}$, let

$$p_i : G_1 \times \cdots \times G_n \to G_i \tag{2.10.5}$$

be the map defined by

$$p_i(a_1, \ldots, a_n) = a_i,\ \forall\, (a_1, \ldots, a_n) \in G_1 \times \cdots \times G_n. \tag{2.10.6}$$

Clearly p_i is a surjective group homomorphism (verify!). Let H be a group and let $\{f_i : H \to G_i\}_{1\leq i\leq n}$ be a family of group homomorphisms. Define a map $f : H \to G_1 \times \cdots \times G_n$ by

(2.10.7) $$f(h) = (f_1(h), \ldots, f_n(h)), \ \forall\, h \in H.$$

Then given any $a, b \in H$ we have

$$\begin{aligned} f(ab) &= (f_1(ab), \ldots, f_n(ab)) \\ &= (f_1(a)f_1(b), \ldots, f_n(a)f_n(b)) \\ &= (f_1(a), \ldots, f_n(a))(f_1(b), \ldots, f_n(b)) \\ &= f(a)f(b). \end{aligned}$$

Therefore, f is a group homomorphism. Clearly $p_i \circ f = f_i$, for all $i \in \{1, \ldots, n\}$. Suppose that $f' : H \to G_1 \times \cdots \times G_n$ is any group homomorphism such that $p_i \circ f' = f_i$, for all $i \in \{1, \ldots, n\}$. Let $h \in H$ be arbitrary. Let $f'(h) = (a_1, \ldots, a_n) \in G_1 \times \cdots \times G_n$. Then $f_i(h) = (p_i \circ f')(h) = p_i(a_1, \ldots, a_n) = a_i$, for all $i \in \{1, \ldots, n\}$, and hence $f'(h) = (a_1, \ldots, a_n) = (f_1(h), \ldots, f_n(h)) = f(h)$. Therefore, $f' = f$, and hence by universal property of product of groups (see Definition 2.10.1) we conclude that $G_1 \times \cdots \times G_n$ is a direct product of $G_1, \ldots, G_n$. The group $G_1 \times \cdots \times G_n$ is also known as the *external direct product of $G_1, \ldots, G_n$*.

Corollary 2.10.8. *The direct product of a finite family of finite groups $G_1, \ldots, G_n$ is a group of order $|G_1| \cdots |G_n|$. Moreover, $G_1 \times \cdots \times G_n$ is abelian if and only if G_i is abelian, for all $i \in I_n$.*

Exercise 2.10.9. Given any two groups G and H, show that $Z(G \times H) = Z(G) \times Z(H)$.

Proposition 2.10.10. *Let $G := G_1 \times \cdots \times G_n$ be the external direct product of the family of groups $G_1, \ldots, G_n$. For each $i \in I_n := \{1, \ldots, n\}$, let $H_i = \{(a_1, \ldots, a_n) \in G : a_j = e_j, \ \forall\, j \neq i\} \subseteq G$. Then we have the following.*

(i) H_i is a normal subgroup of G, for all $i \in I_n$.

(ii) Every element $a \in G$ can be uniquely expressed as $a = h_1 \cdots h_n$, with $h_i \in H_i$, for all $i \in I_n$.

(iii) $H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_n) = \{e\}$, for all $i \in I_n$.

(iv) $G = H_1 \cdots H_n$.

Proof. (i) Since $(e_1, \ldots, e_n) \in H_i$, so $H_i \neq \emptyset$. Let $a := (a_1, \ldots, a_n), b := (b_1, \ldots, b_n) \in H_i$. Then $a_j = e_j = b_j, \ \forall\, j \neq i$, and hence $a_j^{-1} b_j = e_j$, for all $j \neq i$. Therefore, $a^{-1}b = (a_1^{-1}b_1, \ldots, a_n^{-1}b_n) \in H_i$, and hence H_i is a subgroup of G. Let $a = (a_1, \ldots, a_n) \in G$ and $b := (b_1, \ldots, b_n) \in H_i$ be arbitrary. Then $b_j = e_j$, for all $j \neq i$, and so $a_j b_j a_j^{-1} = a_j e_j a_j^{-1} = e_j$, for all $j \neq i$. This shows that $aba^{-1} = (a_1, \ldots, a_n)(b_1, \ldots, b_n)(a_1^{-1}, \ldots, a_n^{-1}) \in H_i$. Therefore, H_i is a normal subgroup of G, for all $i \in I_n$.

(ii) Let $a \in G$ be given. Then $a = (a_1, \ldots, a_n)$, where $a_i \in G_i, \ \forall\, i \in I_n$. Let $h_i \in G$ be the element whose i-th entry is a_i and for $j \neq i$, its j-th entry is $e_j \in G_j$. In other words, $h_i := (h_{i1}, \ldots, h_{in}) \in G$, where

$$h_{ij} := \begin{cases} e_j, & \text{if} \quad j \neq i, \\ a_i, & \text{if} \quad j = i. \end{cases}$$

Then $h_i \in H_i$, for all $i \in I_n$, and $h_1 \cdots h_n = (a_1, \ldots, a_n) = a$. To show uniqueness of this expression, let $a = k_1 \cdots k_n$, where $k_i \in H_i$, for all $i \in I_n$. If $k_{ij} \in G_j$ denote the j-th entry of $k_i \in H_i$, then $k_{ij} = e_j$, for $j \neq i$. Therefore,

$$(a_1, \ldots, a_n) = a = h_1 \cdots h_n = k_1 \cdots k_n = (k_{11}, \ldots, k_{nn}).$$

Then $a_i = h_{ii}$, for all $i \in I_n$. This shows that $k_i = h_i$, for all $i \in I_n$. This proves uniqueness.

(iii) Let $a = (a_1, \ldots, a_n) \in H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_n)$. Since $a \in H_i$, we have $a_j = e_j,\ \forall\, j \neq i$. Since $a \in H_1 \cdots H_{i-1} H_{i+1} \cdots H_n$, we have

$$a = h_1 \cdots h_{i-1} h_{i+1} \cdots h_n \tag{2.10.11}$$

for some $h_j \in H_j,\ \forall\, j \neq i$. Since $h_j = (h_{1j}, \ldots, h_{nj}) \in H_j$, we have

$$h_{kj} = e_k \in G_k,\ \forall\, k \neq j.$$

If b_k denote the k-th component of the product $h_1 \cdots h_{i-1} h_{i+1} \cdots h_n$ in $G_1 \times \cdots \times G_n$, then

$$b_k = \begin{cases} e_i, & \text{if} \quad k = i, \\ h_{kk}, & \text{if} \quad k \neq i. \end{cases} \tag{2.10.12}$$

Comparing the j-th component of both sides of the equation (2.10.11), we have

$$a_j = e_j \in G_j,\ \forall\, j \in I_n.$$

(iv) It follows from (ii) that $G \subseteq H_1 \cdots H_n$. Since H_i is a subgroup of G, for all $i \in I_n$, we have $H_1 \cdots H_n \subseteq G$. Hence the result follows. □

Lemma 2.10.13. *Let G be a group. Let H, K be two normal subgroups of G such that $H \cap K = \{e\}$ Then given any $h \in H$ and $k \in K$ we have $hk = kh$. Consequently, $[H, K] = \{e\}$.*

Proof. Since H is normal in G, we have $(hk)(kh)^{-1} = h(kh^{-1}k^{-1}) \in H$. Similarly, since K is normal in G, we have $(hk)(kh)^{-1} = (hkh^{-1})k^{-1} \in K$. Therefore, $(hk)(kh)^{-1} \in H \cap K = \{e\}$, and hence $hk = kh$ in G. □

Exercise 2.10.14. Is the conclusion of the Lemma 2.10.13 still holds if we assume exactly one of H and K is normal in G?

Lemma 2.10.15. *Let G be a group. Let H and K be normal subgroups of G. Then HK is a normal subgroup of G.*

Proof. Since H and K are normal in G, it follows that HK is a subgroup of G. Let $a \in G$ and $h \in H, k \in K$ be arbitrary. Then $a(hk)a^{-1} = (aha^{-1})(aka^{-1}) \in HK$. Therefore, HK is a normal subgroup of G. □

Definition 2.10.16. Let G be a group and let $H_1, \ldots, H_n$ be normal subgroups of G. Then G is said to be an *internal direct product of $H_1, \ldots, H_n$* if every element $a \in G$ can be **uniquely** expressed as $a = h_1 \cdots h_n$ with $h_i \in H_i$, for all $i \in \{1, \ldots, n\}$.

Proposition 2.10.17. *Let $G = G_1 \times \cdots \times G_n$ be the external direct product of a finite collection of (not necessarily distinct) groups $G_1, \ldots, G_n$, and $H_i := \{(a_1, \ldots, a_n) \in G : a_j = e_j,\ \forall\, j \neq i\}$, for each $i \in I_n$. Then G is an internal direct product of $H_1, \ldots, H_n$, respectively.*

Proof. It follows from Proposition 2.10.10 (ii) that given $a \in G$ there exists $a_i \in H_i$, for each $i \in I_n$, such that $a = a_1 \cdots a_n$. To show that this expression for a is unique, let

$$a = a_1 \cdots a_n = b_1 \cdots b_n,$$

for some $a_i, b_i \in H_i,\ \forall\, i \in I_n$. Note that each H_i is a normal subgroup of G by Proposition 2.10.10 (i), and $K_i := H_1 \cdots H_{i-1} H_{i+1} \cdots H_n$ is a normal subgroups of G by Lemma 2.10.15. Moreover, $H_i \cap K_i = \{e\}$ by Proposition 2.10.10 (iii). Then using Lemma 2.10.13 we have

$$\begin{aligned} e = a^{-1}a &= (a_1 \cdots a_n)^{-1} b_1 \cdots b_n \\ &= a_n^{-1} \cdots a_1^{-1} b_1 \cdots b_n \\ &= (a_1^{-1} b_1) \cdots (a_n^{-1} b_n). \end{aligned}$$

Then for each $i \in I_n$, we have

$$b_i^{-1}a_i = (a_1^{-1}b_1)\cdots(a_{i-1}^{-1}b_{i-1})(a_{i+1}^{-1}b_{i+1})\cdots(a_n^{-1}b_n) \in H_i \cap K_i = \{e\},$$

and hence $a_i = b_i$, for all $i \in I_n$. This completes the proof. □

Theorem 2.10.18. *Let $\{H_1, \ldots, H_n\}$ be a finite collection of normal subgroups of G. Let $K_i := H_1 \cdots H_{i-1}H_{i+1}\cdots H_n$, $\forall\ i \in I_n$. Then G is an internal direct product of $H_1, \ldots, H_n$ if and only if*

(i) $G = H_1 \cdots H_n$, *and*

(ii) $H_i \cap K_i = \{e\}$, *for all* $i \in I_n$.

Moreover, in this case we have an isomorphism of groups $G \cong H_1 \times \cdots \times H_n$.

Proof. Suppose that G is an internal direct product of $H_1, \ldots, H_n$, respectively. Let $a \in G$ be given. Then for each $i \in I_n$, there exists unique $a_i \in H_i$ such that $a = a_1 \cdots a_n$. Therefore, $G \subseteq H_1 \cdots H_n$, and hence $G = H_1 \cdots H_n$. Let $a \in H_i \cap K_i$. Then $a \in H_i$ gives $a = e_1 \cdots e_{i-1}ae_{i+1}\cdots e_n$, where $e_j \in H_j$ is the neutral element of H_j, for all j. Again, $a \in K_i = H_1 \cdots H_{i-1}H_{i+1}\cdots H_n$ gives $a = a_1 \cdots a_{i-1}ea_{i+1}\cdots a_n$, where $a_j \in H_j, \forall\ j \neq i$. Then form the uniqueness of representation of a as product of elements from H_j's, we see that $a = e$. Therefore, $H_i \cap K_i = \{e\}$.

Conversely, suppose that (i) and (ii) holds. By (i) given $a \in G$, there exists $a_i \in H_i$, for each $i \in I_n$, such that $a = a_1 \cdots a_n$. Suppose that for each $i \in I_n$, there exists $b_i \in H_i$ such that $a = b_1 \cdots b_n$. Then as shown in the proof of the above Proposition, we have

$$\begin{aligned} e = a^{-1}a &= (a_1 \cdots a_n)^{-1}b_1 \cdots b_n \\ &= a_n^{-1} \cdots a_1^{-1}b_1 \cdots b_n \\ &= (a_1^{-1}b_1)\cdots(a_n^{-1}b_n). \end{aligned}$$

Then for each $i \in I_n$, we have

$$b_i^{-1}a_i = (a_1^{-1}b_1)\cdots(a_{i-1}^{-1}b_{i-1})(a_{i+1}^{-1}b_{i+1})\cdots(a_n^{-1}b_n) \in H_i \cap K_i = \{e\},$$

and hence $a_i = b_i$, for all $i \in I_n$. This completes the proof. □

Exercise 2.10.19. Let G be a finite group of order mn, where $\gcd(m, n) = 1$. If H and K are normal subgroups of G of orders m and n, respectively, show that G is isomorphic to the direct product group $H \times K$.

Corollary 2.10.20. *If $m, n \in \mathbb{Z}$ with $\gcd(m, n) = 1$, then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.*

Proposition 2.10.21 (Direct Sum of Groups). *Let $\{G_\alpha : \alpha \in \Lambda\}$ be a family of groups. Let $\iota : \bigoplus\limits_{\alpha\in\Lambda} G_\alpha \hookrightarrow \prod\limits_{\alpha\in\Lambda} G_\alpha$ be a subset such that $\pi_\alpha \circ \iota = c_{e_\alpha}$, for all but finitely many $\alpha \in \Lambda$, where c_{e_α} is the constant map sending all elements to the neutral element $e_\alpha \in G_\alpha$, for all $\alpha \in \Lambda$. Then $\bigoplus\limits_{\alpha\in\Lambda} G_\alpha$ is a subgroup of $\prod\limits_{\alpha\in\Lambda} G_\alpha$, called the direct sum of the family of groups $\{G_\alpha : \alpha \in \Lambda\}$.*

Exercise 2.10.22. Let G and H be cyclic groups of prime order p generated by $x \in G$ and $y \in H$, respectively. Show that $G \times H$ is an abelian group of order p^2 that is not cyclic. Show that

$$\langle x \rangle,\ \langle xy \rangle,\ \langle xy^2 \rangle, \ldots, \langle xy^{p-1} \rangle \text{ and } \langle y \rangle$$

are all possible distinct subgroups of $G \times H$ of order p.

Exercise 2.10.23. Find the number of distinct subgroups of order p of the cyclic group $\mathbb{Z}_{p^n}$, where $p > 0$ is a prime number and $n \in \mathbb{N}$.

2.11 Group Action

Let G be a group and let X be a non-empty set.

Definition 2.11.1. A *left G-action* on 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) $\sigma(b, \sigma(a, x)) = \sigma(ba, x), \ \forall\, a, b \in G, \ x \in X$.

For notational simplicity, we write ax for $\sigma(a, x)$.

Remark 2.11.2. We can define a *right G-action* on X to be a map

$$\tau : X \times G \to X$$

satisfying the following conditions:

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

(ii) $\tau(\tau(x, a), b) = \tau(x, ab), \ \forall\, a, b \in G, \ x \in X$.

For notational simplicity, we write xa for $\tau(a, x)$.

Example 2.11.3. (i) Given a group G and a non-empty set X, the map

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

defined by

$$\sigma(a, x) = x, \ \forall\, a \in G \text{ and } x \in X,$$

is a left G-action on X, known as the *trivial left G-action on X*. Similarly, we have a trivial right G-action $\tau : X \times G \to X$ on X that sends $(x, a) \in X \times G$ to $x \in X$.

(ii) For each integer $n \geq 2$, the group S_n acts on the set $I_n := \{k \in \mathbb{N} : 1 \leq k \leq n\}$ by sending $(\sigma, i) \in S_n \times I_n$ to $\sigma(i) \in I_n$. Clearly for $\sigma = e \in S_n$ we have $\sigma(i) = i, \ \forall\, i \in I_n$, and $(\sigma\tau)(i) = \sigma(\tau(i)), \ \forall\, i \in I_n, \ \sigma, \tau \in S_n$.

(iii) Given a non-empty set X, let $S(X)$ be the group of all symmetries on X; its elements are bijective maps from X onto itself, and the group operation is given by composition of maps. Then the group $S(X)$ acts on X from the left.

(iv) Let H be a normal subgroup of a group G. For example, $H = Z(G)$. Then the map $\varphi : G \times H \to H$ defined by

$$\varphi(a, h) = aha^{-1}, \ \forall\, a \in G, \ h \in H,$$

is a G-action on H. Indeed, $\varphi(e, h) = ehe^{-1} = h, \ \forall\, h \in H$, and

$$\varphi(a, \varphi(b, h)) = \varphi(a, bhb^{-1}) = a(bhb^{-1})a^{-1} = (ab)h(ab)^{-1} = \varphi(ab, h), \ \forall\, a, b \in G, \ h \in H.$$

Lemma 2.11.4. *Given a group G and a non-empty set X, there is a one-to-one correspondence between the set of all left G-actions on X and the set of all group homomorphisms from G into the symmetric group $S(X)$ on X.*

Proof. Let $\mathscr{A}$ be the set of all left G-actions on X, and let $\mathscr{B} := \mathcal{H}om(G, S(X))$ be the set of all group homomorphisms from G into $S(X)$. Define a map $\Phi : \mathscr{A} \to \mathscr{B}$ by sending a left G-action $\sigma : G \times X \to X$ to the map

$$f_\sigma : G \to S(X) \tag{2.11.5}$$

that sends $a \in G$ to the map

$$f_\sigma(a) : X \to X,\ x \mapsto \sigma(a, x). \tag{2.11.6}$$

We first show that $f_\sigma(a)$ is bijective and hence is an element of $\in S(X)$. Let $x, y \in X$ be such that $\sigma(a, x) = \sigma(a, y)$. Then we have

$$\begin{aligned} x = \sigma(e, x) &= \sigma(a^{-1}, \sigma(a, x)) \\ &= \sigma(a^{-1}, \sigma(a, y)) \\ &= \sigma(e, y) = y. \end{aligned}$$

Therefore, $f_\sigma(a)$ is injective. Given $y \in X$, note that $x := \sigma(a^{-1}, y) \in X$, and that

$$f_\sigma(a)(x) = \sigma(a, x) = \sigma(a, \sigma(a^{-1}, y)) = \sigma(e, y) = y.$$

This shows that σ_a is surjective. Therefore, $f_\sigma(a) \in S(X)$, for all $a \in G$. To show $f_\sigma : G \to S(X)$ is a group homomorphism, note that given $a, b \in G$ we have

$$\begin{aligned} f_\sigma(ab)(x) = \sigma(ab, x) &= \sigma(a, \sigma(b, x)) \\ &= f_\sigma(a)(f_\sigma(b)(x)) \\ &= (f_\sigma(a) \circ f_\sigma(b))(x),\ \forall\, x \in X, \end{aligned}$$

and hence $f_\sigma(ab) = f_\sigma(a) \circ f_\sigma(b),\ \forall\, a, b \in G$. Therefore, f_σ is a group homomorphism, known as the *permutation representation* of G associated to the left G-action σ on X. Thus, $f_\sigma \in \mathscr{B}$.

Given a group homomorphism $f : G \to S(X)$, consider the map $\sigma_f : G \times X \to X$ defined by

$$\sigma_f(a, x) = f(a)(x),\ \forall\, a \in G, x \in X.$$

We show that σ_f is a left G-action on X. Since $f : G \to S(X)$ is a group homomorphism, $f(e) = \mathrm{Id}_X$ in $S(X)$. Therefore, $\sigma_f(e, x) = f(e)(x) = x,\ \forall\, x \in X$. Since $f : G \to S(X)$ is a group homomorphism, given $a, b \in G$ we have $f(ab) = f(a) \circ f(b)$, and hence given any $x \in X$ we have

$$\begin{aligned} f(ab)(x) &= (f(a) \circ f(b))\,(x) \\ \Rightarrow \sigma_f(ab, x) &= f(a)(\sigma_f(b, x)) \\ \Rightarrow \sigma_f(ab, x) &= \sigma_f(a, \sigma_f(b, x)). \end{aligned}$$

Therefore, σ_f is a left G-action on X. Thus we get a map $\Psi : \mathscr{B} \to \mathscr{A}$ defined by

$$\Psi(f) = \sigma_f,\ \forall\, f \in \mathscr{B}.$$

It remains to check that $\Psi \circ \Phi = \mathrm{Id}_{\mathscr{A}}$ and $\Phi \circ \Psi = \mathrm{Id}_{\mathscr{B}}$. Given a left G-action $\tau : G \times X \to X$ on X, we have $(\Psi \circ \Phi)(\tau) = \Psi(f_\tau) = \sigma_{f_\tau}$. Since

$$\sigma_{f_\tau}(a, x) = f_\tau(a)(x) = \tau(a, x),\ \forall\, (a, x) \in G \times X,$$

we have $(\Psi \circ \Phi)(\tau) = \tau,\ \forall\, \tau \in \mathscr{A}$. Therefore, $\Psi \circ \Phi = \mathrm{Id}_{\mathscr{A}}$. Conversely, given a group homomorphism $g : G \to S(X)$, we have $(\Phi \circ \Psi)(g) = \Phi(\sigma_g) = f_{\sigma_g}$. Since $f_{\sigma_g}(a) = \sigma_g(a, -) = g(a),\ \forall\, a \in G$, we conclude that $(\Phi \circ \Psi)(g) = g,\ \forall\, g \in \mathscr{B}$. Therefore, $\Phi \circ \Psi = \mathrm{Id}_{\mathscr{B}}$. This completes the proof. □

Definition 2.11.7 (Faithful action)**.** A left G-action $\sigma : G \times X \to X$ on a non-empty set X is said to be *faithful* if $\mathrm{Ker}(f_\sigma) = \{e\}$, where $f_\sigma : G \to S(X)$ is the permutation representation of G associated to σ (see (2.11.5) and (2.11.6) in Lemma 2.11.4).

Example 2.11.8. The multiplicative group $\mathbb{R}^* := \mathbb{R}\backslash\{0\}$ acts on $V := \mathbb{R}^n$ by scalar multiplication

$$\sigma : \mathbb{R}^* \times V \to V$$

defined by

$$\sigma(t, (a_1, \ldots, a_n)) := (ta_1, \ldots, ta_n),\ \forall\, t \in \mathbb{R}^*,\ (a_1, \ldots, a_n) \in \mathbb{R}^n.$$

Note that σ is a left $\mathbb{R}^*$-action on $V = \mathbb{R}^n$. The permutation representation

$$f_\sigma : \mathbb{R}^* \to S(V)$$

associated to σ is given by sending $t \in \mathbb{R}^*$ to the map

$$f_\sigma(t) : V \to V,\ \ (a_1, \ldots, a_n) \mapsto (ta_1, \ldots, ta_n).$$

Since

$$\begin{aligned}\mathrm{Ker}(f_\sigma) &= \{t \in \mathbb{R}^* : f_\sigma(t) = \mathrm{Id}_V\}\\ &= \{t \in \mathbb{R}^* : tv = v,\ \forall\, v \in V\}\\ &= \{1\}\end{aligned}$$

is trivial, we conclude that σ is a faithful left $\mathbb{R}^*$-action on $V = \mathbb{R}^n$.

Example 2.11.9. Recall that Cayley's theorem (Theorem 2.6.21) says that any group G is isomorphic to a subgroup of the permutation group $S(G)$ on G. This can be explained using group action as follow. Consider the left translation map

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

defined by

$$\sigma(a, x) = ax,\ \forall\, a, x \in G.$$

Note that σ is a left G-action on itself, called the *left regular action of G on itself*, and the associated permutation representation $f_\sigma : G \to S(G)$ that sends $a \in G$ to the bijective map

$$f_\sigma(a) : G \to G,\ \ x \mapsto ax,$$

Then f_σ is a group homomorphism with

$$\begin{aligned}\mathrm{Ker}(f_\sigma) &= \{a \in G : f_\sigma(a) = \mathrm{Id}_G\}\\ &= \{a \in G : ax = x,\ \forall\, x \in G\}\\ &= \{e_G\}\end{aligned}$$

is trivial, and hence σ is a faithful action.

Given a left G-action $\sigma : G \times X \to X$ on X, we define a relation $\sim_\sigma$ on X by setting

(2.11.10) $$x \sim_\sigma y\ \text{ if }\ y = \sigma(a, x),\ \ \text{for some } a \in G.$$

Note that $\sim_\sigma$ is an equivalence relation on X (verify!). The $\sim_\sigma$-equivalence class of $x \in X$ is the subset

(2.11.11) $$\mathrm{Orb}_G(x) := \{\sigma(a, x) : a \in G\} \subseteq X,$$

called the *orbit* of x under the left G-action σ on X. Note that

(i) $x \in \mathrm{Orb}_G(x)$, $\forall\, x \in X$, and

(ii) given $x, y \in X$, either $\mathrm{Orb}_G(x) = \mathrm{Orb}_G(y)$ or $\mathrm{Orb}_G(x) \cap \mathrm{Orb}_G(y) = \emptyset$.

Therefore, X is a disjoint union of distinct G-orbits of elements of X. A G-action $\sigma : G \times X \to X$ is said to be *transitive* if $\mathrm{Orb}_G(x) = \mathrm{Orb}_G(y)$, for all $x, y \in X$. Therefore, σ is transitive if and only if given any two elements $x, y \in X$, there exists $a \in G$ such that $\sigma(a, x) = y$.

Proposition 2.11.12. *Let $\sigma : G \times X \to X$ be a left G-action on X. For each $x \in X$ the subset*

$$G_x := \{a \in G : \sigma(a, x) = x\}$$

is a subgroup of G, called the stabilizer or the isotropy subgroup of x.

Proof. Since $\sigma(e, x) = x$, $e \in G_x$. Let $a, b \in G_x$ be arbitrary. Then $x = \sigma(a, x)$ gives

$$\sigma(a^{-1}, x) = \sigma(a^{-1}, \sigma(a, x)) = \sigma(a^{-1}a, x) = \sigma(e, x) = x.$$

Since $\sigma(b, x) = x$, we have $\sigma(a^{-1}b, x) = \sigma(a^{-1}, \sigma(b, x)) = \sigma(a^{-1}, x) = x$. Therefore, $a^{-1}b \in G_x$. Thus G_x is a subgroup of G. □

Exercise 2.11.13. Let $\sigma : G \times X \to X$ be a left G-action on X. If $f_\sigma : G \to S(X)$ is the group homomorphism induced by σ, then show that $\mathrm{Ker}(f_\sigma) = \bigcap\limits_{x \in X} G_x$, where G_x is the isotropy subgroup of $x \in X$.

Exercise 2.11.14. Let $\sigma : G \times X \to X$ be a left G-action on X. Given $x \in X$ and $a \in G$, show that $G_y = aG_xa^{-1}$, where $y = \sigma(a, x) \in X$. Deduce that if σ is a transitive G-action on X, show that $\mathrm{Ker}(f_\sigma) = \bigcap\limits_{a \in G} aG_xa^{-1}$.

Exercise 2.11.15. Let X be a non-empty set. Let G be a subgroup of the symmetric group $S(X)$ on X. Given $\sigma \in G$ and $x \in X$ we have $\sigma G_x \sigma^{-1} = G_{\sigma(x)}$. Deduce that if G acts transitively on X, then $\bigcap\limits_{\sigma \in G} \sigma G_x \sigma^{-1} = \{e\}$.

Corollary 2.11.16 (Generalized Cayley's Theorem)**.** *Let H be a subgroup of G, and let $X = \{aH : a \in G\}$ be the set of all distinct left cosets of H in G. Let $S(X)$ be the symmetric group on the set X. Then there exists a group homomorphism $\varphi : G \to S(X)$ such that $\mathrm{Ker}(\varphi) \subseteq H$.*

Proof. Consider the map $\sigma : G \times X \to X$ defined by

$$\sigma(a, bH) = (ab)H,\ \forall\, a \in G, bH \in X.$$

If $bH = cH$, for some $b, c \in G$, then given any $a \in G$, we have $(ab)^{-1}(ac) = b^{-1}a^{-1}ac = b^{-1}c \in H$. Therefore, σ is well-defined. Note that $\sigma(e, bH) = bH$, $\forall\, bH \in X$, and $\sigma(a_1, \sigma(a_2, bH)) = \sigma(a_1, a_2bH) = (a_1a_2b)H = \sigma(a_1a_2, bH)$, for all $a_1, a_2 \in G$ and $bH \in X$. Therefore, σ is a left G-action on X. Then σ give rise to the group homomorphism

$$f_\sigma : G \to S(X)$$

that sends $a \in G$ to the map

$$\sigma(a, -) : X \to X,\ \ x \mapsto \sigma(a, x).$$

Since $\mathrm{Ker}(f_\sigma) \subseteq G_x$, for all $x \in X$ by Exercise 2.11.13, taking $x = H \in X$ we see that

$$G_H = \{a \in G : \sigma(a, H) = H\} = \{a \in G : a \in H\} = H,$$

and hence $\mathrm{Ker}(f_\sigma) \subseteq H$. □

Exercise 2.11.17. Let H be a subgroup of G, and let X be the set of all left cosets of H in X. Let $\sigma : G \times X \to X$ be the left G-action on X defined by $\sigma(a, bH) = (ab)H, \ \forall\, a, b \in G$. Show that σ is a transitive action.

Exercise 2.11.18. Let G be a group and H a subgroup of G with $[G : H] = n < \infty$. Show that there is a normal subgroup K of G with $K \subseteq H$ and $[G : K] \leq n!$.

Corollary 2.11.19 (Cayley's Theorem)**.** *Any group G is isomorphic to a subgroup of the symmetric group $S(G)$ on G.*

Proof. Take $H = \{e\}$ in Corollary 2.11.16. □

Corollary 2.11.20. *Let G be a finite group of order n. Let $p > 0$ be a smallest prime number that divides n. If H is subgroup of G with $[G : H] = p$, then H is normal in G.*

Proof. Let H be a subgroup of index p in G. Let $X := \{aH : a \in G\}$ be the set of all distinct left cosets of H in G. Then $|X| = p$. Let $f : G \to S(X)$ be the map that sends $a \in G$ to

$$f(a) : X \to X, \ \ bH \mapsto (ab)H.$$

Then f is a group homomorphism. Then $K := \mathrm{Ker}(f) \subseteq H$ by Corollary 2.11.16, and $[G : K] = [G : H] \cdot [H : K] = pk$, where $k := [H : K]$. Since $|X| = [G : H] = p$, the quotient group G/K is isomorphic to a subgroup of the symmetric group S_p by first isomorphism theorem (see Theorem 2.9.2). Then by Lagrange's theorem $pk = |G/K|$ divides $|S_p| = p!$. Then k divides $(p-1)!$. Since k is a divisor of n and p is the smallest prime divisor of n, unless $k = 1$, any prime divisor of k must be greater than or equal to p. But since k divides $(p-1)!$, any prime divisor of k is less than p. Thus we get a contradiction unless $k = 1$. Therefore, $[H : K] = k = 1$, and so $H = K = \mathrm{Ker}(f)$. Thus H is a normal subgroup of G. □

Exercise 2.11.21. Let G be a finite group of order p^n, for some prime number p and integer $n > 0$. Show that every subgroup of G of index p is normal in G. Deduce that every group of order p^2 has a normal subgroup of order p.

Exercise 2.11.22. Let G be a non-abelian group of order 6. Show that G has a non-normal subgroup of order 2. Use this to classify groups of order 6. (*Hint:* Produce a monomorphism into S_3).

Proposition 2.11.23. *Let $\sigma : G \times X \to X$ be a left G-action on X. Fix $x \in X$, and let $G/G_x = \{aG_x : a \in G\}$ be the set of all distinct left cosets of G_x in G. Then the map $\varphi : G/G_x \to \mathrm{Orb}_G(x)$ defined by $\varphi(aG_x) = \sigma(a, x), \ \forall\, a \in G$, is a well-defined bijective map. Consequently, $[G : G_x] = |\mathrm{Orb}_G(x)|$.*

Proof. Let $a, b \in G$ be such that $aG_x = bG_x$. Then $a^{-1}b \in G_x$, and so $\sigma(a^{-1}b, x) = x$. Applying $\sigma(a, -)$ both sides, we have $\sigma(b, x) = \sigma(a, \sigma(a^{-1}b, x)) = \sigma(a, x)$. Therefore, the map φ is well-defined. To show that φ is injective, suppose that $\sigma(a, x) = \sigma(b, x)$, for some $a, b \in G$. Then $\sigma(a^{-1}b, x) = \sigma(a^{-1}, \sigma(b, x)) = \sigma(a^{-1}, \sigma(a, x)) = \sigma(e, x) = x$. Therefore, $a^{-1}b \in G_x$, and hence $aG_x = bG_x$. Thus φ is injective. To show φ is surjective, note that $\sigma(a, x) = \varphi(aG_x)$, for all $a \in G$. Therefore, φ is bijective. □

Corollary 2.11.24 (Class Equation)**.** *Let $\sigma : G \times X \to X$ be a left G-action on a non-empty finite set X, and let $\mathcal{O}$ be a subset of X containing exactly one element from each G-orbits in X. Then we have*

$$|X| = \sum_{x \in \mathcal{O}} [G : G_x].$$

Proof. Since $X = \bigsqcup_{x \in \mathcal{O}} \mathrm{Orb}_G(x)$, the result follows from Proposition 2.11.23. □

Exercise 2.11.25. Let G be a group of order $2n$, where $n \geq 1$ is an odd integer. Show that G has a normal subgroup of order n.

Exercise 2.11.26. Let G be a group. Let H be a subgroup of G such that $|H| = 11$ and $[G : H] = 4$. Show that H is a normal subgroup of G.

Exercise 2.11.27. Fix $n \in \mathbb{N}$. Show that the map $\sigma : \mathrm{GL}_n(\mathbb{R}) \times \mathbb{R}^n \to \mathbb{R}^n$ defined by

$$\sigma(A, v) = Av, \ \forall\, A \in \mathrm{GL}_n(\mathbb{R}),\ v = (v_1, \ldots, v_n)^t \in \mathbb{R}^n,$$

is a left $\mathrm{GL}_n(\mathbb{R})$-action on $\mathbb{R}^n$. Is σ transitive? Find the set of all $\mathrm{GL}_n(\mathbb{R})$-orbits in $\mathbb{R}^n$.

Exercise 2.11.28. Let $\sigma : G \times G \to G$ be the left G-action on itself given by

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

If $f_\sigma : G \to S(G)$ is the permutation representation of G associated to σ, show that $\mathrm{Ker}(f_\sigma) = Z(G)$.

Theorem 2.11.29 (Burnside's Theorem)**.** *Let G be a finite group acting from the left on a non-empty finite set X. Then the number of distinct G-orbits in X is equal to*

$$\frac{1}{|G|} \sum_{a \in G} F(a),$$

where $F(a) = \#\{x \in X : ax = x\}$, the number of elements of X fixed by a.

Proof. Let $T := \{(a, x) \in G \times X : ax = x\}$. Note that $|T| = \sum\limits_{a \in G} F(a)$. Also $|T| = \sum\limits_{x \in X} |G_x|$, where G_x is the stabilizer of $x \in X$. Let $\{x_1, \ldots, x_n\}$ be the subset of X consisting of exactly one element from each of the G-orbits in X. Note that two elements x and y of X are in the same G-orbit if and only if $\mathrm{Orb}_G(x) = \mathrm{Orb}_G(y)$. Since $|G|/|G_x| = [G : G_x] = |\mathrm{Orb}_G(x)|$, we conclude that $|G_x| = |G_y|$ whenever x and y are in the same G-orbit. Then we have

$$\begin{aligned}\sum_{a \in G} F(a) = |T| &= \sum_{x \in X} |G_x| \\ &= \sum_{i=1}^{n} |\mathrm{Orb}_G(x_i)||G_{x_i}| \\ &= \sum_{i=1}^{n} |G| = n|G|,\end{aligned}$$

and hence $n = \frac{1}{|G|} \sum\limits_{a \in G} F(a)$. This completes the proof. $\square$

2.12 Conjugacy Action & Class Equations

Let G be a group. Consider the map

(2.12.1) $$\sigma : G \times G \to G,\ (a, b) \mapsto aba^{-1}.$$

Note that σ is a left action of G on itself, known as the conjugation action. Given $x \in G$, its σ-stabilizer

$$G_x = \{a \in G : axa^{-1} = x\} = \{a \in G : ax = xa\}.$$

is a subgroup of G, called the *centralizer* or the *normalizer* of x in G. The equivalence relation $\sim_\sigma$ on G induced by the conjugation action of G on itself is known as the *conjugate* relation on G. An element $b \in G$ is said to be a *conjugate of* $a \in G$ if there exists $g \in G$ such that $b = gag^{-1}$.

Given $x \in G$, its G-orbit

$$\mathrm{Orb}_G(x) = \{gxg^{-1} : g \in G\} \tag{2.12.2}$$

consists of all conjugates of x in G.

More generally, G acts on its power set $X := \mathcal{P}(G)$ by conjugation:

$$\sigma : G \times \mathcal{P}(G) \to \mathcal{P}(G),\ \ (a, S) \mapsto aSa^{-1}, \tag{2.12.3}$$

where

$$aSa^{-1} := \begin{cases} \{aga^{-1} \in G : g \in S\}, & \text{if} \quad S \neq \emptyset, \text{ and} \\ \emptyset, & \text{if} \quad S = \emptyset. \end{cases}$$

Two non-empty subset S and T of G are said to be conjugates if there exists $a \in G$ such that $T = aSa^{-1}$. Given a subset $S \subseteq G$, its stabilizer

$$N_G(S) := \{a \in G : aSa^{-1} = S\} \tag{2.12.4}$$

for the conjugation action in (2.12.3), is a subgroup of G, known as the *normalizer* of S in G. Then we have the following.

Corollary 2.12.5. *Let S be a non-empty subset of G. Then the number of distinct conjugates of S in G is the index $[G : N_G(S)]$. In particular, the number of distinct conjugates of an element $a \in G$ is $[G : C_G(a)]$, where $C_G(a)$ is the centralizer of a in G.*

Proof. Follows from Proposition 2.11.23. □

Note that given $a \in G$ we have $C_G(a) = G$ if and only if $a \in Z(G)$. Therefore, we have the following.

Theorem 2.12.6 (Class Equation)**.** *Let G be a finite group, and let $\{a_1, \ldots, a_n\}$ be the subset of G consisting of exactly one element from each conjugacy class that are not contained in $Z(G)$. Then we have*

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

Proof. Follows from Corollary 2.11.24 by taking $X = G$ and σ to be the conjugation action of G on itself. □

Corollary 2.12.7. *Let G be a group of order p^n, where $p > 0$ is a prime number and $n \in \mathbb{N}$. Then G has non-trivial center.*

Proof. The class equation (see Theorem 2.12.6) for the conjugacy action of G on itself gives

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

where $\{a_1, \ldots, a_n\}$ is a subset consisting of exactly one element from each conjugacy class that are not in the center $Z(G)$. Since $C_G(a_i)$ is a subgroup of G, by Lagrange's theorem $|C_G(a_i)|$ divides $|G| = p^n$, and hence its index $[G : C_G(a_i)] = |G|/|C_G(a_i)|$ is of the form p^{n_i}, for some $n_i \in \mathbb{N} \cup \{0\}$. Since $a_i \notin Z(G)$, we have $C_G(a_i) \neq G$, and so $n_i \geq 1$, for all i. Since $Z(G)$ is a subgroup of G, we have $|Z(G)| \geq 1$. Then by above class equation we see that $|Z(G)| = p^n - \sum\limits_{i=1}^{r} p^{n_i}$ is divisible by p. Therefore, $Z(G) \neq \{e\}$. □

Corollary 2.12.8. *Let G be a group of order p^2, where $p > 0$ is a prime number. Then G is isomorphic to either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Proof. Since $Z(G) \neq \{e\}$ by Corollary 2.12.7, we see that $G/Z(G)$ has order p or 1, and hence is cyclic. Then G is abelian by Exercise 2.8.21. If G has an element of order p^2, then G is cyclic. Suppose that G has no element of order p^2. Then every non-neutral element of G has order p. Fix an $a \in G \setminus \{e\}$, and take $b \in G \setminus \langle a \rangle$. Then we have $|\langle a, b\rangle| > |\langle a \rangle| = p$, and hence $\langle a, b\rangle = G$. Since both a and b has order p, it follows that $\langle a \rangle \times \langle b \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Note that both $H := \langle a \rangle$ and $K := \langle b \rangle$ are normal subgroups of G of order p. Since $H \cap K$ is a subgroup of both H and K, $|H \cap K|$ is either p or 1 by Lagrange's theorem (Theorem 2.7.5). If $|H \cap K| = p$, then $K = H \cap K = H$, which contradicts the choice of $b \in G \setminus H$. Therefore, $H \cap K = \{e\}$. Since HK is a subgroup of G by Theorem 2.4.3 with

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = p^2 = |G|$$

by Lemma 2.4.7, we have $G = HK$. Then $G \cong H \times K$ by Theorem 2.10.18. □

Proposition 2.12.9. *Let G be a finite abelian group of order $n \geq 2$. If $p > 0$ is a prime number dividing n, then G has an element of order p.*

Proof. We prove this by induction on $n = |G|$. The case $n = 2$ is trivial. Assume that $n > 2$, and the result holds for any abelian group of order r with $2 \leq r < n$. Let $a \in G \setminus \{e\}$ be given. If $\langle a \rangle = G$, then we are done by Proposition 2.3.14. Assume that $H := \langle a \rangle$ is a proper non-trivial subgroup of G. Let $m := \operatorname{ord}(a)$. Then $1 < m < n$. If $p \mid m$, then by induction hypothesis H has an element, say b, of order p, and we are done. Assume that $p \nmid m$. Since G is abelian, H is a normal subgroup of G. Then p divides the order of the quotient group G/H. Since $|G/H| = n/m < n$, by induction hypothesis G/H has an element, say $bH \in G/H$, of order p. Then $b^pH = (bH)^p = H$ in G/H, and so $b^p \in H$. Since $H = \langle a \rangle$ is a cyclic group of order m, we have $(b^m)^p = (b^p)^m = e$. Then $\operatorname{ord}(b^m) \mid p$. Since p is a prime number, either $b^m = e$ or $\operatorname{ord}(b^m) = p$. If $b^m = e$, then $(bH)^m = b^mH = eH = H$, and so $p = \operatorname{ord}(bH) \mid m$. This contradicts our assumption that $p \nmid m$. Therefore, $b^m \neq e$, and hence $\operatorname{ord}(b^m) = p$. □

Theorem 2.12.10 (Cauchy). *Let G be a finite group of order n. Then for each prime number $p > 0$ dividing n, G has an element of order p.*

Proof. Fix a prime number $p > 0$ that divides n. The case $n = 2$ is trivial. Suppose that $n > 2$, and the statement holds for any finite group of order r with $2 \leq r < n$. The class equation for G associated to the conjugacy action of G on itself is given by

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(a_i)], \tag{2.12.11}$$

where $\{a_1, \ldots, a_r\}$ is the subset of G consisting of exactly one element from each G-orbits of that does not intersect $Z(G)$. Since $a \in Z(G)$ if and only if $C_G(a) = G$, we see that $|C_G(a_i)| < n$, for all $i \in \{1, \ldots, r\}$. If $p \mid |C_G(a_i)|$, for some $i \in \{1, \ldots, r\}$, then by induction hypothesis $C_G(a_i) \subseteq G$ has an element of order p, and we are done. Suppose that $p \nmid |C_G(a_i)|$, $\forall\, i \in \{1, \ldots, r\}$. Since $p \mid n = |G|$ and $|G| = |C_G(a_i)|[G : C_G(a_i)]$, we see that $p \mid [G : C_G(a_i)]$, $\forall\, i \in \{1, \ldots, r\}$. Since $Z(G)$ is a subgroup of G, $|Z(G)| \geq 1$. Then from class equation above, we see that p divides $|Z(G)|$. Since $Z(G)$ is abelian, it contains an element of order p by Proposition 2.12.9. This completes the proof. □

As an immediate corollary, we have the following result, known as the *converse of Lagrange's theorem for finite abelian groups*.

Corollary 2.12.12. *Let G be a finite abelian group of order n. Let $m > 0$ be an integer that divides n. Then G has a subgroup of order m.*

Proof. The cases $n = 2$ and $m = 1$ are trivial. So we assume that $m > 1$ and $n > 2$, and we prove it by induction on n. Suppose that the statement holds for any finite abelian group of order r with $2 \leq r < n$. Let G be an abelian group of order n. Since $m > 1$, there is a prime number, say $p \in \mathbb{N}$, such that $p \mid m$. Then $m = pk$, for some $k \in \mathbb{N}$. Then by Cauchy's theorem (Theorem 2.12.10) G has a subgroup, say H, of order p. Since G is abelian, that H is normal in G. Then the quotient group G/H exists and we have $1 \leq |G/H| = n/p < n$. Since $m \mid n$, we have $n = m\ell$, for some $\ell \in \mathbb{N}$. Then

$$|G/H| = \frac{n}{p} = \frac{m\ell}{p} = \frac{pk\ell}{p} = k\ell.$$

Since G/H is abelian group with $|G/H| < n$ and $k \mid |G/H$, by induction hypothesis G/H has a subgroup, say S, of order k. Now $S = K/H$, for some subgroup K of G containing H by Exercise 2.9.19. Since $|K| = |S| \cdot |H| = kp = m$, that K is a required subgroup of G of order m. This completes the proof. □

2.13 Simple Groups

2.13.1 Simplicity of A_n, $n \geq 5$

2.14 Sylow's Theorems

2.14.1 Groups of small orders

2.15 Semi-direct product

Let H and K be groups. We say that *K acts on H by automorphisms* if there is a group homomorphism $f : K \to \mathrm{Aut}(H)$, where $\mathrm{Aut}(H)$ is the group of all automorphisms of H. To simplify the notation, we denote by f_k the automorphism $f(k) \in \mathrm{Aut}(H)$.

On the Cartesian product $H \times K$ of H with K, we define a binary operation by setting

$$(h_1, k_1) \cdot (h_2, k_2) := (h_1 f_{k_1}(h_2), k_1 k_2), \quad \forall\, (h_1, k_1), (h_2, k_2) \in H \times K. \tag{2.15.1}$$

Note that if f is the trivial homomorphism, then $f_k(h) = h$, $\forall\, h \in H, k \in K$, and in that case the above binary operation become the component-wise binary operation on the direct product group $H \times K$. For notational simplicity, we denote by $k_1 \cdot h_2$ the element $f_{k_1}(h_2) \in H$ whenever there is no ambiguity with the homomorphism f. Given $(h_1, k_1), (h_2, k_2), (h_3, k_3) \in H \times K$, we have

$$\begin{aligned}
((h_1, k_1)(h_2, k_2))\,(h_3, k_3) &= (h_1 f_{k_1}(h_2), k_1 k_2)(h_3, k_3) \\
&= (h_1 f_{k_1}(h_2) f_{k_1 k_2}(h_3), (k_1 k_2) k_3) \\
&= (h_1 f_{k_1}(h_2) f_{k_1}(f_{k_2}(h_3)), k_1(k_2 k_3)) \\
&= (h_1 f_{k_1}(h_2 f_{k_2}(h_3)), k_1(k_2 k_3)) \\
&= (h_1, k_1)(h_2 f_{k_2}(h_3), k_2 k_3) \\
&= (h_1, k_1)\,((h_2, k_2)(h_3, k_3))\,.
\end{aligned}$$

Therefore, the binary operation on $H \times K$ defined in (2.15.1) is associative. Note that given $(h, k) \in H \times K$, we have

$$\begin{aligned} & (h,k)(e_H, e_K) = (hf_k(e_H), ke_K) = (he_H, k) = (h,k), \\ \text{and } & (e_H, e_K)(h,k) = (e_H f_{e_K}(h), e_K k) = (h,k), \end{aligned}$$

where $e_H \in H$ and $e_K \in K$ are the neutral elements of H and K, respectively. Finally, given $(h, k) \in H \times K$, we have

$$\begin{aligned} (h,k)(f_{k^{-1}}(h^{-1}), k^{-1}) &= (hf_k(f_{k^{-1}}(h^{-1})), kk^{-1}) \\ &= (h(f_k \circ f_k^{-1})(h^{-1}), e_K) \\ &= (hh^{-1}, e_K) \\ &= (e_H, e_K), \\ \text{and } (f_{k^{-1}}(h^{-1}), k^{-1})(h,k) &= (f_{k^{-1}}(h^{-1}) f_{k^{-1}}(h), k^{-1}k) \\ &= (f_{k^{-1}}(h^{-1}h), e_K) \\ &= (f_{k^{-1}}(e_H), e_K) \\ &= (e_H, e_K). \end{aligned}$$

Therefore, $(h,k)^{-1} = (f_{k^{-1}}(h^{-1}), k^{-1})$, $\forall\, (h,k) \in H \times K$. Therefore, the binary operation (2.15.1) on $H \times K$ makes it a group, called the *semidirect product of H with K along f*, and is denoted by $H \rtimes_f K$ or simply by $H \rtimes K$, if there is no confusion about f.

2.15.1 Finitely Generated Abelian Groups

2.16 Free Group

2.17 Solvable & Nilpotent Groups

2.18 Linear Groups