

---

# MA2205: Basic Algebra

## *An Introduction to 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](mailto:arjun.paul@iiserkol.ac.in).

Version: January 17, 2025 at 12:46 Noon (IST).  
Available at: [https://arjunpaul29.github.io/home/notes/Basic\\_Algebra.pdf](https://arjunpaul29.github.io/home/notes/Basic_Algebra.pdf)

*Note: This note will be updated from time to time.*  
*If you find any potential mistakes/typos, please bring it to my notice.*  
*Advice:* Red coloured *\*Theorem, \*Proposition, \*Lemma, \*Corollary, \*Exercises,*  
*\*Remarks* are generally additional materials which can be skipped.



*To my students ...*



## MA2205 (Basic Algebra) Syllabus

Groups: Definition of groups, subgroups, group homomorphisms and isomorphisms, normal subgroups, quotient groups, Lagrange's theorem, isomorphism theorems, direct sum of abelian groups, direct products, Permutation groups, group as symmetries.

Group Action: Group actions, conjugacy classes, orbits and stabilizers, class equations.

### Suggested Text Books:

1. Artin, M., *Algebra*, Prentice-Hall.
2. Dummit, D.S. and Foote, R.M., *Abstract Algebra*, Wiley.
3. Malik, D.S., Mordeson, J.M. and Sen, M.K., *Fundamentals of Abstract Algebra*, McGraw-Hill.
4. Gopalakrishnan, N.S., *University Algebra*, New Age International.
5. Herstein, I.N., *Topics in Algebra*, Wiley.
6. Hungerford, T.W., *Algebra*, Springer-Verlag.
7. Fraleigh, J.B., *A First Course in Abstract Algebra*, Narosa Publishers.



# Contents

<b>List of Symbols</b>	<b>ix</b>
<b>1 Introduction to Groups</b>	<b>1</b>
1.1 Group . . . . .	1
1.2 Subgroup . . . . .	12
1.3 Cyclic group . . . . .	17
1.4 Product of subgroups . . . . .	21
<b>2 Permutation Groups</b>	<b>25</b>
2.1 Definition and examples . . . . .	25
2.2 Cycles . . . . .	26
2.3 Even and odd permutations . . . . .	32
2.4 Alternating subgroup $A_n$ . . . . .	34
<b>3 Group Homomorphism</b>	<b>37</b>
3.1 Definition and examples . . . . .	37
3.2 Basic properties . . . . .	39
3.3 Kernel . . . . .	42
3.4 Quotient group . . . . .	44
<b>4 Quotient Groups</b>	<b>47</b>
4.1 What is a quotient by a subgroup? . . . . .	47
4.2 Left and right cosets . . . . .	48
4.3 Normal Subgroups . . . . .	52
4.4 Construction of quotient groups . . . . .	54

<b>5</b>	<b>Isomorphism Theorems</b>	<b>57</b>
5.1	First isomorphism theorem . . . . .	57
5.2	Abelianization . . . . .	60
5.3	Inner Automorphisms . . . . .	62
5.4	Second isomorphism theorem . . . . .	63
5.5	Third isomorphism theorem . . . . .	64
<b>6</b>	<b>Direct product and direct sum</b>	<b>67</b>
6.1	Direct product of groups . . . . .	67
6.2	Direct sum of abelian groups . . . . .	72
<b>7</b>	<b>Group Action</b>	<b>75</b>
7.1	Definition and examples . . . . .	75
7.2	Orbits and isotropy subgroups . . . . .	79
7.3	Class equation for conjugacy action . . . . .	84
7.4	$p$ -groups . . . . .	88
7.5	Simple Groups . . . . .	90
<b>8</b>	<b>Miscellaneous Exercises</b>	<b>95</b>



# 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 exist
$\forall$	For all
$\in$	Belongs to
$\notin$	Does not belong to
$\sum$	Sum
$\prod$	Product
$\pm$	Plus and minus
$\infty$	Infinity
$\sqrt{a}$	Square root of $a$
$\cup$	Union
$\sqcup$	Disjoint union
$\cap$	Intersection
$A \rightarrow B$	$A$ mapping into $B$
$a \mapsto b$	$a$ maps to $b$
$\hookrightarrow$	Inclusion map
$A \setminus B$	$A$ setminus $B$
$\cong$	Isomorphic to
$A := \dots$	$A$ is defined to be ...
$a \mid b$	$a$ divides $b$
$\square$	End of a proof

Symbol	Name	Symbol	Name
$\alpha$	alpha	$\beta$	beta
$\gamma$	gamma	$\delta$	delta
$\pi$	pi	$\phi$	phi
$\varphi$	var-phi	$\psi$	psi
$\epsilon$	epsilon	$\varepsilon$	var-epsilon
$\zeta$	zeta	$\eta$	eta
$\theta$	theta	$\iota$	iota
$\kappa$	kappa	$\lambda$	lambda
$\mu$	mu	$\nu$	nu
$\upsilon$	upsilon	$\rho$	rho
$\varrho$	var-rho	$\xi$	xi
$\sigma$	sigma	$\tau$	tau
$\chi$	chi	$\omega$	omega
$\Omega$	Capital omega	$\Gamma$	Capital gamma
$\Theta$	Capital theta	$\Delta$	Capital delta
$\Lambda$	Capital lambda	$\Xi$	Capital xi
$\Sigma$	Capital sigma	$\Pi$	Capital pi
$\Phi$	Capital phi	$\Psi$	Capital psi

Some of the useful Greek alphabets

# Chapter 1

## Introduction to Groups

### 1.1 Group

Let  $G$  be a non-empty set. A *law of composition* or a *binary operation* on  $G$  is a map  $*$  :  $G \times G \rightarrow G$ ; for given  $(a, b) \in G \times G$  its image under the map  $*$  is denoted by  $a * b$ . A *group* is a non-empty set  $G$  equipped with a law of composition such that all elements of  $G$  has an inverse. The precise definition is given below.

**Definition 1.1.1.** 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  $a * b = e = b * a$ .

**\*Remark 1.1.1.** A *semigroup* is a pair  $(G, *)$  consisting of a non-empty set  $G$  together with an associative binary operation  $*$  :  $G \times G \rightarrow G$  (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.

**Notation 1.1.1.** A group  $(G, *)$  is said to be *finite* or *infinite* according as its underlying set  $G$  is finite or infinite; the cardinality<sup>1</sup> of  $G$  is called the *order* of the group  $(G, *)$ , and we denote it by the symbol  $|G|$ . For notational simplicity,

---

<sup>1</sup>The cardinality of a finite set is the number of elements in it.

we write  $ab$  to mean  $a * b$ , for all  $a, b \in G$ . When there is no confusion likely to arise, we simply denote a group  $(G, *)$  by  $G$  without specifying the binary operation.

**Example 1.1.1.** The set of all integers

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

admits a binary operation, namely the *addition* of integers:

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

This binary operation has the following basic properties:

- (i) *Associativity*:  $a + (b + c) = (a + b) + c$ ,  $\forall a, b, c \in \mathbb{Z}$ ,
- (ii) *Existence of a neutral element*: There exists a distinguished element  $0 \in \mathbb{Z}$  that satisfies

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

- (iii) *Existence of additive inverse*: For given  $a \in \mathbb{Z}$ , there exists an element  $b \in \mathbb{Z}$  (depending on  $a$ ) such that  $a + b = 0 = b + a$ ; generally, we denote this element  $b$  by  $-a$ .

**Example 1.1.2.** Fix an integer  $n \geq 1$ , and let

$$n\mathbb{Z} := \{nk : k \in \mathbb{Z}\} \subseteq \mathbb{Z}.$$

Clearly  $n\mathbb{Z}$  is a non-empty set. Let  $a, b \in n\mathbb{Z}$  be any two elements. Then  $a = nk$  and  $b = nk'$ , for some  $k, k' \in \mathbb{Z}$ . Then

$$a + b = nk + nk' = n(k + k') \in n\mathbb{Z}.$$

Thus, the usual addition of integers defines a binary operation on  $n\mathbb{Z}$ . Since

$$\begin{aligned} (nk_1 + nk_2) + nk_3 &= n(k_1 + k_2) + nk_3 \\ &= n((k_1 + k_2) + k_3) \\ &= n(k_1 + (k_2 + k_3)) \\ &= nk_1 + (nk_2 + nk_3), \end{aligned}$$

we see that addition is associative on  $n\mathbb{Z}$ . Clearly  $0 = n \cdot 0 \in n\mathbb{Z}$ , and it satisfies

$$0 + nk = nk \quad \text{and} \quad nk + 0 = nk, \quad \forall nk \in n\mathbb{Z}.$$

So 0 is a neutral element in  $n\mathbb{Z}$ . For given  $a \in n\mathbb{Z}$ , we have  $a = nk$ , for some  $k \in \mathbb{Z}$ . Since  $-k \in \mathbb{Z}$  and

$$nk + n(-k) = n(k + (-k)) = n \cdot 0 = 0$$

$$\text{and } n(-k) + nk = n(-k + k) = n \cdot 0 = 0,$$

we see that  $-a = n(-k) \in n\mathbb{Z}$  is an additive inverse of  $a$  in  $n\mathbb{Z}$ . Thus  $n\mathbb{Z}$  is a group with respect to the usual addition of integers.

**Example 1.1.3.** (i) The sets  $\mathbb{Q}$ ,  $\mathbb{R}$  and  $\mathbb{C}$  form groups with respect to the usual addition.

(ii) The set  $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$  of all non-zero rational numbers forms a group with respect to the usual multiplication.

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

(iv) *Circle group:* The set

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

forms a group with respect to multiplication of complex numbers.

(v) Let  $\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ . Note that  $\mathbb{Q}[\sqrt{2}] \subseteq \mathbb{R}$ , and it is closed under usual addition of real numbers (i.e., usual addition of two elements of  $\mathbb{Q}[\sqrt{2}]$  is again in  $\mathbb{Q}[\sqrt{2}]$ ). It is easy to see that  $\mathbb{Q}[\sqrt{2}]$  is a group.

**Lemma 1.1.1** (Uniqueness of neutral element). *Let  $G$  be a group. Then there is a unique element  $e \in G$  such that  $ae = a = ea$ , for all  $a \in G$ .*

*Proof.* Since  $G$  is a group, by axiom (G2) we have an element  $e \in G$  that satisfies  $ae = a$ , for all  $a \in G$ . Suppose that  $e' \in G$  be any element that plays the role of a neutral element. Then  $e'a = a$ , for all  $a \in G$ . Then putting  $a = e'$  in the first relation we have  $e'e = e'$ , and putting  $a = e$  in the second relation we have  $e'e = e$ . Thus we have  $e' = e$ .  $\square$

**Notation 1.1.2.** The unique neutral element  $e \in G$  is also known as the *identity element* of  $G$ .

**Lemma 1.1.2** (Uniqueness of inverse). *Let  $G$  be a group. For given  $a \in G$ , there exists a unique element  $b \in G$  such that  $ab = ba = e$ .*

*Proof.* Existence of such an  $b \in G$  is ensured by axiom (G3). Suppose that  $b' \in G$  be any other element that plays the role of inverse of  $a$  in  $G$ . Then composing  $b'$  from the left side of the relation  $ab = e$  we have

$$b'ab = b'$$

$$\Rightarrow eb = b'$$

$$\Rightarrow b = b'.$$

This proves uniqueness of inverse element in  $G$ .  $\square$

**Notation 1.1.3.** For given  $a \in G$ , henceforth the unique inverse element of  $a$  in  $G$  will be denoted by the symbol  $a^{-1}$ .

**\*Proposition 1.1.3.** A semigroup  $G$  is a group if and only if

- (i) there exists  $e \in G$  such that  $ae = a$ , for all  $a \in G$ , and
- (ii) for given  $a \in G$  there exists  $b \in G$  such that  $ab = e$ .

*Proof.* Suppose that  $G$  is a semigroup satisfying (i) and (ii). Let  $a \in G$  be given. By (ii) there exists  $b \in G$  such that  $ab = e$ . For this  $b$ , there exists  $c \in G$  such that  $bc = e$ . Since  $a = ae$  by (i), we have  $a = ae = a(bc) = (ab)c = ec$ , which gives  $ba = b(ec) = (be)c = bc = e$ . Therefore,  $ab = e = ba$ . Again,  $ea = (ab)a = a(ba) = ae = a = ae$ . Thus,  $e$  is a neutral element in  $G$  and that  $b$  is the inverse of  $a$  in  $G$ . Therefore,  $G$  is a group. The converse part is trivial.  $\square$

**\*Exercise 1.1.1.** Let  $G$  be a semigroup. Show that  $G$  is a group if and only if

- (i) there exists  $e \in G$  such that  $ea = a$ , for all  $a \in G$ , and
- (ii) for given  $a \in G$  there exists  $b \in G$  such that  $ba = e$ .

**Lemma 1.1.4** (Law of cancellation). Let  $G$  be a group. Let  $a, b, c \in G$  be such that  $ab = ac$ . Then  $b = c$ .

*Proof.* Composing  $a^{-1}$  from the left side of the relation  $ab = ac$  we have  $b = eb = a^{-1}ab = a^{-1}ac = ec = c$ .  $\square$

**Exercise 1.1.2.** Let  $G$  be a group. If  $a, b, c \in G$  satisfies  $ac = bc$ , show that  $a = c$ .

**Notation 1.1.4.** 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  $a^n := (a^{-1})^{-n}$ . For  $n = 0$ , we define  $a^0 := e$ , the neutral element of  $G$ .

**Exercise 1.1.3.** 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  $n \in \mathbb{Z}$ .

*Answer:* (i) Set  $b := a^{-1}$ . Since  $b^{-1}b = e = bb^{-1}$  and  $ab = e = ba$ , it follows from uniqueness of inverse element in a group that  $b^{-1} = a$ , i.e.,  $(a^{-1})^{-1} = a$ .

(ii) Since  $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e$  and  $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$ , it follows from the uniqueness of inverse element in a group that  $(ab)^{-1} = b^{-1}a^{-1}$ .

(iii)–(v): Left as exercises. □

All the examples discussed above are of infinite groups. Now we give some useful examples of finite groups. In fact, we shall see shortly that for given any integer  $n \geq 1$ , there is a group of order  $n$ .

**Example 1.1.4.** (i) *The 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 group of order 2:* 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) *The group of order 3:* The set  $G := \{e, a, b\}$  together with the binary operation  $*$  given by the following table of binary operation, is a group with three elements.

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

TABLE 1.1.0.1: A group with 3 elements

**Notation 1.1.5.** 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) *Klein's 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 table 1.1.0.2 below. Verify that  $K_4$  is a group.

(v) *The group of  $n$ -th roots of unity:* Fix an integer  $n \geq 2$ , and let  $\mu_n = \{\zeta \in \mathbb{C} : \zeta^n = 1\} \subset \mathbb{C}^*$ . Then  $\mu_n$  is a group with respect to the binary operation given by multiplication of complex numbers. Note that  $\mu_n$  is a group of order  $n$ .

*	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 1.1.0.2: Klein four group

**Example 1.1.5** (The groups  $\mathbb{Z}_n$ ). 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  $n$* . Note that  $\equiv_n$  is an equivalence relation on  $\mathbb{Z}$  (verify!). Given any  $a \in \mathbb{Z}$ , its  $\equiv_n$ -equivalence class in  $\mathbb{Z}$  is the subset

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

Observation 1.  $a \in [a]$ , for all  $a \in \mathbb{Z}$ . This is because  $a - a = 0 \in n\mathbb{Z}$ .

Observation 2. If  $b \in [a]$ , then  $[a] \subseteq [b]$ . To see this, let  $c \in [a]$  be arbitrary. Then  $c \equiv_n a$ . Again  $b \equiv_n a$  implies that  $a \equiv_n b$ . Then by transitivity of  $\equiv_n$  we have  $c \equiv_n b$ . Therefore,  $c \in [b]$ . Since  $c \in [a]$  is an arbitrary element, we have  $[a] \subseteq [b]$ .

Observation 3. If  $b \in [a]$  then  $[a] = [b]$ . Since  $a \in [a]$  by Observation 1 and since  $[a] \subseteq [b]$  by Observation 2, we conclude that  $a \in [b]$ . Then  $[b] \subseteq [a]$  by Observation 2, and hence  $[a] = [b]$ .

Consequently, for any two integers  $a, b \in \mathbb{Z}$ , either  $[a] \cap [b] = \emptyset$  or  $[a] = [b]$ .

Let

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

be the set of all  $\equiv_n$ -equivalence classes of elements of  $\mathbb{Z}$ . Let  $a, b \in \{k \in \mathbb{Z} : 0 \leq k \leq n-1\}$  with  $a \neq b$ . Then  $b - a$  is not an integer multiple of  $n$ , and so  $[b] \neq [a]$ . Thus

$$[0], [1], \dots, [n-1]$$

are  $n$  distinct elements in  $\mathbb{Z}_n$ . We claim that  $\mathbb{Z}_n = \{[k] : 0 \leq k \leq n-1\}$ . To see this, let  $a \in \mathbb{Z}$  be given. Then by division algorithm there exists a unique  $r \in \mathbb{Z}$  satisfying  $0 \leq r < n$  such that  $a = qn + r$ , for some  $q \in \mathbb{Z}$ . Then  $a - r = qn \in n\mathbb{Z}$  shows that  $a \equiv_n r$  and hence  $[a] = [r]$  in  $\mathbb{Z}_n$ . This proves our claim.



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

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

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  $[a] \in \mathbb{Z}_n$ .

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

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

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

**Example 1.1.6** (The group  $\mathbb{Z}_n^\times$ ). Continuing with the notations from the above Example 1.1.5, we now define the *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

$$\begin{aligned} ab - a'b' &= (a - a')b + a'(b - b') \\ &= nk_1b + a'nk_2 \\ &= n(k_1b + a'k_2), \end{aligned}$$

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

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

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

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

Therefore,  $[1] \in \mathbb{Z}_n$  is the multiplicative identity in  $\mathbb{Z}_n$ . Since  $n \geq 2$  by assumption,  $n$  does not divide 1 in  $\mathbb{Z}_n$ . So  $[0] \neq [1]$  in  $\mathbb{Z}_n$ . 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  $an + bk = 1$ . 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

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

Note that,  $[0] \notin \mathbb{Z}_n^\times$ , while  $[1] \in \mathbb{Z}_n^\times$ . If  $[k_1], [k_2] \in \mathbb{Z}_n^\times$ , 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,

$$[k_1] \cdot [k_2] = [k_1 k_2] \in \mathbb{Z}_n^\times, \forall [k_1], [k_2] \in \mathbb{Z}_n^\times.$$

Thus we get a well-defined binary operation on  $\mathbb{Z}_n^\times$ . Clearly this binary operation is associative, and  $[1]$  plays the role of neutral element in  $\mathbb{Z}_n^\times$ . Given  $[a] \in \mathbb{Z}_n^\times$ , since  $\gcd(a, n) = 1$ , there exists  $b, k \in \mathbb{Z}$  such that  $ab + nk = 1$ . Then  $[a][b] + [n][k] = [1]$ . Since  $[n] = [0]$  in  $\mathbb{Z}_n$ , it follows that  $[a][b] = [1]$ . Now it is easy to see that  $\mathbb{Z}_n^\times$  is an abelian group with respect to the binary operation *multiplication of integer classes modulo  $n$* .

**Definition 1.1.2.** A group  $G$  is said to be *commutative* or *abelian* if  $ab = ba$ , for all  $a, b \in G$ . A group  $G$  is said to be *non-commutative* or *non-abelian* if it is not commutative (i.e., there exists at least two elements  $a, b \in G$  such that  $ab \neq ba$ ).

Note that the examples of groups discussed above are all commutative or abelian. Now we give some examples of non-abelian groups.

**Example 1.1.7** (General linear group). Fix a natural number  $n \geq 1$ , and consider the set  $\text{GL}_n(\mathbb{R})$  of all invertible  $n \times n$  matrices with entries from  $\mathbb{R}$ . Note that  $\text{GL}_n(\mathbb{R})$  admits a natural binary operation given by matrix multiplication:

$$\cdot : \text{GL}_n(\mathbb{R}) \times \text{GL}_n(\mathbb{R}) \rightarrow \text{GL}_n(\mathbb{R}), (A, B) \mapsto AB.$$

Note that

- (i) given any  $A, B, C \in \text{GL}_n(\mathbb{R})$ , we have  $(AB)C = A(BC)$ .
- (ii) there is a distinguished element, namely the identity matrix  $I_n \in \text{GL}_n(\mathbb{R})$  which satisfies the relation  $AI_n = I_nA = A$ , for all  $A \in \text{GL}_n(\mathbb{R})$ .
- (iii) given any  $A \in \text{GL}_n(\mathbb{R})$ , there is a element  $B := A^{-1} \in \text{GL}_n(\mathbb{R})$  such that  $AB = BA = I_n$ .

Verify that  $\text{GL}_n(\mathbb{R})$  is a non-abelian group for all  $n \geq 2$ .

**Example 1.1.8** (Special linear group). Fix an integer  $n \geq 2$ , and let

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

Note that  $\text{SL}_n(\mathbb{R})$  being a subset of  $\text{GL}_n(\mathbb{R})$ , all matrices in  $\text{SL}_n(\mathbb{R})$  are invertible. Since

$$(1.1.0.1) \quad \det(AB) = \det(A) \det(B),$$

it follows that the matrix multiplication is a binary operation on the set  $\text{SL}_n(\mathbb{R})$ . Clearly matrix multiplication is associative, and the identity matrix  $I_n \in \text{SL}_n(\mathbb{R})$  plays the role of the neutral element in  $\text{SL}_n(\mathbb{R})$ . Moreover, for given  $A \in \text{SL}_n(\mathbb{R})$ , the equation (1.1.0.1) shows that  $A^{-1} \in \text{SL}_n(\mathbb{R})$ . Thus,  $\text{SL}_n(\mathbb{R})$  is a group with respect to the matrix multiplication.

**Example 1.1.9** (The symmetric group on a set). 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:

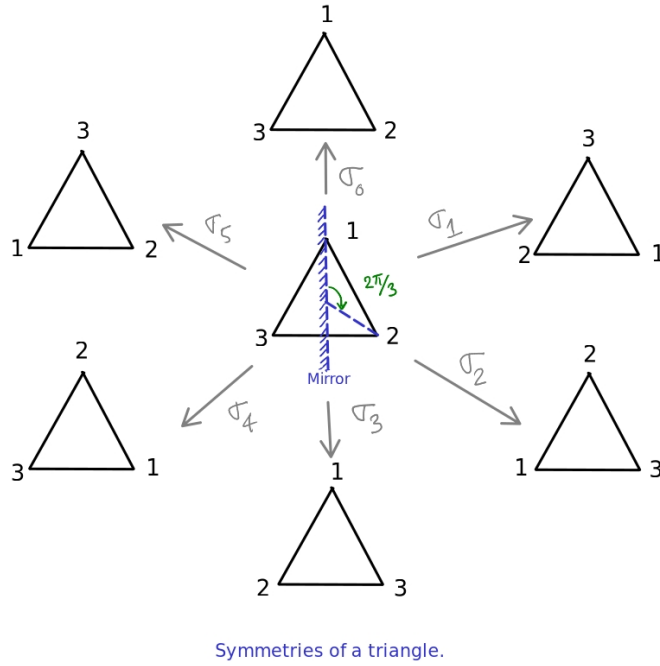
$$\circ : S(X) \times S(X) \longrightarrow S(X), \quad (f, g) \longmapsto g \circ f.$$

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  $\text{Id}_X \in S(X)$  such that  $f \circ \text{Id}_X = f = \text{Id}_X \circ f$ , 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  $f \circ g = \text{Id}_X = g \circ f$ .

Thus,  $S(X)$  is a group. We shall see in Exercise 1.1.4 that  $S(X)$  is non-commutative if  $X$  has at least three elements.

**Example 1.1.10** (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:

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

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, we get a binary operation

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

Note that  $\sigma_0$ , being the identity map of  $J_3$  onto itself, plays the role of the neutral element for the group structure on  $S_3$ .

**Exercise 1.1.4.** 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  $\sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1$ .

**Example 1.1.11.** Define a binary operation on  $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$  by *component-wise addition*:

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

Since the usual addition operation on  $\mathbb{R}$  is associative, the above binary operation on  $\mathbb{R}^2$  is associative. Indeed, for given  $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathbb{R}^2$ , we have

$$\begin{aligned} ((x_1, y_1) + (x_2, y_2)) + (x_3, y_3) &= (x_1 + x_2, y_1 + y_2) + (x_3, y_3) \\ &= ((x_1 + x_2) + x_3, (y_1 + y_2) + y_3) \\ &= (x_1 + (x_2 + x_3), y_1 + (y_2 + y_3)) \\ &= (x_1, y_1) + (x_2 + x_3, y_2 + y_3) \\ &= (x_1, y_1) + ((x_2, y_2) + (x_3, y_3)). \end{aligned}$$

The element  $(0, 0) \in \mathbb{R}^2$  plays the role of the neutral element; indeed, for all  $(x, y) \in \mathbb{R}^2$  we have

$$\begin{aligned} (x, y) + (0, 0) &= (x + 0, y + 0) = (x, y) \\ \text{and } (0, 0) + (x, y) &= (0 + x, 0 + y) = (x, y). \end{aligned}$$

For given  $(x, y) \in \mathbb{R}^2$ , the element  $(-x, -y) \in \mathbb{R}^2$  satisfies

$$\begin{aligned} (x, y) + (-x, -y) &= (x + (-x), y + (-y)) = (0, 0) \\ \text{and } (-x, -y) + (x, y) &= ((-x) + x, (-y) + y) = (0, 0). \end{aligned}$$

Thus  $(\mathbb{R}^2, +)$  is a group.

**Exercise 1.1.5.** Fix an integer  $n \geq 2$ , and let  $\mathbb{R}^n$  be the  $n$ -fold Cartesian product of  $\mathbb{R}$  with itself. Show that the component-wise addition of real numbers:

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) := (a_1 + b_1, \dots, a_n + b_n), \quad \forall a_j, b_j \in \mathbb{R},$$

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

**Exercise 1.1.6** (Direct product of a finite family of groups). Given a finite family of groups  $\{G_1, \dots, G_n\}$ , not necessarily distinct, we define a binary operation on the Cartesian product  $G := G_1 \times \dots \times G_n$  by setting

$$(a_1, \dots, a_n)(b_1, \dots, b_n) := (a_1 b_1, \dots, a_n b_n),$$

for all  $(a_1, \dots, a_n), (b_1, \dots, b_n) \in G$ .

- (i) Show that  $G$  is a group with respect to the above defined binary operation; we call  $G = G_1 \times \dots \times G_n$  the *direct product* of  $G_1, \dots, G_n$ .
- (ii) Show that  $G$  is abelian if and only if all  $G_i$ 's are abelian.

## 1.2 Subgroup

**Definition 1.2.1** (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. If  $H$  is a subgroup of  $G$ , we express it symbolically by  $H \leq G$ .

**Example 1.2.1.** (i)  $\mathbb{Z}$  is a subgroup of  $\mathbb{Q}$ .

(ii)  $\mathbb{Q}$  is a subgroup of  $\mathbb{R}$ .

(iii)  $\mathbb{R}$  is a subgroup of  $\mathbb{C}$ .

(iv)  $S^1$  is a subgroup of  $\mathbb{C}^*$ .

**Example 1.2.2.** For each integer  $n$ , let  $n\mathbb{Z} := \{nk : k \in \mathbb{Z}\}$ . We have seen in Example 1.1.2 that  $n\mathbb{Z}$  is a group with respect to the binary operation, the usual addition of integers, induced from  $\mathbb{Z}$ . Therefore,  $n\mathbb{Z}$  is a subgroup of  $\mathbb{Z}$ . We now show that any subgroup of  $\mathbb{Z}$  is of the form  $n\mathbb{Z}$ , for some  $n \in \mathbb{Z}$ . For this, let  $H$  be a subgroup of  $\mathbb{Z}$ . If  $H = \{0\}$ , then we can take  $n = 0$ . Suppose that  $H \neq \{0\}$ . Then there exists a non-zero element, say  $k \in H$ . Since  $H$  is a group,  $-k \in H$ . Since  $k \neq 0$ , exactly one of  $k$  and  $-k$  is positive. Without loss of generality, we may assume that  $k > 0$ . Then

$$H^+ := \{k \in H : k > 0\}$$

is a non-empty subset of  $\mathbb{N}$ , and so it has a least element, say  $n$ , by well-ordering principle of  $(\mathbb{N}, \leq)$ . We claim that  $H = n\mathbb{Z}$ . Since  $H$  is a group containing  $n$ , we have  $-n \in H$ . Let  $k \in \mathbb{Z}$  be given. Since

$$nk = \begin{cases} 0, & \text{if } k = 0, \\ \underbrace{n + \cdots + n}_{k\text{-times}}, & \text{if } k > 0, \\ \underbrace{(-n) + \cdots + (-n)}_{-k\text{-times}}, & \text{if } k < 0, \end{cases}$$

we conclude that  $nk \in H$ , for all  $k \in \mathbb{Z}$ . Therefore,  $n\mathbb{Z} \subseteq H$ . To see the converse, let  $h \in H$  be given. Then by division algorithm there exists  $q, r \in \mathbb{Z}$  with  $0 \leq r < n$  such that  $h = nq + r$ . Since  $h, n \in H$ , we have  $r = h - nq \in H$ . Since  $n$  is the smallest positive number in  $H$  and  $0 \leq r < n$ , we must have  $r = 0$ . Then  $h = nq \in n\mathbb{Z}$ . Thus,  $H = n\mathbb{Z}$ .

**Exercise 1.2.1.** Show that  $\{1, -1, i, -i\}$  is a subgroup of  $\mathbb{C}^*$ , where  $i = \sqrt{-1}$ .

**Example 1.2.3.** Fix an integer  $n \geq 1$ , and let

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

Since  $|\zeta| = 1$ , for all  $\zeta \in \mu_n$ , we see that  $\mu_n \subseteq S^1$ . Since  $\mu_n$  is a group with respect to the binary operation the multiplication of nonzero complex numbers (see Example 1.1.4 (v)), we see that  $\mu_n$  is a subgroup of  $S^1$ .

**Exercise 1.2.2.** Let  $H$  be a finite subgroup of the multiplicative group  $\mathbb{C}^*$ .

- (i) Show that  $H$  is a subgroup of the circle group  $S^1$ .
- (ii) If  $|H| = n$ , show that  $H = \mu_n$ .

**Exercise 1.2.3.** For each integer  $n \geq 1$ , show that there is a commutative group of order  $n$ .

**Remark 1.2.1.** 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; c.f. Example 1.1.10.

**Lemma 1.2.1.** 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 1.2.4.** Let  $G$  be a group. Show that a non-empty subset  $H \subseteq G$  forms a subgroup of  $G$  if and only if  $a^{-1}b \in H$ , for all  $a, b \in H$ .

**Exercise 1.2.5.** Let  $G$  be a group. Let  $H$  be a finite non-empty subset of  $G$ . Show that  $H$  forms a subgroup of  $G$  if and only if  $ab \in H$ , for all  $a, b \in H$ . Show by an example that this fails if  $H$  is infinite.

**Exercise 1.2.6** (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  $n \geq 2$ .

**Exercise 1.2.7.** Let  $G_1$  and  $G_2$  be two groups. Let  $H_1$  and  $H_2$  be subgroups of  $G_1$  and  $G_2$ , respectively. Consider the direct products  $G_1 \times G_2$  and  $H_1 \times H_2$ , as defined in Exercise 1.1.6. Show that  $H_1 \times H_2$  is a subgroup of  $G_1 \times G_2$ .

**Proposition 1.2.2** (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 1.2.8.** Show that a group  $G$  is commutative if and only if  $Z(G) = G$ .

**Exercise 1.2.9.** Find the center of  $S_3$ .

**\*Exercise 1.2.10.** Find the centers of  $GL_n(\mathbb{R})$  and  $SL_n(\mathbb{R})$ , for  $n \geq 2$ .

**Exercise 1.2.11 (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 1.2.3.** 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  $G$ .  $\square$

**Corollary 1.2.4.** Let  $G$  be a group and  $S$  a subset of  $G$ . Let  $\mathcal{C}_S$  be the collection of all subgroups of  $G$  that contains  $S$ . Then  $\langle S \rangle := \bigcap_{H \in \mathcal{C}_S} H$  is the smallest subgroup of  $G$  containing  $S$ .

*Proof.* By Lemma 1.2.3,  $\langle S \rangle := \bigcap_{H \in \mathcal{C}_S} H$  is a subgroup of  $G$  containing  $S$ . If  $H'$  is any subgroup of  $G$  containing  $S$ , then  $H' \in \mathcal{C}_S$ , and hence  $\langle S \rangle := \bigcap_{H \in \mathcal{C}_S} H \subseteq H'$ .  $\square$

**Exercise 1.2.12.** Recall Exercise 1.2.2, and find the subgroup  $2\mathbb{Z} \cap 3\mathbb{Z}$  of  $\mathbb{Z}$ .

**Exercise 1.2.13.** Is  $2\mathbb{Z} \cup 3\mathbb{Z}$  a subgroup of  $\mathbb{Z}$ ? Justify your answer.

**Exercise 1.2.14.** Show that a group cannot be written as a union of its two proper subgroups.

**Definition 1.2.2.** 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 1.2.15.** Let  $G$  be a group. Find the subgroup of  $G$  generated by the empty subset of  $G$ .

**Proposition 1.2.5** (Subgroup generated by a subset). *Let  $G$  be a group, and let  $S$  be a non-empty subset of  $G$ . Then*

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

*Proof.* Let

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

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 1.2.4, 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,  $K \subseteq \bigcap_{H \in \mathcal{C}_S} H = \langle S \rangle$ .  $\square$

**Definition 1.2.3.** 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 1.2.4.** (i) Any finite group is finitely generated.

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

**Exercise 1.2.16.** Let  $G$  and  $H$  be finitely generated groups. Verify if the direct product  $G \times H$  of  $G$  and  $H$ , as defined in Exercise 1.1.6, is finitely generated.

**Example 1.2.5.** 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  $a$ .

Let  $G$  be a group. An element  $a \in G$  is said to have *finite order* if there exists a positive integer  $n \in \mathbb{N}$  such that  $a^n = e$ . For example, the neutral element  $e$  in any group  $G$  has finite order because  $e^1 = e$ . If  $a \in G$  has finite order, then

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

is a non-empty subset of  $\mathbb{N}$ , and has a least element<sup>2</sup>, denoted by  $\text{ord}(a)$ . The number  $\text{ord}(a) := \inf S_a$  is called the *order of  $a$*  in  $G$ . If there exists no positive integer  $n \in \mathbb{N}$  such that  $a^n = e$ , then we say that  $a$  is of *infinite order* and in this case we express it symbolically as  $\text{ord}(a) = \infty$ .

<sup>2</sup>By well-ordering principal of  $(\mathbb{N}, \leq)$ .

**Exercise 1.2.17.** 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 1.2.18.** 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  $\text{ord}(a) \mid m$ .

(ii) Show that  $\text{ord}(a^n) = \frac{\text{ord}(a)}{\gcd(n, \text{ord}(a))}$ , 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 1.2.19.** Let  $G$  be a group, and let  $a$  and  $b$  two elements of  $G$  of finite orders with  $ab = ba$ .

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

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

**Remark 1.2.2.** If we remove the assumption that  $ab = ba$  from the above Exercise 1.2.19 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  $\text{ord}(a) = m$ ,  $\text{ord}(b) = n$  and  $\text{ord}(ab) = r$ . The proof of this surprising fact requires some advanced techniques, and may appear at the end of this course.

**Exercise 1.2.20.** Consider the matrices

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 2 \\ 1/2 & 0 \end{pmatrix}$$

in  $\text{GL}_2(\mathbb{R})$ . Show that  $\text{ord}(A) = \text{ord}(B) = 2$  while  $\text{ord}(AB) = \infty$ . Consequently, the subgroup  $\langle A, B \rangle \leq \text{GL}_2(\mathbb{R})$  generated by two order 2 elements of  $\text{GL}_2(\mathbb{R})$  is infinite.

**Exercise 1.2.21.** Let  $G$  be an abelian group. Let  $H := \{a \in G : \text{ord}(a) \text{ is finite}\}$ . Show that  $H$  is a subgroup of  $G$ .

**Exercise 1.2.22.** Show that any finite group of even order contains an element of order 2.

**Exercise 1.2.23.** Let  $G$  be a group such that any non-identity element of  $G$  has order 2. Show that  $G$  is abelian.

**Exercise 1.2.24.** Find two elements  $\sigma$  and  $\tau$  of  $S_3$  such that  $\langle \sigma, \tau \rangle = S_3$ .

**Exercise 1.2.25 (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.

**\*Exercise 1.2.26.** Fix an integer  $n \geq 3$ , and consider the group  $\mathrm{SL}_n(\mathbb{R})$ . For any pair of indices  $(i, j)$  with  $i \neq j$ , let  $E_{ij}$  be the  $n \times n$  matrix whose  $(i, j)$ -th entry is 1, and all other entries are 0. Given  $c \in \mathbb{R}$ , consider the matrix

$$A_{ij}(c) := I_n + cE_{ij},$$

where  $I_n$  is the  $n \times n$  identity matrix in  $\mathrm{SL}_n(\mathbb{R})$ .

- (i) Show that  $A_{ij}(c) \in \mathrm{SL}_n(\mathbb{R})$ , for all  $i \neq j$  and  $c \in \mathbb{R}$ .
- (ii) Compute the commutator  $[A_{ij}(c), A_{kl}(d)]$ .
- (iii) Show that  $\{A_{ij}(c) : 1 \leq i, j \leq n, i \neq j, c \in \mathbb{R}\}$  generates  $\mathrm{SL}_n(\mathbb{R})$  as a group.
- (iv) Show that  $\mathrm{SL}_n(\mathbb{R})$  is the derived subgroup of itself.

## 1.3 Cyclic group

We end this chapter by studying groups that can be generated by a single element. 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  $a^n \cdot (a^m)^{-1} = a^{n-m} \in \langle a \rangle$ . 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 1.3.1.** 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 a *generator* of  $\langle a \rangle$ .

**Remark 1.3.1.** 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  $a^{-1}$ .

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 1.3.1.** The additive group  $\mathbb{Z}_n$  in Example 1.1.5 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

$$[m] = \underbrace{[1] + \cdots + [1]}_{m\text{-times}} = m[1] \in \langle [1] \rangle \subseteq \mathbb{Z}_n.$$

Therefore,  $\mathbb{Z}_n \subseteq \langle [1] \rangle$ , and hence  $\mathbb{Z}_n = \langle [1] \rangle$ .

**Proposition 1.3.1.** 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,  $ma + (-d)n = 1$ , and hence  $\gcd(a, n) = 1$ . 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 1.3.2.** 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 1.1.4 (iv) is abelian but not cyclic (verify).

**Exercise 1.3.1.** Give an example of an infinite abelian group which is not cyclic.

**Proposition 1.3.3.** 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  $(\mathbb{N}, \leq)$  the subset  $S$  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 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  $h = a^n = a^{mq} \in \langle a^m \rangle$ . Therefore,  $H \subseteq \langle a^m \rangle$ , and hence  $H = \langle a^m \rangle$ .  $\square$

**Lemma 1.3.4.** *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 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.  $\square$

**Corollary 1.3.5.** *Let  $G = \langle a \rangle$  be a cyclic group generated by  $a \in G$ . Then  $G$  is infinite if and only if  $\text{ord}(a)$  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 1.3.4. Therefore,  $\text{ord}(a)$  is infinite. Conversely, if  $\text{ord}(a)$  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  $f : \mathbb{Z} \rightarrow G$  given by  $f(n) = a^n$ ,  $\forall n \in \mathbb{Z}$ , is injective. Therefore, since  $\mathbb{Z}$  is infinite,  $G$  must be infinite.  $\square$

**Corollary 1.3.6.** *Let  $G$  be a finite cyclic group generated by  $a$ . Then  $|G| = \text{ord}(a)$ .*

*Proof.* Since  $G$  is finite,  $\text{ord}(a)$  must be finite by Corollary 1.3.5. Suppose that  $\text{ord}(a) = n \in \mathbb{N}$ . 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  $|r-s| < n = \text{ord}(a)$ . Then all the elements in the collection  $\mathcal{C} := \{a^k : k \in \mathbb{Z} \text{ with } 0 \leq k \leq n-1\}$  are distinct, and that  $\mathcal{C}$  has  $n$  elements. Clearly  $\mathcal{C} \subseteq G$ . Given any  $b \in G = \langle a \rangle$ ,  $b = a^m$ , for some  $m \in \mathbb{Z}$ . Then by division algorithm there exist  $q, r \in \mathbb{Z}$  with  $0 \leq r < n$  such that  $m = nq + r$ . Then  $b = a^m = a^{nq+r} = (a^n)^q a^r = a^r \in \mathcal{C}$ , since  $a^n = e$ . Therefore,  $G \subseteq \mathcal{C}$ , and hence  $G = \mathcal{C}$ . Thus,  $|G| = \text{ord}(a)$ .  $\square$

**Corollary 1.3.7.** *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 1.3.6. Conversely, if  $G$  contains an element  $a$  of order  $n$ , then it follows from the proof of Corollary 1.3.6 that the cyclic subgroup  $\langle a \rangle$  of  $G$  has  $n$  elements, and hence  $\langle a \rangle = G$ .  $\square$

**Corollary 1.3.8.** *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 1.3.3, 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 1.3.4, 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.  $\square$

**Proposition 1.3.9.** *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  $\text{ord}(a) = n$  by Corollary 1.3.6. 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  $\text{ord}(a) = n$ , we see that  $d$  is the least positive integer such that  $(a^q)^d = a^{qd} = a^n = e$ . Therefore,  $\text{ord}(a^q) = d$ , and hence  $|H| = d$  by Corollary 1.3.6.

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  $K$  be any subgroups of  $G$  of order  $d$ , where  $d \mid n$ . Since  $H$  is cyclic by Proposition 1.3.3, we have  $H = \langle a^k \rangle$ , for some  $k \in \mathbb{N}$ . Since subgroup of a finite group is finite, by Corollary 1.3.5 we have  $\text{ord}(a^k) = d$ . Then  $a^{kd} = (a^k)^d = e$ . Now by division algorithm there exists unique integers  $\ell, r$  with  $0 \leq r < q$  such that  $k = \ell q + r$ . Since  $qd = n$ , we have  $kd = (\ell q + r)d = \ell n + dr$ . This gives

$$e = (a^k)^d = a^{\ell n + dr} = (a^n)^\ell a^{rd} = e \cdot a^{rd} = a^{rd}.$$

Since  $0 \leq r < q$ , we have  $0 \leq dr < dq = n$ . If  $r \neq 0$ , it would contradict the fact that  $\text{ord}(a) = n$ . Therefore, we must have  $r = 0$ , and hence

$$a^k = a^{\ell q + r} = a^{\ell q} = (a^q)^\ell \in \langle a^q \rangle = H.$$

Therefore,  $K \subseteq H$ . Since  $|H| = |K| = d$ , we have  $K = H$ .  $\square$

**Proposition 1.3.10.** *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 1.3.4 we have  $mn = 1$ . Since both  $m$  and  $n$  are integers, we must have  $m, n \in \{1, -1\}$ . Therefore,  $b \in \{a, a^{-1}\}$ .  $\square$

**Exercise 1.3.2.** 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 1.3.1.*)

**Remark 1.3.2.** The map  $\phi : \mathbb{N} \rightarrow \mathbb{N}$  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 1.3.3.** Give an example of a non-abelian group  $G$  such that all of its proper subgroups are cyclic.

**Exercise 1.3.4.** Show that a non-commutative group always has a non-trivial proper subgroup.

**Exercise 1.3.5.** Show that a group having at most two non-trivial subgroups is cyclic.

**Exercise 1.3.6.** Let  $G$  be a finite group having exactly one non-trivial subgroup. Show that  $|G| = p^2$ , for some prime number  $p$ .

**Exercise 1.3.7.** Give examples of infinite abelian groups having

- (i) exactly one element of finite order;
- (ii) all of its non-trivial elements have order 2.

**Exercise 1.3.8.** (i) Show that  $(\mathbb{Q}, +)$  is not cyclic.

(ii) Show that any finitely generated subgroup of  $(\mathbb{Q}, +)$  is cyclic.

(iii) Conclude that  $(\mathbb{Q}, +)$  is not finitely generated.

(iv) Give an example of a proper subgroup of  $(\mathbb{Q}, +)$  that is not cyclic.

## 1.4 Product of subgroups

**Definition 1.4.1.** 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 1.4.1.** Show by example that  $HK$  need not be a group in general even if both  $H$  and  $K$  are subgroups of a group.

**Theorem 1.4.1.** 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  $hk = ((hk)^{-1})^{-1} = k_1^{-1}h_1^{-1} \in KH$ . 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 1.4.2.** *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 1.4.1.** 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 1.4.2.** 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 1.4.3.** *If  $H$  and  $K$  are finite subgroups of a group  $G$ , then*

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

*Proof.* For each positive integer  $n$ , let  $J_n := \{k \in \mathbb{N} : k \leq n\}$ . Let  $H = \{h_i : i \in J_n\}$  and  $K = \{k_j : j \in J_m\}$ . Then  $HK = \{h_i k_j : i \in J_n, j \in J_m\}$ . To find the



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

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

This completes the proof.  $\square$

**Proposition 1.4.4.** *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.  $\square$



## Chapter 2

# Permutation Groups

### 2.1 Definition and examples

Let  $X$  be a non-empty set. A *permutation* on  $X$  is a bijective map  $\sigma : X \rightarrow X$ . 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  $J_n := \{1, 2, 3, \dots, n\} \subset \mathbb{N}$  we may identify  $S_X$  with  $S_n$ . An element  $\sigma \in S_n$  can be described by a *two-column notation* as follow.

$$(2.1.0.1) \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix} \quad \text{or,} \quad \sigma = \begin{cases} 1 \mapsto \sigma(1) \\ 2 \mapsto \sigma(2) \\ \vdots \\ n \mapsto \sigma(n) \end{cases}.$$

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  $J_n \rightarrow J_n$  is associative, and for any  $\sigma \in S_n$  its pre-composition and post-composition with the identity map of  $J_n$  is  $\sigma$  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 2.1.1.** 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*

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

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

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

For example,

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

**Exercise 2.1.1.** Show that  $S_1$  is a trivial group, and  $S_2$  is an abelian group with two elements.

**Lemma 2.1.1.** For all integer  $n \geq 3$ , the group  $S_n$  is non-commutative.

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

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

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.  $\square$

## 2.2 Cycles

Let  $\sigma \in S_n$  be given. Consider its two-column notation as in (2.1.0.1).

(R1) 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  $k_1, \dots, k_r$  are all distinct.

By re-indexing, if required, we can find a partition of  $\{k_1, \dots, k_r\}$  into **disjoint subsets**, say

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

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

$$(2.2.0.1) \quad \sigma(k_{i,j}) = \begin{cases} k_{i,j+1}, & \text{if } j \in \{1, \dots, r_i - 1\}, \\ k_{i,1}, & \text{if } j = r_i, \text{ and} \\ k_{ij}, & \text{if } k_{ij} \in J_n \setminus \{k_1, \dots, k_r\}. \end{cases}$$

Then  $\sigma$  can be expressed as

$$(2.2.0.2) \quad \sigma = \begin{pmatrix} k_{1,1} & \cdots & k_{1,r_1-1} & k_{1,r_1} & \cdots & k_{m,1} & \cdots & k_{m,r_m} & k_{m,r_m-1} \\ k_{1,2} & \cdots & k_{1,r_1} & k_{1,1} & \cdots & k_{m,2} & \cdots & k_{m,r_m} & k_{m,1} \end{pmatrix}.$$

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

$$(2.2.0.3) \quad \sigma = \begin{pmatrix} k_1 & k_2 & \cdots & k_{r-1} & k_r \\ k_2 & k_3 & \cdots & k_r & k_1 \end{pmatrix}.$$

Such a permutation is called a cycle.

**Definition 2.2.1 (Cycle).** An element  $\sigma \in S_n$  is called a  $r$ -cycle or a cycle of length  $r$  if there exists distinct  $r$  elements, say  $k_1, \dots, k_r \in J_n := \{1, \dots, n\}$  such that  $\sigma(k) = k$ , for all  $k \in J_n \setminus \{k_1, \dots, k_r\}$  and

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

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

**Remark 2.2.1.** Note that according to our definition 2.2.1, a cycle in  $S_n$  always have length at least 2. So we don't talk about 1-cycle as used in some of the standard text books.

With the notation above, the permutation  $\sigma$  in (2.2.0.2) can be written as a product of cycles

$$\begin{aligned}\sigma &= \begin{pmatrix} k_{1,1} & \cdots & k_{1,r_1-1} & k_{1,r_1} \\ k_{1,2} & \cdots & k_{1,r_1} & k_{1,1} \end{pmatrix} \circ \cdots \circ \begin{pmatrix} k_{m,1} & \cdots & k_{m,r_m-1} & k_{m,r_m} \\ k_{m,2} & \cdots & k_{m,r_m} & k_{m,1} \end{pmatrix} \\ &= (k_{1,1} \cdots k_{1,r_1-1} k_{1,r_1}) \circ \cdots \circ (k_{m,1} \cdots k_{m,r_m-1} k_{m,r_m})\end{aligned}$$

**Remark 2.2.2.** 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 2.2.1.** 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 2.2.1.** 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

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

It remains to show that  $(\tau\sigma\tau^{-1})(k) = k$ ,  $\forall k \in J_n \setminus \{\tau(k_1), \dots, \tau(k_r)\}$ . For this, note that  $\tau^{-1}(k) \in J_n \setminus \{k_1, \dots, k_r\}$ , 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.  $\square$

**Corollary 2.2.2.** Let  $\sigma \in S_n$  is a product of pairwise disjoint cycles  $\sigma_1, \dots, \sigma_r$  in  $S_n$ . Suppose that  $\sigma_i = (k_{i1}\ \cdots\ k_{i\ell_i}) \in S_n$ , for all  $i \in \{1, \dots, r\}$ . Then for any  $\tau \in S_n$  we have  $\tau\sigma\tau^{-1} = (\tau(k_{11})\ \cdots\ \tau(k_{1\ell_1})) \circ \cdots \circ (\tau(k_{r1})\ \cdots\ \tau(k_{r\ell_r}))$ . In particular, both  $\sigma$  and  $\tau\sigma\tau^{-1}$  have the same cycle type.

*Proof.* Since  $\tau\sigma\tau^{-1} = (\tau\sigma_1\tau^{-1}) \circ \cdots \circ (\tau\sigma_r\tau^{-1})$ , the result follows from Proposition 2.2.1.  $\square$

**Proposition 2.2.3.** Let  $\sigma \in S_n$  be a cycle. Then  $\sigma$  is a  $r$  cycle if and only if  $\text{ord}(\sigma) = r$ .

*Proof.* Let  $\sigma = (k_1\ k_2\ \cdots\ k_r)$ , for some distinct elements  $k_1, \dots, k_r \in J_n$ . Then for any  $k \in J_n \setminus \{k_1, \dots, k_r\}$  we have  $\sigma(k) = k$ . It follows from the definition of the cyclic expression of  $\sigma$  given in (2.2.0.1) that  $\sigma^i(k_1) = k_{i+1}$ , for all  $i \in$

$\{1, \dots, k-1\}$  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  $\ell \in \{1, \dots, r-1\}$ , and hence  $\sigma^r(k_i) = k_i$ , for all  $i \in \{1, \dots, r\}$ . 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  $s \in \{1, \dots, r-1\}$  (see (2.2.0.1)), we conclude that  $r$  is the smallest positive integer such that  $\sigma^r = e$  in  $S_n$ . Therefore,  $\text{ord}(\sigma) = r$ . Conversely, suppose that  $\sigma$  is a  $t$  cycle with  $\text{ord}(\sigma) = r$ . But then as shown above  $\text{ord}(\sigma) = t$ , and hence  $t = r$ .  $\square$

**Exercise 2.2.1.** Show that the number of distinct  $r$  cycles in  $S_n$  is  $\frac{n!}{r(n-r)!}$ .

*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  $\sigma = (k_1 \ k_2 \ \dots \ k_r) \in S_n$ . Note that, the cycles

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

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

$$\phi, \psi : \{2, 3, \dots, r\} \rightarrow \{2, 3, \dots, r\},$$

two  $r$  cycles (note that  $k_1$  is fixed!)

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

represents the same element of  $S_n$  if and only if  $\phi = \psi$ . Since there are  $(r-1)!$  number of distinct bijective maps  $\{2, 3, \dots, r\} \rightarrow \{2, 3, \dots, r\}$  (verify!), fixing  $k_1$  in one choice of  $r$  cycle  $(k_1 \ k_2 \ \dots \ k_r)$  in  $S_n$ , considering all permutations of the remaining  $(r-1)$  entries  $k_2, \dots, k_r$ , 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.  $\square$

**Definition 2.2.2.** Two cycles  $\sigma = (i_1 \ i_2 \ \dots \ i_r)$  and  $\tau = (j_1 \ j_2 \ \dots \ j_s)$  in  $S_n$  are said to be *disjoint* if  $\{i_1, i_2, \dots, i_r\} \cap \{j_1, j_2, \dots, j_s\} = \emptyset$ .

**Proposition 2.2.4.** If  $\sigma$  and  $\tau$  are disjoint cycles in  $S_n$ , show that  $\sigma \circ \tau = \tau \circ \sigma$ .

*Proof.* Let  $\sigma = (i_1 \ i_2 \ \dots \ i_r)$  and  $\tau = (j_1 \ j_2 \ \dots \ j_s)$  be two disjoint cycles in  $S_n$ . Let  $k \in J_n$  be arbitrary. If  $k \notin \{i_1, \dots, i_r\} \cup \{j_1, \dots, j_s\}$ , then  $\sigma(k) = k = \tau(k)$  and hence  $(\sigma\tau)(k) = (\tau\sigma)(k)$  in this case. Suppose that  $k \in \{i_1, \dots, i_r\}$ . Then

$\sigma(k) \in \{i_1, \dots, i_r\}$  and  $k \notin \{j_1, \dots, j_s\}$  together gives  $\tau\sigma(k) = \sigma(k) = \sigma\tau(k)$ . Interchanging the roles of  $\sigma$  and  $\tau$  we see that  $\tau\sigma(k) = \sigma(k) = \sigma\tau(k)$  holds for the case  $k \in \{j_1, \dots, j_s\}$ . Therefore,  $\sigma\tau = \tau\sigma$ .  $\square$

**Lemma 2.2.5.** *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

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

are all distinct, and defines an  $r$ -cycle

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

in  $S_n$ . Let  $B := J_n \setminus A$ . In cases  $\sigma|_B$  is the identity map of  $B$  onto itself or  $B = \emptyset$ , we have  $\tau = \sigma$  and so  $\sigma$  is a cycle in  $S_n$ . Assume that  $B \neq \emptyset$  and  $\pi := \sigma|_B$  is not the identity map. Then  $\pi$  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  $\pi_1, \dots, \pi_\ell$  of lengths at least 2 in  $S_k$ . Then for each  $i \in \{1, \dots, \ell\}$  we define  $\sigma_i \in S_n$  by setting

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

Then  $\sigma_1, \dots, \sigma_\ell, \tau$  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  $\sigma$  into product of disjoint cycles of lengths  $\geq 2$  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  $i \in \{1, \dots, r\}$ . Suppose that  $\sigma_i = (k_1\ k_2\ \dots\ k_t)$  with  $t \geq 2$ . Then  $\sigma(k_1) \neq k_1$ . Since  $\tau_1, \dots, \tau_r$  are pairwise disjoint cycles of lengths  $\geq 2$  in  $S_n$ , there is a unique element, say  $\delta(i) \in \{1, \dots, r\}$  such that  $\tau_{\delta(i)}(k_1) \neq k_1$ . By reordering, if required, we may write  $\tau_{\delta(i)} = (k_1\ v_2\ \dots\ v_u)$ . Then we have

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



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  $r$ .  $\square$

**Definition 2.2.3 (Cycle type).** Given  $\sigma \in S_n$ , by Lemma 2.2.5 there exists a unique finite set of pairwise disjoint cycles  $\{\sigma_1, \dots, \sigma_r\}$  in  $S_n$  such that  $\sigma = \sigma_1 \circ \dots \circ \sigma_r$ . Since disjoint cycles commutes by Proposition 2.2.4, by reindexing  $\sigma_j$ 's, if required, we may assume that  $n_1 \geq \dots \geq n_r$ , where  $n_j = \text{length}(\sigma_j)$ , for all  $j \in \{1, \dots, r\}$ . Since  $\sigma_1, \dots, \sigma_r$  are pairwise disjoint cycles in  $S_n$ , we have  $\ell + \sum_{j=1}^r n_j = n$ , for some non-negative integer  $\ell$ . If  $\ell = 0$ , then the sequence  $(n_1, \dots, n_r)$  is called the *cycle type* of  $\sigma$ , and if  $\ell > 0$ , then the sequence  $(n_1, \dots, n_r, f_1, \dots, f_\ell)$ , where  $f_1 = \dots = f_\ell = 1$ , is called the *cycle type* of  $\sigma$ .

**Example 2.2.2.** (i) The cycle type of  $\sigma := (1\ 2) \circ (3\ 6) \circ (4\ 5\ 7) \in S_7$  is  $(3, 2, 2)$ .

(ii) The cycle type of  $\tau := (1\ 4\ 3) \circ (2\ 5) \in S_7$  is  $(3, 2, 1, 1)$ .

(iii) The cycle type of  $\delta := (1\ 3\ 5) \circ (2\ 4\ 7) \in S_6$  is  $(3, 3, 1)$ .

**Definition 2.2.4.** Two permutations  $\sigma$  and  $\tau$  in  $S_n$  are said to be *conjugate* in  $S_n$  if there exists  $\delta \in S_n$  such that  $\tau = \delta \circ \sigma \circ \delta^{-1}$ .

**Theorem 2.2.6.** Two elements  $\sigma, \tau \in S_n$  are conjugate if and only if they have the same cycle type.

*Proof.* Conjugate permutations in  $S_n$  have the same cycle type by Corollary 2.2.2. Conversely suppose that  $\sigma, \tau \in S_n$  have the same cycle type, say  $(n_1, \dots, n_r, f_1, \dots, f_\ell)$ , where  $n_1 \geq \dots \geq n_r \geq 2$  and  $f_1 = \dots = f_\ell = 1$ ,  $\ell \geq 0$  and that  $\sum_{j=1}^r n_j + \ell = n$ . Let  $\sigma = \sigma_1 \circ \dots \circ \sigma_r$  and  $\tau = \tau_1 \circ \dots \circ \tau_r$ , where  $\sigma_i, \tau_j$  are cycles in  $S_n$  of lengths  $n_i$  and  $n_j$ , respectively. Suppose that  $\sigma_i = (a_{i1} \ \dots \ a_{in_i})$  and  $\tau_j = (b_{j1} \ \dots \ b_{jn_j})$ . If  $\ell > 0$ , then we write the subset  $I_n \setminus \{a_{ij} : 1 \leq i \leq r, 1 \leq j \leq n_i\}$  as  $\{a_1, \dots, a_\ell\}$ . Then  $I_n$  is a disjoint union of the subsets  $\{a_{11}, \dots, a_{1n_1}\}, \dots, \{a_{r1}, \dots, a_{rn_r}\}, \{a_1, \dots, a_\ell\}$ . Similarly if we write the subset  $I_n \setminus \{b_{ij} : 1 \leq i \leq r, 1 \leq j \leq n_i\}$  as  $\{b_1, \dots, b_\ell\}$ , then  $I_n$  is a disjoint union of the subsets  $\{b_{11}, \dots, b_{1n_1}\}, \dots, \{b_{r1}, \dots, b_{rn_r}\}, \{b_1, \dots, b_\ell\}$ . Then we define a map  $\delta : I_n \rightarrow I_n$  by sending  $a_{ij}$  to  $b_{ij}$ , for all  $(i, j) \in \{1, \dots, r\} \times \{1, \dots, n_i\}$ , and by sending  $a_k$  to  $b_k$ , for all  $k \in \{1, \dots, \ell\}$ , if  $\ell > 0$ . Clearly  $\delta$  is a bijective map, and hence is an element of  $S_n$ . Then Proposition 2.2.1 ensures that  $\delta \sigma_i \delta^{-1} = \tau_i$ , for all  $i \in \{1, \dots, r\}$ . Then we have

$$\begin{aligned} \delta \sigma \delta^{-1} &= \delta(\sigma_1 \dots \sigma_r) \delta^{-1} \\ &= (\delta \sigma_1 \delta^{-1}) \dots (\delta \sigma_r \delta^{-1}) \\ &= \tau_1 \dots \tau_r \\ &= \tau. \end{aligned}$$

This completes the proof.  $\square$

**Exercise 2.2.2.** Find the number of elements of order 2 and 3 in  $S_4$ . Show that  $S_4$  has no element of order 4.

**Corollary 2.2.7.** For  $n \geq 2$ , every element of  $S_n$  can be written as a finite product of transpositions.

*Proof.* In view of above Lemma 2.2.5 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.  $\square$

## 2.3 Even and odd permutations

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

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

**Corollary 2.3.2.** 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  $\sigma_i, \tau_j$  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 2.3.1.** A permutation  $\sigma \in S_n$  is called *even* (respectively, *odd*) if  $\sigma$  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  $\sigma_1, \dots, \sigma_r$  are 2-cycles in  $S_n$ , then by Corollary 2.3.2 we see that  $\sigma$  is even if and only if  $(-1)^r = 1$ . Thus we have a well-defined map  $\text{sgn} : S_n \rightarrow \{1, -1\}$  given by sending  $\sigma \in S_n$  to  $(-1)^r$ , where  $r$  is a number of 2-cycles appearing in the decomposition of  $\sigma$  into a product of 2-cycles in  $S_n$ . In other words,

$$(2.3.0.1) \quad \text{sgn}(\sigma) = \begin{cases} -1, & \text{if } \sigma \text{ is odd,} \\ 1, & \text{if } \sigma \text{ is even,} \end{cases}$$

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

**Proposition 2.3.3.** 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 2.3.1.** 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  $\sigma$  is a product of 5 transpositions in  $S_8$ , we conclude that  $\sigma$  is odd.

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

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

**Exercise 2.3.2.** If  $\sigma \in S_5$  has order 3, show that  $\sigma$  is a 3-cycle. More generally, if  $\sigma \in S_n$  has order  $p > 0$ , a prime number, such that  $n < 2p$ , show that  $\sigma$  is a  $p$ -cycle in  $S_n$ .

## 2.4 Alternating subgroup $A_n$

**Proposition 2.4.1.** 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  $\tau_1, \dots, \tau_{2r}$  are transpositions in  $S_n$ . Since transpositions are elements of order 2 (see Proposition 2.2.3), they are self inverse in  $S_n$ . Now it follows from Exercise 1.1.3 (ii) that

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

Therefore,  $\tau^{-1}$  is also an even permutation. Since  $\sigma$  and  $\tau^{-1}$  are even, their product  $\sigma \circ \tau^{-1} \in A_n$ . Therefore,  $A_n$  is a subgroup of  $S_n$  by Lemma 1.2.1.  $\square$

**Remark 2.4.1.** 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 2.4.1.** 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 2.3.3, 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  $\sigma$  and  $\tau$  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  $\sigma$  and  $\tau$  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.  $\square$

**Exercise 2.4.2.** Show that  $|A_n| = n!/2$ .

*Solution:* Let  $\{\sigma_1, \dots, \sigma_r\}$  and  $\{\tau_1, \dots, \tau_s\}$  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  $\pi\sigma_1, \dots, \pi\sigma_r$  are all distinct (verify) odd permutations in  $S_n$ , and hence  $r \leq s$ . Similarly  $s \leq r$ , and hence  $r = s$ , as required.  $\square$

**Exercise 2.4.3.** Determine the groups  $A_3$  and  $A_4$ .

**Exercise 2.4.4.** 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  $\sigma$  and  $\tau$*  in  $S_n$ . Deduce that  $A_n$  is generated by  $\{[\sigma, \tau] : \sigma, \tau \in S_n\}$ , for all  $n \geq 3$ .

**Exercise 2.4.5.** Show that  $S_n$  is generated by  $\{(1 \ 2), (1 \ 2 \ \dots \ n)\}$ , for all  $n \geq 3$ .

**Example 2.4.1** (Dihedral group  $D_n$ ). Consider a regular  $n$ -gon in the plane  $\mathbb{R}^2$  whose vertices are labelled as  $1, 2, 3, \dots, n$  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  $\text{ord}(a) = n$ ,  $\text{ord}(b) = 2$  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

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

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

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

Note that each element of  $D_n$  is given by a bijection of the set  $J_n := \{1, 2, \dots, n\}$  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 2.4.6 below). We can define a binary operation on  $D_n$  by composition of bijective maps. Then it is easy to check using Lemma 1.2.1 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 2.4.6.** Show that  $D_3 = S_3$ , and  $D_n$  is a proper subgroup of  $S_n$ , for all  $n \geq 4$ .

**Exercise 2.4.7.** 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.

## Chapter 3

# Group Homomorphism

### 3.1 Definition and examples

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

**Example 3.1.1.** (i) For any group  $G$ , the constant map  $c_e : G \rightarrow G$ , 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

$$\text{Id}_G : G \rightarrow G, \quad a \mapsto a$$

is a group homomorphism.

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

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

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,  $\varphi_m$  is a group homomorphism. Note that,  $\varphi_m$  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

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

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  $f : \mathbb{R} \rightarrow S^1 := \{z \in \mathbb{C}^* : |z| = 1\}$  defined by  $f(t) = e^{2\pi it}$ ,  $\forall t \in \mathbb{R}$  is a surjective group homomorphism. Is it injective?

(vi) Let

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

Verify that  $\phi$  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

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

Verify that  $\psi$  is a surjective group homomorphism.

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

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

Therefore,  $F$  is a group homomorphism, known as the *Frobenius endomorphism*.

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

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

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  $\varphi : \mathbb{Z}_m \rightarrow \mathbb{Z}_n$  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  $\varphi_a : G \rightarrow G$  defined by  $\varphi_a(b) = aba^{-1}$ ,  $\forall b \in G$ , is a group homomorphism.

**Exercise 3.1.1.** 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  $\tilde{\sigma} : J_{n+1} \rightarrow J_{n+1}$  defined by

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

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

$$f : S_n \rightarrow S_{n+1}, \quad \sigma \mapsto \tilde{\sigma},$$

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



**Lemma 3.1.1.** *Let  $n \geq 2$  be an integer. Then the map  $\text{sgn} : S_n \rightarrow \{1, -1\}$  defined by sending  $\sigma \in S_n$  to*

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

*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  $\sigma_i, \tau_j$  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  $\text{sgn}(\sigma \circ \tau) = (-1)^{r+s} = (-1)^r (-1)^s = \text{sgn}(\sigma) \text{sgn}(\tau)$ .  $\square$

## 3.2 Basic properties

**Proposition 3.2.1.** *Let  $f : G \rightarrow H$  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  $\text{ord}(a) < \infty$ , then  $\text{ord}(f(a)) \mid \text{ord}(a)$ .

*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  $n := \text{ord}(a) < \infty$ . Since  $f(a)^n = f(a^n) = f(e_G) = e_H$ , it follows from Exercise 1.2.18 (i) that  $\text{ord}(f(a)) \mid n$ .

$\square$

**Exercise 3.2.1.** Let  $G$  and  $H$  be two groups. Show that there is a unique constant group homomorphism from  $G$  to  $H$ .

**Proposition 3.2.2.** *Let  $f : G \rightarrow H$  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 3.2.1 (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 3.2.3.** *Composition of group homomorphisms is a group homomorphism.*

*Proof.* Let  $f : G_1 \rightarrow G_2$  and  $g : G_2 \rightarrow G_3$  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. □

Given any two groups  $G$  and  $H$ , we denote by  $\text{Hom}(G, H)$  the set of all group homomorphisms from  $G$  into  $H$ .

**Exercise 3.2.2.** Let  $G$  and  $H$  be two groups. Show that the projection maps  $\pi_G : G \times H \rightarrow G$  and  $\pi_H : G \times H \rightarrow H$  defined by

$$\pi_G(a, b) = a \quad \text{and} \quad \pi_H(a, b) = b, \quad \forall (a, b) \in G \times H,$$

are surjective group homomorphisms.

**Proposition 3.2.4.** *Let  $G, H$  and  $K$  be groups. Then there is a natural bijective map from  $\text{Hom}(G, H \times K)$  onto  $\text{Hom}(G, H) \times \text{Hom}(G, K)$ .*

*Proof.* Let  $\pi_H : H \times K \rightarrow H$  and  $\pi_K : H \times K \rightarrow K$  be the projection maps onto the first and the second factors, respectively (see Exercise 3.2.2). Since both  $\pi_H$  and  $\pi_K$  are group homomorphisms, given any group homomorphism  $f : G \rightarrow H \times K$ , we have  $\pi_H \circ f \in \text{Hom}(G, H)$  and  $\pi_K \circ f \in \text{Hom}(G, K)$  by Proposition 5.2.2. Thus we get a map  $\Phi : \text{Hom}(G, H \times K) \rightarrow \text{Hom}(G, H) \times \text{Hom}(G, K)$  defined by

$$\Phi(f) = (\pi_H \circ f, \pi_K \circ f), \quad \forall f \in \text{Hom}(G, H \times K).$$

To show that  $\Phi$  is surjective, given  $f \in \text{Hom}(G, H)$  and  $g \in \text{Hom}(G, K)$ , let  $h : G \rightarrow H \times K$  be the map defined by

$$h(a) = (f(a), g(a)), \quad \forall a \in G.$$

Since for given any  $a, b \in G$ , we have

$$\begin{aligned} h(ab) &= (f(ab), g(ab)) = (f(a)f(b), g(a)g(b)) \\ &= (f(a), g(a))(f(b), g(b)) \\ &= h(a)h(b), \end{aligned}$$

we see that  $h \in \text{Hom}(G, H \times K)$ . Clearly  $\Phi(h) = (\pi_H \circ h, \pi_K \circ h) = (f, g)$ . Therefore,  $\Phi$  is surjective. To show that  $\Phi$  is injective, note that given any  $f \in \text{Hom}(G, H \times K)$ , we have

$$f(a) = ((\pi_H \circ f)(a), (\pi_K \circ f)(a)), \quad \forall a \in G.$$

Therefore, if  $\Phi(f) = \Phi(g)$  for some  $f, g \in \text{Hom}(G, H \times K)$ , then the conditions  $\pi_H \circ f = \pi_H \circ g$  and  $\pi_K \circ f = \pi_K \circ g$  together forces that  $f = g$ . This completes the proof.  $\square$

**Definition 3.2.1.** A group homomorphism  $f : G \rightarrow H$  is said to be

- (i) a *monomorphism* if  $f$  is injective,
- (ii) an *epimorphism* if  $f$  is surjective, and
- (iii) an *isomorphism* if  $f$  is bijective.

If  $f : G \rightarrow H$  is an isomorphism, we say that  $G$  is *isomorphic to*  $H$ , and express it as  $G \cong H$ .

**Lemma 3.2.5.** *Being isomorphic groups is an equivalence relation.*

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

**Proposition 3.2.6.** *Given a group  $G$ , the set  $\text{Aut}(G)$  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  $\text{Aut}(G)$  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

$$G \times G \rightarrow G, \quad (f, g) \mapsto f \circ g,$$

is a binary operation on  $\text{Aut}(G)$ . Clearly composition of maps is associative. The identity map  $\text{Id}_G : G \rightarrow G$  plays the role of a neutral element in a group. Given  $f \in \text{Aut}(G)$ , its inverse  $f^{-1} : G \rightarrow G$  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  $f^{-1} \in \text{Aut}(G)$ . This proves that  $\text{Aut}(G)$  is a group.  $\square$

**Example 3.2.1.** The complex conjugation map  $z \mapsto \bar{z}$  from the additive group  $\mathbb{C}$  into itself is an automorphism of  $\mathbb{C}$ .

**Exercise 3.2.3.** Show that  $\text{Aut}(K_4)$  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  $f \in \text{Aut}(K_4)$ , then  $f(e) = e$  and hence  $f|_{\{a,b,c\}}$  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  $\varphi : \text{Aut}(K_4) \rightarrow S_3$ . Verify that  $\varphi$  is a group isomorphism.)

### 3.3 Kernel

**Definition 3.3.1.** The *kernel* of a group homomorphism  $f : G \rightarrow H$  is the subset

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

Since  $f(e_G) = e_H$  by Proposition 3.2.1 (i), we have  $e_G \in \text{Ker}(f)$ . Therefore,  $\text{Ker}(f)$  is a non-empty subset of  $G$ . Given any two elements  $a, b \in \text{Ker}(f)$  we have  $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = e_H \cdot e_H^{-1} = e_H$ . Therefore,  $\text{Ker}(f)$  is a subgroup of  $G$ .

**Example 3.3.1.** (i) Fix an integer  $n$  and consider the homomorphism

$$f : \mathbb{Z} \rightarrow \mathbb{Z}_n, \quad a \mapsto [a].$$

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

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

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

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

**Proposition 3.3.1.** A group homomorphism  $f : G \rightarrow H$  is injective if and only if  $\text{Ker}(f)$  is trivial.

*Proof.* If  $\text{Ker}(f) \neq \{e\}$ , clearly  $f$  is not injective. Conversely, suppose that  $\text{Ker}(f) = \{e\}$ . 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  $\text{Ker}(f) = \{e\}$ . This completes the proof.  $\square$

**Proposition 3.3.2.** *Any infinite cyclic group is isomorphic to  $\mathbb{Z}$ .*

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

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

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,  $\text{Ker}(f) = \{e\}$ , and so  $f$  is injective. Clearly  $f$  is surjective, and hence is an isomorphism.  $\square$

**Proposition 3.3.3.** *Let  $G$  be a cyclic group generated by  $a \in G$ . A homomorphism  $f : G \rightarrow G$  is an automorphism of  $G$  if and only if  $f(a)$  is a generator of  $G$ .*

*Proof.* Let  $f : G \rightarrow G$  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  $f : G \rightarrow G$  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 1.3.10, and hence  $f$  must be either  $\text{Id}_G$  or the map given by sending  $b \in G$  to  $b^{-1}$ . In both cases,  $f$  is injective, and hence is in  $\text{Aut}(G)$ .  $\square$

**Theorem 3.3.4 (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

$$\varphi_a : G \rightarrow G, \quad g \mapsto ag,$$

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

### 3.4 Quotient group

Let  $G$  be a group.

**Definition 3.4.1.** A *quotient group* of  $G$  is a pair  $(Q, \pi)$ , where  $Q$  is a group and  $\pi : G \rightarrow Q$  is a surjective group homomorphism.

The homomorphism  $\pi : G \rightarrow Q$  in the above definition is also called a quotient map. For notational simplicity, we simply say that  $Q$  is a quotient group of  $G$  when the quotient map  $\pi$  is clear or there is no ambiguity about it.

**Example 3.4.1.** (i) Every group  $G$  is a quotient group of itself. Indeed, we can take the identity map  $\text{Id}_G : G \rightarrow G$  as a surjective group homomorphism.

(ii) The trivial group  $\{e\}$  is a quotient group of every group. Indeed, given any group  $G$  we can take the constant map  $c : G \rightarrow \{e\}$  that sends all elements of  $G$  to  $e \in \{e\}$ , which is clearly a surjective group homomorphism.

(iii) The circle group  $S^1 = \{z \in \mathbb{C} : |z| = 1\}$  in Example 1.1.3 (iv) is a quotient group of the additive group  $\mathbb{R}$ . Indeed, the map  $f : \mathbb{R} \rightarrow S^1$  defined by

$$f(t) = e^{2\pi it}, \forall t \in \mathbb{R},$$

is a surjective group homomorphism.

(iv) Given any two groups  $G$  and  $H$ , both  $G$  and  $H$  are quotient groups of their direct product  $G \times H$  (see Exercise 1.1.6). Indeed, the projection maps onto each factors

$$\pi_1 : G \times H \rightarrow G \text{ and } \pi_2 : G \times H \rightarrow H$$

defined by  $\pi_1(a, b) = a$  and  $\pi_2(a, b) = b$ , for all  $(a, b) \in G \times H$ , are surjective group homomorphisms.

(v) The group  $\mathbb{Z}_n$  in Example 1.1.5 is a quotient group of the additive group  $\mathbb{Z}$ . Indeed, the map  $f : \mathbb{Z} \rightarrow \mathbb{Z}_n$  defined by sending an integer  $a \in \mathbb{Z}$  to its congruence class  $[a] \in \mathbb{Z}_n$  is a surjective group homomorphism.

**Proposition 3.4.1.** Any group homomorphism factor through a quotient map.

*Proof.* Let  $f : G \rightarrow H$  be a group homomorphism. Since the image

$$f(G) = \{f(g) : g \in G\} \subseteq H$$

of  $f$  is a subgroup of  $H$ , the map  $f$  factors as  $f = \iota \circ \pi$ , where  $\pi : G \rightarrow f(G)$  is the surjective group homomorphism defined by  $\pi(g) = f(g)$ ,  $\forall g \in G$ , and

$\iota : f(G) \hookrightarrow H$  is the inclusion map, which is an injective group homomorphism.

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ & \searrow \pi & \nearrow \iota \\ & f(G) & \end{array}$$

This completes the proof.  $\square$

Note that, given any group homomorphism  $f : G \rightarrow H$ , we can naturally associate a subgroup of  $G$ , namely its kernel

$$\text{Ker}(f) := \{g \in G : \pi(g) = e_Q\}.$$

This subgroup has the following special property:

$$(3.4.0.1) \quad gag^{-1} \in \text{Ker}(f), \quad \forall g \in G \text{ and } a \in \text{Ker}(f).$$

Indeed,  $f(gag^{-1}) = f(g)f(a)f(g^{-1}) = f(g)e_H f(g)^{-1} = f(g)f(g)^{-1} = e_H$ . A subgroup having such a property is called a normal subgroup.

**Definition 3.4.2.** Let  $H$  be a subgroup of a group  $G$ . Then  $H$  is said to be a *normal subgroup* of  $G$  if  $ghg^{-1} \in H$ , for all  $g \in G$  and  $h \in H$ .

We just have seen above that kernel of a group homomorphism  $G \rightarrow H$  is a normal subgroup of  $G$ . In particular, for given a quotient group  $(Q, \pi)$  of  $G$ , we have a normal subgroup of  $G$  associated to  $(Q, \pi)$ , namely  $N := \text{Ker}(\pi)$ . Surprisingly, the subgroup  $N$  holds complete information about the quotient group  $(Q, f)$  in the sense that one can reconstruct the pair  $(Q, \pi)$  from  $N$  essentially in a unique way. The next chapter is devoted to this construction.





## Chapter 4

# Quotient Groups

### 4.1 What is a quotient by a subgroup?

Let  $G$  be a group, and  $H$  a subgroup of  $G$ . In this section we introduce the notion of a *quotient 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 4.1.1 (Quotient Group).** Let  $H$  be a subgroup of a group  $G$ . The *quotient of  $G$  by  $H$*  is a pair  $(Q, \pi)$ , where  $Q$  is a group and  $\pi : G \rightarrow Q$  is an epimorphism (i.e., surjective homomorphism) of groups such that

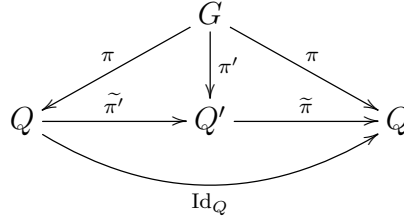
- (i)  $\pi(h) = e_Q$ , the neutral element of  $Q$ , for all  $h \in H$ , and
- (ii) *Universal property of quotient:* given a group  $T$  and a group homomorphism  $t : G \rightarrow T$  satisfying  $H \subseteq \text{Ker}(t)$ , there exists a **unique** group homomorphism  $\tilde{t} : Q \rightarrow T$  such that  $\tilde{t} \circ \pi = t$ ; i.e., the following diagram commutes.

$$(4.1.0.1) \quad \begin{array}{ccc} G & \xrightarrow{t} & T \\ \pi \downarrow & \nearrow \exists! \tilde{t} & \\ Q & & \end{array}$$

Interesting point is that, without knowing existence of such a pair  $(Q, \pi)$ , it follows immediately from the properties (i) and (ii) in Definition 4.1.1 that such a pair  $(Q, \pi)$ , if it exists, must be unique up to a unique isomorphism of groups in the following sense.

**Proposition 4.1.1 (Uniqueness of Quotient).** With the above notations, if  $(Q, \pi)$  and  $(Q', \pi')$  are two quotients of  $G$  by  $H$ , then there exists a **unique** group isomorphism  $\varphi : Q \rightarrow Q'$  such that  $\varphi \circ \pi = \pi'$ .

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



it follows that  $\tilde{\pi} \circ \tilde{\pi}' = \text{Id}_Q$ . Similarly  $\tilde{\pi}' \circ \tilde{\pi} = \text{Id}_{Q'}$ . Therefore,  $\tilde{\pi}' : Q \rightarrow Q'$  is the unique group isomorphism such that  $\tilde{\pi}' \circ \pi = \pi'$ . This completes the proof.  $\square$

## 4.2 Left and right cosets

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 (i) in Definition 4.1.1 says that  $\pi(H) = \{e_Q\}$ . Since  $\pi : G \rightarrow Q$  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<sup>1</sup> of the map  $\pi : G \rightarrow Q$  if  $a^{-1}b \in H$ . Since the set of all fibers of any set map  $f : G \rightarrow Q$  gives a partition of  $G$ , and hence an equivalence relation on  $G$ , the condition (i) suggests us to define a relation  $\rho_L$  on  $G$  by setting

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

It is easy to check that  $\rho_L$  is an equivalence relation on  $G$  (verify!). The  $\rho_L$ -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

<sup>1</sup>The *fiber* of a map  $f : X \rightarrow Y$  over a point  $y \in Y$  is the subset  $f^{-1}(y) = \{x \in X : f(x) = y\} \subseteq X$ .

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

**Proposition 4.2.1.** For each  $a \in G$ , the map  $\varphi_a : H \rightarrow aH$  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  $\varphi_a$  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  $\varphi_a$  is injective. Therefore,  $\varphi_a$  is bijective. Thus, both  $H$  and  $aH$  have the same cardinality.  $\square$

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

**Theorem 4.2.2 (Lagrange's Theorem).** Let  $G$  be a finite group, and  $H$  a subgroup of  $G$ . Then  $|H|$  divides  $|G|$ .

*Proof.* Since  $\rho_L$  is an equivalence relation on  $G$ , it follows from Proposition ?? 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 4.2.1), 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.  $\square$

**Exercise 4.2.1.** 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 4.2.3.** Let  $G$  be a finite group of order  $n$ . Then for any  $a \in G$ ,  $\text{ord}(a)$  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 4.2.2,  $|H|$  divides  $|G| = n$ . Since  $|H| = \text{ord}(a)$ , the result follows. To see the second part, note that if  $\text{ord}(a) = k$ , then  $n = km$ , for some  $m \in \mathbb{N}$ , and so  $a^n = (a^k)^m = e^m = e$ .  $\square$

**Exercise 4.2.2.** Let  $G$  be a finite group of order  $n$ . Let  $k \in \mathbb{N}$  be such that  $\gcd(n, k) = 1$ . Show that the map  $f : G \rightarrow G$  defined by  $f(a) = a^k$ ,  $\forall a \in G$ , is injective, and hence is bijective.

**Corollary 4.2.4.** 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  $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$  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.  $\square$

**Corollary 4.2.5 (Euler's Theorem).** *Let  $n \geq 2$  be an integer. Then for any positive integer  $a$  with  $\gcd(a, n) = 1$ , we have  $a^{\phi(n)} \equiv 1 \pmod{n}$ , 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,  $a^{\phi(n)} \equiv 1 \pmod{n}$ .  $\square$

**Corollary 4.2.6 (Fermat's little theorem).** *If  $p > 0$  is a prime number, then for any positive integer  $a$  with  $\gcd(a, p) = 1$ , we have  $a^{p-1} \equiv 1 \pmod{p}$ .*

*Proof.* Since  $\phi(p) = |U_p| = p - 1$ , the result follows from the Corollary 4.2.5.  $\square$

**Exercise 4.2.3.** 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.  $\square$

**Exercise 4.2.4.** Show that  $15^{1000} - 1$  and  $105^{1200} - 1$  are divisible by 8.

**Exercise 4.2.5.** Define a relation  $\rho_R$  on  $G$  by setting

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

(i) Show that  $\rho_R$  is an equivalence relation on  $G$ .

(ii) Show that the  $\rho_R$ -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 4.2.7.** *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  $\varphi : G/H \rightarrow H \backslash G$ . Therefore, both the sets  $G/H$  and  $H \backslash G$  have the same cardinality.*

*Proof.* Define a map  $\varphi : \{aH : a \in G\} \rightarrow \{Hb : b \in G\}$  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,  $\varphi$  is well-defined and injective. To show  $\varphi$  bijective, note that given any  $Hb \in \{Hb : b \in G\}$  we have  $\varphi(b^{-1}H) = Hb$ . Thus,  $\varphi$  is surjective, and hence is a bijective map.  $\square$

**Definition 4.2.1.** 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 4.2.6.** 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 4.2.1.** 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 1.1.5), we conclude that the index of  $n\mathbb{Z}$  in  $\mathbb{Z}$  is  $[\mathbb{Z} : n\mathbb{Z}] = n$ . We shall explain it later using group homomorphism and quotient group.

**Exercise 4.2.7.** (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  $\mathbb{Z}$ ?

### 4.3 Normal Subgroups

In this section we recall the notion of normal subgroup and give a construction of quotient of a group by its normal subgroup. Recall that the condition (i) in Definition 4.1.1 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  $f : G \rightarrow T$  such that  $H \subseteq \text{Ker}(f)$ . Then we have  $f(a) = f(b)$  if  $a^{-1}b \in H$ . The commutativity of the diagram (4.1.0.1) tells us to send  $aH \in Q$  to  $f(a) \in T$  to define the map  $\tilde{f} : Q \rightarrow T$  which needs to be a group homomorphism. Then we should have

$$(4.3.0.1) \quad \tilde{f}((aH)(bH)) = f(ab) = \tilde{f}((ab)H), \forall a, b \in G.$$

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

$$(4.3.0.2) \quad (aH)(bH) := (ab)H, \forall a, b \in G.$$

**Proposition 4.3.1.** *The map  $G/H \times G/H \rightarrow G/H$  defined by sending  $(aH, bH)$  to  $(ab)H$  is well-defined if and only if*

$$(4.3.0.3) \quad g^{-1}hg \in H, \forall g \in G \text{ and } h \in H.$$

*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 4.3.1 suggests us to reserve a terminology for those subgroups  $H$  of  $G$  that satisfies the property (4.3.0.3).

**Definition 4.3.1** (Normal Subgroup). A subgroup  $H$  of a group  $G$  is said to be *normal* in  $G$  if  $g^{-1}hg \in H$ ,  $\forall g \in G$ ,  $h \in H$ . In this case we express it symbolically by  $H \trianglelefteq G$ .

**Exercise 4.3.1.** 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 4.3.2.** 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 4.3.3.** For all  $n \geq 3$ ,  $A_n$  is a normal subgroup of  $S_n$ .

**Exercise 4.3.2.** (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  $SL_n(\mathbb{R})$  is a normal subgroup of  $GL_n(\mathbb{R})$ , for all  $n \in \mathbb{N}$ .

**Exercise 4.3.3.** Show that  $S_4$  has no normal subgroup of order 3. (*Hint:* If  $\sigma \in S_4$  has order 3, then  $\sigma$  is a 3-cycle in  $S_4$ . Since there are  $\frac{4!}{3} = 8$  distinct 3-cycles in  $S_4$  (see Exercise 2.2.1), and all of them are conjugates (see Proposition 2.2.1), a normal subgroup  $H$  of  $S_4$  containing a 3-cycle contains at least 8 elements.)

**Exercise 4.3.4.** 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  $\rho$  is an equivalence relation on  $G$ . Show that  $H$  is a normal subgroup of  $G$  if and only if  $\rho$  is a subgroup of the direct product group  $G \times G$  (see Exercise 1.1.6).

**Lemma 4.3.4.** The kernel of a group homomorphism  $f : G \rightarrow H$  is a normal subgroup of  $G$ .

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

**Exercise 4.3.5.** For  $n \geq 2$ , show that  $A_n$  is a normal subgroup of  $S_n$  by constructing a group homomorphism  $\varphi : S_n \rightarrow \mu_2 = \{1, -1\}$  such that  $\text{Ker}(\varphi) = A_n$ .

**Exercise 4.3.6.** For  $n \geq 1$ , show that  $\text{SL}_n(\mathbb{R})$  is a normal subgroup of  $\text{GL}_n(\mathbb{R})$  by constructing a group homomorphism  $\varphi : \text{GL}_n(\mathbb{R}) \rightarrow \mathbb{R}^*$  such that  $\text{Ker}(\varphi) = \text{SL}_n(\mathbb{R})$ .

**Lemma 4.3.5.** Let  $f : G \rightarrow H$  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  $aba^{-1} \in f^{-1}(K)$ .  $\square$

**Exercise 4.3.7.** Show that  $N := \{A \in \text{GL}_n(\mathbb{C}) : |\det(A)| = 1\}$  is a normal subgroup of  $\text{GL}_n(\mathbb{C})$ .

**Remark 4.3.1.** 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?

## 4.4 Construction of quotient groups

**Theorem 4.4.1 (Existence of Quotient Group).** Let  $H$  be a normal subgroup of a group  $G$ . Then the quotient group  $(Q, \pi)$  of  $G$  by  $H$  exists and is unique in the sense that if  $(Q, \pi)$  and  $(Q', \pi')$  are two quotients of  $G$  by  $H$ , then there exists a unique isomorphism of groups  $\varphi : Q \rightarrow Q'$  such that  $\varphi \circ \pi' = \pi$ . We denote  $Q$  by  $G/H$ .

*Proof.* Since  $H$  is a normal subgroup of  $G$ ,

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

is a well-defined binary operation on the set  $G/H := \{aH : a \in G\}$ ; see Proposition 4.3.1. 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

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



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

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

Therefore,  $G/H$  is a group. Set  $Q := G/H$  and consider the map

$$(4.4.0.1) \quad \pi : G \longrightarrow Q \text{ defined by } \pi(a) = aH, \forall a \in G.$$

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

$$(4.4.0.2) \quad \tilde{t} : G/H \rightarrow T, \quad aH \longmapsto t(a),$$

is well-defined. Since

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

we conclude that  $\tilde{t}$  is a group homomorphism. Since  $(\tilde{t} \circ \pi)(a) = \tilde{t}(aH) = f(a)$ ,  $\forall a \in G$ , we have  $\tilde{t} \circ \pi = f$ . If  $\xi : G/H \rightarrow T$  is any group homomorphism satisfying  $\xi \circ \pi = f$ , then for any  $a \in G$  we have  $\tilde{t}(aH) = (\tilde{t} \circ \pi)(a) = f(a) = (\xi \circ \pi)(a) = \xi(aH)$ , and hence  $\tilde{t} = \xi$ . Therefore, the pair  $(G/H, \pi)$  satisfy the properties (i) and (ii), and hence is a quotient of  $G$  by  $H$ . Uniqueness is already shown in Proposition 4.1.1.  $\square$

**Corollary 4.4.2.** *Let  $H$  be a normal subgroup of a group  $G$ , and let  $(G/H, \pi)$  be the associated quotient of  $G$  by  $H$ . Then  $\text{Ker}(\pi) = H$ .*

*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

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

This completes the proof.  $\square$

**Exercise 4.4.1.** Let  $G$  be a group such that  $G/Z(G)$  is cyclic. Show that  $G$  is abelian.

*Solution:* Let  $Z := Z(G)$ . Suppose that  $G/Z$  is cyclic. Then  $G/Z = \langle aZ \rangle$ , for some  $a \in G$ . Let  $x \in G$  be arbitrary. Then  $xZ = (aZ)^n = a^nZ$ , for some  $n \in \mathbb{Z}$ . Then  $a^{-n}x = (a^n)^{-1}x \in Z$ . Therefore,  $a^{-n}x = z$ , for some  $z \in Z$ , and so  $x = a^n z$ , for some  $z \in Z = Z(G)$ . Let  $y \in G$  be given. Then as before,  $y = a^m w$ , for some  $m \in \mathbb{Z}$  and  $w \in Z(G)$ . Since  $z, w \in Z(G)$ , we have  $xy = a^n z a^m w = a^m w a^n z = yx$ , as required.  $\square$

**Corollary 4.4.3.** *There is no group  $G$  such that  $|G/Z(G)|$  is a prime number.*

## Chapter 5

# Isomorphism Theorems

### 5.1 First isomorphism theorem

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

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

is the natural quotient homomorphism given by

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

**Theorem 5.1.1.** *Let  $f : G \rightarrow H$  be a group homomorphism. Let  $K$  be a normal subgroup of  $G$  such that  $K \subseteq \text{Ker}(f)$ . Then there is a unique group homomorphism  $\tilde{f} : G/K \rightarrow H$  such that  $\tilde{f} \circ \pi = f$ , where  $\pi : G \rightarrow G/K$  is the quotient homomorphism.*

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \pi \downarrow & \nearrow \tilde{f} & \\ G/K & & \end{array}$$

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

*Proof.* Since  $K$  is a normal subgroup of  $G$ , the quotient group  $G/K$  exists with the natural surjective group homomorphism  $\pi : G \rightarrow G/K$  defined by  $\pi(a) = aK$ ,  $\forall a \in G$ . Since  $K \subseteq \text{Ker}(f)$ , by universal property of quotient (see Definition 4.1.1) we have a unique group homomorphism  $\tilde{f} : G/K \rightarrow H$  such that  $\tilde{f} \circ \pi = f$ . The fact that  $\tilde{f}$  is a well-defined group homomorphism can also be directly checked by observing that

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

Since  $\text{Ker}(\tilde{f}) = \{gK : f(g) = e_H\} = \{gK : g \in \text{Ker}(f)\}$ , we see that  $\text{Ker}(\tilde{f})$  is trivial (meaning that, it is a trivial subgroup) if and only if  $gK = K, \forall g \in \text{Ker}(f)$ . This is equivalent to say that,  $g \in K, \forall g \in \text{Ker}(f)$ , i.e.,  $\text{Ker}(f) \subseteq K$ . Since  $K \subseteq \text{Ker}(f)$  by assumption, it follows from Proposition 3.3.1 that  $\tilde{f}$  is injective if and only if  $K = \text{Ker}(f)$ .  $\square$

**Slogan:** To get a group homomorphism from a quotient group  $G/H$  to a group  $G'$ , thanks to Theorem 5.1.1 we just need to define a group homomorphism  $f : G \rightarrow G'$  such that  $H \subseteq \text{Ker}(f)$ .

**Example 5.1.1.** Let  $H_1$  and  $H_2$  be a normal subgroups of  $G_1$  and  $G_2$ , respectively. Note that  $H_1 \times H_2$  is a normal subgroup of  $G_1 \times G_2$  (verify!). Let  $\pi_1 : G_1 \rightarrow G_1/H_1$  and  $\pi_2 : G_2 \rightarrow G_2/H_2$  be the natural quotient group homomorphisms. These give rise to a group homomorphism  $\phi : G_1 \times G_2 \rightarrow (G_1/H_1) \times (G_2/H_2)$  given by

$$\phi(a_1, a_2) = (\pi_1(a_1), \pi_2(a_2)) = (a_1H_1, a_2H_2), \forall (a_1, a_2) \in G_1 \times G_2.$$

Note that  $\phi$  is surjective because both  $\pi_1$  and  $\pi_2$  are so. Moreover,  $\text{Ker}(\phi) = H_1 \times H_2$  (verify!). Then by Theorem 5.1.1, given any normal subgroup  $K$  of  $G_1 \times G_2$  with  $K \leq H_1 \times H_2$ , there is a unique group homomorphism  $\tilde{\phi} : (G_1 \times G_2)/K \rightarrow (G_1/H_1) \times (G_2/H_2)$  such that  $\tilde{\phi} \circ \pi_K = \phi$ , where  $\pi_K : G_1 \times G_2 \rightarrow (G_1 \times G_2)/K$  is the natural quotient group homomorphism.

As an immediate corollary, we have the following.

**Corollary 5.1.2** (First Isomorphism Theorem). *Let  $f : G \rightarrow H$  be a surjective homomorphism of groups. Then  $f$  induces a natural isomorphism of groups  $\tilde{f} : G/\text{Ker}(f) \rightarrow H$ .*

*Proof.* Note that  $\text{Ker}(f)$  is a normal subgroup of  $G$ . It follows from Theorem 5.1.1 that the group homomorphism  $\tilde{f} : G/\text{Ker}(f) \rightarrow H$  induced by  $f$  is injective. Since  $f$  is surjective and  $\tilde{f} \circ \pi = f$ , where  $\pi : G \rightarrow G/\text{Ker}(f)$  is the natural surjective homomorphism, it follows that  $\tilde{f}$  is surjective. Therefore,  $\tilde{f}$  is a bijective group homomorphism, and hence is an isomorphism of groups.  $\square$

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  $\pi_N : G \rightarrow G/N$  such that  $\text{Ker}(\pi_N) = N$  (see Definition 4.1.1 and Corollary 4.4.2). On the other hand, given a group  $Q$  and a surjective group homomorphism  $\pi : G \rightarrow Q$ , its kernel  $\text{Ker}(\pi)$  is a normal subgroup of  $G$  such that  $G/\text{Ker}(\pi) \cong Q$  by the First isomorphism theorem (Corollary 5.1.2) for groups. This motivates us to define the following (c.f. Definition 4.1.1).

**Definition 5.1.1.** A *quotient group* of  $G$  is a pair  $(Q, \pi)$ , where  $Q$  is a group and  $\pi : G \rightarrow Q$  is a surjective group homomorphism.

As an immediate consequence, we have the following.

**Corollary 5.1.3.** *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  $\Phi : \mathcal{N}_G \rightarrow \mathcal{Q}_G$  by sending a normal subgroup  $N$  of  $G$  to the associated quotient group  $(G/N, \pi_N) \in \mathcal{Q}_G$ . Since  $\pi_N$  is a surjective group homomorphism with  $\text{Ker}(\pi_N) = N$ , the map  $\Phi$  admits an inverse, namely  $\Psi : \mathcal{Q}_G \rightarrow \mathcal{N}_G$  given by sending a quotient group  $(Q, \pi)$  of  $G$  to the kernel  $N := \text{Ker}(\pi) \in \mathcal{N}_G$ . Since the pairs  $(G/N, \pi_N)$  and  $(Q, \pi)$  are uniquely isomorphic, we conclude that  $\Phi$  and  $\Psi$  are inverse to each other. This completes the proof.  $\square$

**Proposition 5.1.4.** *The group  $\mathbb{Z}_n$  is isomorphic to  $\mathbb{Z}/n\mathbb{Z}$ .*

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

**Proposition 5.1.5.** *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  $f : \mathbb{Z} \rightarrow G$  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  $\mathbb{Z}/\text{Ker}(f)$ . Note that,  $\text{Ker}(f) = \{k \in \mathbb{Z} : a^k = e\}$ . Since  $G$  is a cyclic group of order  $n$  generated by  $a$ , we have  $\text{ord}(a) = n$  (see Corollary 1.3.6). Then we have  $\text{Ker}(f) = \{k \in \mathbb{Z} : a^k = e\} = n\mathbb{Z}$ . Therefore,  $G \cong \mathbb{Z}/n\mathbb{Z}$ . Since  $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$  by Theorem 5.1.4, we have  $G \cong \mathbb{Z}_n$ .  $\square$

**Exercise 5.1.1.** Show that any group of order 4 is isomorphic to either  $\mathbb{Z}_4$  or  $K_4$ .

**Exercise 5.1.2.** Show that any group of order 6 is isomorphic to either  $\mathbb{Z}_6$  or  $S_3$ .

**Exercise 5.1.3.** Use the signature homomorphism  $S_n \rightarrow \mu_2 = \{1, -1\}$  to show that  $A_n$  is the only index 2 subgroup of  $S_n$ .

**Exercise 5.1.4.** Show that  $\text{SL}_2(\mathbb{Z}_3)$  and  $S_4$  are two non-isomorphic non-commutative groups of order 24.

## 5.2 Abelianization

**Theorem 5.2.1 (Abelianization).** *Let  $G$  be a group. Then upto isomorphism there exists a unique pair  $(G_{\text{ab}}, \Phi)$  consisting of an abelian group  $G_{\text{ab}}$  and a surjective group homomorphism  $\Phi : G \rightarrow G_{\text{ab}}$  satisfying the following universal property: given any abelian group  $H$  and a group homomorphism  $f : G \rightarrow H$ , there exists a unique group homomorphism  $\tilde{f} : G_{\text{ab}} \rightarrow H$  such that  $\tilde{f} \circ \Phi = f$ .*

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \Phi \downarrow & \nearrow \tilde{f} & \\ G_{\text{ab}} & & \end{array}$$

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

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

$$\begin{array}{ccccc} & & G & & \\ & g \swarrow & \downarrow \Phi & \searrow g & \\ K & \xrightarrow{\tilde{\Phi}} & G_{\text{ab}} & \xrightarrow{\tilde{g}} & K \end{array}$$

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

*Existence:* To prove existence of the pair  $(G_{\text{ab}}, \Phi)$ , 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

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

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

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

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

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

Now suppose that  $H$  is abelian. Then for any  $a, b \in G$ , we have  $[f(a), f(b)] = e$ , and so  $[a, b] \in \text{Ker}(f)$ . Therefore,  $[G, G] \subseteq \text{Ker}(f)$ . Consequently, by universal property of quotient (see Definition 4.1.1) there is a unique homomorphism  $\tilde{f} : G/[G, G] \rightarrow H$  such that  $\tilde{f} \circ \Phi = f$ . This completes the proof of existence part.  $\square$

**Proposition 5.2.2.** *The commutator subgroup of  $S_n$  is  $A_n$ , for all  $n \geq 3$ .*

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

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

is a group homomorphism (see Lemma 3.1.1), we have  $\text{sgn}(\sigma)^{-1} = \text{sgn}(\sigma)$ , for all  $\sigma \in S_n$ . Therefore, given  $\sigma, \tau \in S_n$  we have

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

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 2.4.1), 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.  $\square$

**Exercise 5.2.1.** Show that the abelianization of  $S_n$  is isomorphic to  $\mathbb{Z}_2$ , for all  $n \geq 3$ .

**Exercise 5.2.2.** Given any two groups  $H$  and  $K$ , let  $\text{Hom}(H, K)$  be the set of all group homomorphisms from  $H$  into  $K$ . Fix an integer  $n \geq 3$ .

- (i) Given an abelian group  $G$ , show that there is a natural bijective map  $\text{Hom}(S_n, G) \rightarrow \text{Hom}(\mathbb{Z}_2, G)$ .
- (ii) Find the number of elements in  $\text{Hom}(S_n, \mathbb{Z}_4 \times \mathbb{Z}_6)$ .

**Exercise 5.2.3.** Show that  $S_4$  has no normal subgroup of order 8. (Hint: If  $H$  is a normal subgroup of  $S_4$  of order 8, the quotient group  $S_4/H$  is abelian, and hence  $A_4 = [S_4, S_4] \subseteq H$ , a contradiction.)

### 5.3 Inner Automorphisms

Let  $G$  be a group. Given  $a \in G$ , the map  $\varphi_a : G \rightarrow G$  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  $\text{Ker}(\varphi_a) = \{b \in G : aba^{-1} = e\} = \{e\}$ ,  $\varphi_a$  is injective. Given  $c \in G$ , note that  $\varphi_a(a^{-1}ca) = a(a^{-1}ca)a^{-1} = c$ , and so  $\varphi_a$  is surjective. Therefore,  $\varphi_a$  is an isomorphism.

**Definition 5.3.1.** An automorphism  $\varphi \in \text{Aut}(G)$  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 5.3.1.** Let  $G$  be a group. Let  $\text{Inn}(G)$  be the set of all inner automorphisms of  $G$ . Then  $\text{Inn}(G)$  is a subgroup of  $\text{Aut}(G)$ .

*Proof.* Note that the identity map  $\text{Id}_G : G \rightarrow G$  is in  $\text{Inn}(G)$ . Given  $f, g \in \text{Inn}(G)$ , 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,  $\text{Inn}(G)$  is a subgroup of  $\text{Aut}(G)$ .  $\square$

**Proposition 5.3.2.** The map  $\varphi : G \rightarrow \text{Inn}(G)$  that sends  $a \in G$  to the map  $\varphi_a : G \rightarrow G$  defined by

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

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



*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,  $\varphi$  is a group homomorphism. Since every element of  $\text{Inn}(G)$  is of the form  $\varphi_a$ , for some  $a \in G$ , the map  $\varphi$  is surjective. Since  $\text{Ker}(\varphi) = \{a \in G : \varphi(a) = \text{Id}_G\} = \{a \in G : aba^{-1} = b, \forall b \in G\} = Z(G)$ , by the first isomorphism theorem for groups we have  $G/Z(G) \cong \text{Inn}(G)$ .  $\square$

**Exercise 5.3.1.** Let  $G$  be a group such that  $G/Z(G)$  is cyclic. Show that  $\text{Inn}(G)$  is a trivial subgroup of  $\text{Aut}(G)$ .

## 5.4 Second isomorphism theorem

**Theorem 5.4.1** (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 1.4.1.

(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  $\varphi : H \rightarrow HK/K$  by  $\varphi(a) = aK$ , for all  $a \in H$ . Since  $\varphi(ab) = (ab)K = (aK)(bK) = \varphi(a)\varphi(b)$ , for all  $a, b \in H$ ,  $\varphi$  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  $\varphi$  is surjective. Since

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

by first isomorphism theorem (see Corollary 5.1.2) we have  $H/(H \cap K) \cong HK/K$ .  $\square$

**Example 5.4.1.** 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  $\text{lcm}(m, n) = mn$ , 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 5.4.1.** 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  $K = 10\mathbb{Z}$ ).

## 5.5 Third isomorphism theorem

**Theorem 5.5.1** (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)  $\phi : G \rightarrow G/H$ ,
- (ii)  $\psi : G \rightarrow G/K$ , and
- (iii)  $\eta : H \rightarrow H/K$

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

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

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  $\pi : G/K \rightarrow (G/K)/(H/K)$  exists. Consider the diagram

$$\begin{array}{ccc} G & \xrightarrow{\psi} & G/K \\ \phi \downarrow & & \downarrow \pi \\ G/H & \xrightarrow{\widetilde{\pi \circ \psi}} & (G/K)/(H/K) \end{array}$$

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

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

Then by first isomorphism theorem (Corollary 5.1.2) applied to the group homomorphism  $\pi \circ \psi$  we have the required isomorphism  $G/H \cong (G/K)/(H/K)$  of groups.  $\square$

**Corollary 5.5.2** (Correspondence Theorem). *Let  $f : G \rightarrow H$  be a surjective group homomorphism. Consider the following two sets:*

- (i)  $\mathcal{A} :=$  the set of all subgroups of  $G$  containing  $\text{Ker}(f)$ , and
- (ii)  $\mathcal{B} :=$  the set of all subgroups of  $H$ .

*Then there is an inclusion preserving bijective map*

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

*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  $\Phi : \mathcal{A} \rightarrow \mathcal{B}$  by sending a subgroup  $N$  of  $G$  containing  $\text{Ker}(f)$  to its image  $f(N)$ . Note that  $f(N)$  is a subgroup of  $H$  by Proposition 3.2.2 (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 3.2.2 (ii). Since  $e_H \in K$  we have  $\text{Ker}(f) = f^{-1}(e) \subseteq f^{-1}(K)$ . Thus,  $f^{-1}(K) \in \mathcal{A}$ . This gives a map

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

It remains to show that  $\Phi$  and  $\Psi$  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  $ab^{-1} \in \text{Ker}(f) \subseteq N$ , 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  $\Psi \circ \Phi = \text{Id}_{\mathcal{A}}$ . Conversely, given  $K \in \mathcal{B}$ , we have  $(\Phi \circ \Psi)(K) = f(f^{-1}(K)) = K$ , since  $f$  is surjective. Thus  $\Phi \circ \Psi = \text{Id}_{\mathcal{B}}$ . This completes the proof.  $\square$

**Exercise 5.5.1.** 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  $H$ .

**Exercise 5.5.2.** Let  $\pi : G \rightarrow Q$  be a surjective group homomorphism. Let  $H$  be a normal subgroup of  $G$  and let  $\pi_H : H \rightarrow Q$  be the restriction of  $\pi$  on  $H$ . If  $K = H \cap \text{Ker}(\pi)$ , show that the induced map  $\widetilde{\pi}_H : H/K \rightarrow Q$  is injective, and it identifies  $H/K$  as a normal subgroup of  $Q$ .



## Chapter 6

# Direct product and direct sum

### 6.1 Direct product of groups

**Definition 6.1.1.** 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  $\{\pi_\alpha : G \rightarrow G_\alpha\}_{\alpha \in \Lambda}$  is a family of group homomorphisms such that given any group  $H$  and a family of group homomorphisms  $\{f_\alpha : H \rightarrow G_\alpha\}_{\alpha \in \Lambda}$  there exists a **unique** group homomorphism  $f : H \rightarrow G$  such that  $\pi_\alpha \circ f = f_\alpha$ , for all  $\alpha \in \Lambda$ .

$$\begin{array}{ccc} H & & \\ \downarrow \exists! f & \searrow f_\alpha & \\ G & \xrightarrow{\pi_\alpha} & G_\alpha \end{array}$$

**Theorem 6.1.1 (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  $(G, \{g_\alpha : G \rightarrow G_\alpha\}_{\alpha \in \Lambda})$  and  $(H, \{h_\alpha : H \rightarrow G_\alpha\}_{\alpha \in \Lambda})$  are direct products of the family of groups  $\{G_\alpha : \alpha \in \Lambda\}$ , then there exists a unique isomorphism of groups  $\phi : G \rightarrow H$  such that  $h_\alpha \circ \phi = g_\alpha$ , for all  $\alpha \in \Lambda$ . We denote by  $\prod_{\alpha \in \Lambda} G_\alpha$  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  $(H, \{h_\beta : H \rightarrow G_\beta\}_{\beta \in \Lambda})$  we have a group homomorphism  $\varphi : G \rightarrow H$  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  $\psi : H \rightarrow G$  such that  $\pi_\alpha \circ \psi = g_\alpha$ ,  $\forall \alpha \in \Lambda$ . Since both  $\psi \circ \varphi : G \rightarrow G$  and  $\text{Id}_G : G \rightarrow G$  are group homomorphisms satisfying

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

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

For a construction, let

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

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

$$fg : \Lambda \rightarrow \prod_{\alpha \in \Lambda} G_{\alpha}$$

by

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

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  $e : \Lambda \rightarrow \prod_{\alpha \in \Lambda} G_{\alpha}$  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  $\pi_{\beta} : \prod_{\alpha \in \Lambda} G_{\alpha} \rightarrow G_{\beta}$  by  $\pi_{\beta}(f) = f(\beta)$ . Then  $\pi_{\beta}$  is a group homomorphism. Given a group  $H$  and a family  $\{h_{\alpha} : H \rightarrow G_{\alpha}\}_{\alpha \in \Lambda}$  of group homomorphisms, we define a map  $\psi : H \rightarrow \prod_{\alpha \in \Lambda} G_{\alpha}$  that sends  $a \in H$  to the function  $\psi_a : \Lambda \rightarrow \prod_{\alpha \in \Lambda} G_{\alpha}$  defined by  $\psi_a(\alpha) = h_{\alpha}(a)$ ,  $\forall \alpha \in \Lambda$ . Then it is straight forward to verify that  $\psi$  is a group homomorphism satisfying  $\pi_{\alpha} \circ \psi = h_{\alpha}$ ,  $\forall \alpha \in \Lambda$ .  $\square$

**Example 6.1.1 (External Direct Product of  $G_1, \dots, G_n$ ).** Let  $G_1, \dots, G_n$  be a finite family of groups, not necessarily distinct. Define a binary operation on the Cartesian product  $G := G_1 \times \dots \times G_n$  by

$$(6.1.0.1) \quad (a_1, \dots, a_n) \cdot (b_1, \dots, b_n) := (a_1b_1, \dots, a_nb_n),$$

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

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

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  $i \in \{1, \dots, n\}$ . Then given any  $a_i \in G_i$ , for each  $i$ , we have

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

Since

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

we conclude that  $(a_1, \dots, a_n)^{-1} = (a_1^{-1}, \dots, a_n^{-1}) \in G$ . Therefore,  $G = G_1 \times \dots \times G_n$  is a group with respect to the binary operation defined in (6.1.0.1).

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

$$(6.1.0.2) \quad p_i : G_1 \times \dots \times G_n \rightarrow G_i$$

be the map defined by

$$(6.1.0.3) \quad p_i(a_1, \dots, a_n) = a_i, \quad \forall (a_1, \dots, a_n) \in G_1 \times \dots \times G_n.$$

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

$$(6.1.0.4) \quad f(h) = (f_1(h), \dots, f_n(h)), \quad \forall h \in H.$$

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

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

Therefore,  $f$  is a group homomorphism. Clearly  $p_i \circ f = f_i$ , for all  $i \in \{1, \dots, n\}$ . Suppose that  $f' : H \rightarrow G_1 \times \dots \times G_n$  is any group homomorphism such that  $p_i \circ f' = f_i$ , for all  $i \in \{1, \dots, n\}$ . Let  $h \in H$  be arbitrary. Let  $f'(h) = (a_1, \dots, a_n) \in G_1 \times \dots \times G_n$ . Then  $f_i(h) = (p_i \circ f')(h) = p_i(a_1, \dots, a_n) = a_i$ , for all  $i \in \{1, \dots, n\}$ , and hence  $f'(h) = (a_1, \dots, a_n) = (f_1(h), \dots, f_n(h)) = f(h)$ . Therefore,  $f' = f$ , and hence by universal property of product of groups (see Definition 6.1.1) we conclude that  $G_1 \times \dots \times G_n$  is a direct product of  $G_1, \dots, G_n$ . The group  $G_1 \times \dots \times G_n$  is also known as the *external direct product of  $G_1, \dots, G_n$* .

**Corollary 6.1.2.** *The direct product of a finite family of finite groups  $G_1, \dots, G_n$  is a group of order  $|G_1| \cdots |G_n|$ . Moreover,  $G_1 \times \dots \times G_n$  is abelian if and only if  $G_i$  is abelian, for all  $i \in I_n$ .*

**Exercise 6.1.1.** Given any two groups  $G$  and  $H$ , show that  $Z(G \times H) = Z(G) \times Z(H)$ .

**Proposition 6.1.3.** *Let  $G := G_1 \times \dots \times G_n$  be the external direct product of the family of groups  $G_1, \dots, G_n$ . For each  $i \in I_n := \{1, \dots, n\}$ , let  $H_i = \{(a_1, \dots, a_n) \in G : a_j = e_j, \forall j \neq i\} \subseteq G$ . 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  $(e_1, \dots, e_n) \in H_i$ , so  $H_i \neq \emptyset$ . Let  $a := (a_1, \dots, a_n)$ ,  $b := (b_1, \dots, b_n) \in H_i$ . 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,  $a^{-1}b = (a_1^{-1}b_1, \dots, a_n^{-1}b_n) \in H_i$ , and hence  $H_i$  is a subgroup of  $G$ . Let  $a = (a_1, \dots, a_n) \in G$  and  $b := (b_1, \dots, b_n) \in H_i$  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  $aba^{-1} = (a_1, \dots, a_n)(b_1, \dots, b_n)(a_1^{-1}, \dots, a_n^{-1}) \in H_i$ . Therefore,  $H_i$  is a normal subgroup of  $G$ , for all  $i \in I_n$ .

(ii) Let  $a \in G$  be given. Then  $a = (a_1, \dots, a_n)$ , 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,  $h_i := (h_{i1}, \dots, h_{in}) \in G$ , where

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

Then  $h_i \in H_i$ , for all  $i \in I_n$ , and  $h_1 \cdots h_n = (a_1, \dots, a_n) = a$ . 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,

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

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  $a = (a_1, \dots, a_n) \in H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_n)$ . 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

$$(6.1.0.5) \quad a = h_1 \cdots h_{i-1} h_{i+1} \cdots h_n$$

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

$$(6.1.0.6) \quad b_k = \begin{cases} e_i, & \text{if } k = i, \\ h_{kk}, & \text{if } k \neq i. \end{cases}$$

Comparing the  $j$ -th component of both sides of the equation (6.1.0.5), 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.  $\square$

**Lemma 6.1.4.** *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  $G$ .  $\square$

**Exercise 6.1.2.** Is the conclusion of the Lemma 6.1.4 still holds if we assume exactly one of  $H$  and  $K$  is normal in  $G$ ?

**Lemma 6.1.5.** *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  $G$ .  $\square$

**Definition 6.1.2.** Let  $G$  be a group and let  $H_1, \dots, H_n$  be normal subgroups of  $G$ . Then  $G$  is said to be an *internal direct product of  $H_1, \dots, H_n$*  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  $i \in \{1, \dots, n\}$ .

**Proposition 6.1.6.** *Let  $G = G_1 \times \cdots \times G_n$  be the external direct product of a finite collection of (not necessarily distinct) groups  $G_1, \dots, G_n$ , and  $H_i := \{(a_1, \dots, a_n) \in G : a_j = e_j, \forall j \neq i\}$ , for each  $i \in I_n$ . Then  $G$  is an internal direct product of  $H_1, \dots, H_n$ , respectively.*

*Proof.* It follows from Proposition 6.1.3 (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 6.1.3 (i), and  $K_i := H_1 \cdots H_{i-1}H_{i+1} \cdots H_n$  is a normal subgroups of  $G$  by Lemma 6.1.5. Moreover,  $H_i \cap K_i = \{e\}$  by Proposition 6.1.3 (iii). Then using Lemma 6.1.4 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.  $\square$

**Theorem 6.1.7.** Let  $\{H_1, \dots, H_n\}$  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  $H_1, \dots, H_n$  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  $H_1, \dots, H_n$ , 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  $a = e_1 \cdots e_{i-1} a e_{i+1} \cdots e_n$ , 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  $a = a_1 \cdots a_{i-1} e a_{i+1} \cdots a_n$ , where  $a_j \in H_j, \forall j \neq i$ . Then from 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.  $\square$

**Exercise 6.1.3.** 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 6.1.8.** If  $m, n \in \mathbb{Z}$  with  $\gcd(m, n) = 1$ , then  $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ .

## 6.2 Direct sum of abelian groups

**Theorem 6.2.1 (Direct Sum of Abelian Groups).** Let  $\{A_\alpha : \alpha \in \Lambda\}$  be a family of abelian groups. Then there is a pair  $(A, \{\iota_\alpha\}_{\alpha \in \Lambda})$ , consisting of a group  $A$  and a

family of group monomorphisms

$$\{\iota_\alpha : A_\alpha \rightarrow A\}_{\alpha \in \Lambda}$$

satisfying the following universal property:

- Given any abelian group  $T$  and a family of group homomorphisms  $\{f_\alpha : A_\alpha \rightarrow T\}_{\alpha \in \Lambda}$ , there exists a unique group homomorphism  $f : A \rightarrow T$  such that  $f \circ \iota_\alpha = f_\alpha$ ,  $\forall \alpha \in \Lambda$ .

$$\begin{array}{ccc} A_\alpha & \xrightarrow{f_\alpha} & T \\ \downarrow \iota_\alpha & \nearrow f & \\ A & & \end{array}$$

The pair  $(A, \{\iota_\alpha\}_{\alpha \in \Lambda})$  is uniquely determined by the universal property, and is called the **direct sum** of the family of groups  $\{A_\alpha\}_{\alpha \in \Lambda}$ , and is denoted by  $\bigoplus_{\alpha \in \Lambda} A_\alpha$ .

*Proof.* Uniqueness of the pair  $(A, \{\iota_\alpha\}_{\alpha \in \Lambda})$  follows from the universal property. We now prove existence. We write the group operation of  $A_\alpha$  additively. Given  $\alpha \in \Lambda$ , let  $0_\alpha$  be the neutral element of  $A_\alpha$ , and  $\pi_\alpha : \prod_{\beta \in \Lambda} A_\beta \rightarrow A_\alpha$  be the natural projection homomorphism. Given  $x \in \prod_{\alpha \in \Lambda} A_\alpha$ , let  $x_\alpha := \pi_\alpha(x) \in A_\alpha$ . Consider the subset

$$A := \left\{ x \in \prod_{\alpha \in \Lambda} A_\alpha \mid \pi_\alpha(x) = 0_\alpha, \text{ for all but finitely many } \alpha \in \Lambda \right\}.$$

Clearly  $0 := (0_\alpha)_{\alpha \in \Lambda} \in A$ , and given any  $x, y \in A$ ,  $\pi_\alpha(x - y) = x_\alpha - y_\alpha = 0_\alpha$ , for all but finitely many  $\alpha \in \Lambda$ , and so  $x - y \in A$ . Therefore,  $A$  is a subgroup of  $\prod_{\alpha \in \Lambda} A_\alpha$ . For each  $\alpha \in \Lambda$ , let  $\iota_\alpha : A_\alpha \rightarrow A$  be the map defined by sending  $a \in A_\alpha$  to the element  $\iota_\alpha(a) = x$ , where

$$\pi_\beta(x) := \begin{cases} a, & \text{if } \beta = \alpha, \\ e_\beta, & \text{if } \beta \neq \alpha. \end{cases}$$

Clearly  $\iota_\alpha$  is an injective group homomorphism, for all  $\alpha \in \Lambda$ . Let  $T$  be an abelian group. Let  $f_\alpha : A_\alpha \rightarrow T$  be a group homomorphism, for each  $\alpha \in \Lambda$ . Define a map  $f : A \rightarrow T$  by

$$f(a) = \sum_{\alpha \in \Lambda} f_\alpha(\pi_\alpha(a)), \quad \forall a \in A.$$

Note that the above sum is finite. Since  $f_\alpha : A_\alpha \rightarrow T$  is a group homomorphism,  $f_\alpha(0_\alpha) = 0_T \in T$ , and hence  $f(\iota_\alpha(g)) = f_\alpha(g)$ , for all  $g \in A_\alpha$ . Therefore,  $f \circ \iota_\alpha = f_\alpha$ ,  $\forall \alpha \in \Lambda$ . Uniqueness of  $f$  is easy to see (verify!).  $\square$

Let  $\{A_1, \dots, A_n\}$  be a finite collection of abelian groups and let  $A_1 \times \dots \times A_n$  be the direct product. Then for each  $i \in \{1, \dots, n\}$  the natural map

$$\varphi_i : A_i \rightarrow A_1 \times \dots \times A_n$$

defined by sending  $a \in A_i$  to the element  $\varphi_i(a) \in A_1 \times \dots \times A_n$  whose  $i$ -th component is  $a$  and all other components are 0, is a group homomorphism. Since  $A_i$ 's are abelian, so is their direct product  $A_1 \times \dots \times A_n$ . Then by universal property of direct sum (Theorem 6.2.1), there is a unique group homomorphism

$$f : A_1 \oplus \dots \oplus A_n \rightarrow A_1 \times \dots \times A_n$$

such that  $f \circ \iota_i = \varphi_i$ , for all  $i \in \{1, \dots, n\}$ . Clearly  $f$  is injective; in fact, it is the inclusion map. Given any  $(a_1, \dots, a_n) \in A_1 \times \dots \times A_n$ , we have  $f(\sum_{i=1}^n \iota_i(a_i)) =$

$\sum_{i=1}^n \varphi_i(a_i) = (a_1, \dots, a_n)$ . Therefore,  $f$  is surjective, and hence is an isomorphism.

Thus, for a finite index set  $\Lambda$ , we have  $\bigoplus_{\alpha \in \Lambda} A_\alpha = \prod_{\alpha \in \Lambda} A_\alpha$ .

**Remark 6.2.1.** If we remove *abelian* hypothesis from  $A_\alpha$ 's and also from the test objects  $T$  in Theorem 6.2.1, then also the associated pair  $(A, \{\iota_\alpha\}_{\alpha \in \Lambda})$  exists (in general, as a non-abelian group), and is known as the **free product** of the family of groups  $\{A_\alpha : \alpha \in \Lambda\}$ . We do not attempt to discuss it here; interested readers may see Serge Lang's Algebra book.

**Definition 6.2.1.** Let  $A$  be an abelian group. A subset  $S$  of  $A$  is said to be  $\mathbb{Z}$ -linearly independent if given any finite number of distinct elements  $a_1, \dots, a_n \in S$ , we have  $r_1 a_1 + \dots + r_n a_n = 0$  implies  $r_1 = \dots = r_n = 0$ .

**Exercise 6.2.1.** 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

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

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

**Exercise 6.2.2.** 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  $n \in \mathbb{N}$ .

## Chapter 7

# Group Action

### 7.1 Definition and examples

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

**Definition 7.1.1.** A *left  $G$ -action* on  $X$  is a map

$$\sigma : G \times X \rightarrow X$$

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 7.1.1.** We can define a *right  $G$ -action* on  $X$  to be a map

$$\tau : X \times G \rightarrow X$$

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  $\tau(x, a)$ .

**Example 7.1.1.** (i) Given a group  $G$  and a non-empty set  $X$ , the map

$$\sigma : G \times X \rightarrow X$$

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  $\tau : X \times G \rightarrow X$  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  $\varphi : G \times H \rightarrow H$  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 7.1.1** (*Permutation representation of a  $G$ -action*). 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  $\mathcal{A}$  be the set of all left  $G$ -actions on  $X$ , and let  $\mathcal{B} := \text{Hom}(G, S(X))$  be the set of all group homomorphisms from  $G$  into  $S(X)$ . Define a map  $\Phi : \mathcal{A} \rightarrow \mathcal{B}$  by sending a left  $G$ -action  $\sigma : G \times X \rightarrow X$  to the map

$$(7.1.0.1) \quad f_\sigma : G \rightarrow S(X)$$

that sends  $a \in G$  to the map

$$(7.1.0.2) \quad f_\sigma(a) : X \rightarrow X, x \mapsto \sigma(a, x).$$

We first show that  $f_\sigma(a)$  is bijective and hence is an element of  $S(X)$ . 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  $\sigma_a$  is surjective. Therefore,  $f_\sigma(a) \in S(X)$ , for all  $a \in G$ . To show  $f_\sigma : G \rightarrow S(X)$  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,  $f_\sigma$  is a group homomorphism, known as the *permutation representation* of  $G$  associated to the left  $G$ -action  $\sigma$  on  $X$ . Thus,  $f_\sigma \in \mathcal{B}$ .

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

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

We show that  $\sigma_f$  is a left  $G$ -action on  $X$ . Since  $f : G \rightarrow S(X)$  is a group homomorphism,  $f(e) = \text{Id}_X$  in  $S(X)$ . Therefore,  $\sigma_f(e, x) = f(e)(x) = x$ ,  $\forall x \in X$ . Since  $f : G \rightarrow S(X)$  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,  $\sigma_f$  is a left  $G$ -action on  $X$ . Thus we get a map  $\Psi : \mathcal{B} \rightarrow \mathcal{A}$  defined by

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

It remains to check that  $\Psi \circ \Phi = \text{Id}_{\mathcal{A}}$  and  $\Phi \circ \Psi = \text{Id}_{\mathcal{B}}$ . Given a left  $G$ -action  $\tau : G \times X \rightarrow X$  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  $(\Psi \circ \Phi)(\tau) = \tau$ ,  $\forall \tau \in \mathcal{A}$ . Therefore,  $\Psi \circ \Phi = \text{Id}_{\mathcal{A}}$ . Conversely, given a group homomorphism  $g : G \rightarrow S(X)$ , 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  $(\Phi \circ \Psi)(g) = g$ ,  $\forall g \in \mathcal{B}$ . Therefore,  $\Phi \circ \Psi = \text{Id}_{\mathcal{B}}$ . This completes the proof.  $\square$

**Definition 7.1.2 (Faithful action).** A left  $G$ -action  $\sigma : G \times X \rightarrow X$  on a non-empty set  $X$  is said to be *faithful* if  $\text{Ker}(f_\sigma) = \{e\}$ , where  $f_\sigma : G \rightarrow S(X)$  is the permutation representation of  $G$  associated to  $\sigma$  (see (7.1.0.1) and (7.1.0.2) in Lemma 7.1.1).

**Example 7.1.2.** The multiplicative group  $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$  acts on  $V := \mathbb{R}^n$  by scalar multiplication

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

defined by

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

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

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

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

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

Since

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

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

**Example 7.1.3.** Recall that Cayley's theorem (Theorem 3.3.4) 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

$$\sigma : G \times G \rightarrow G$$

defined by

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

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

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

Then  $f_\sigma$  is a group homomorphism with

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

is trivial, and hence  $\sigma$  is a faithful action.



## 7.2 Orbits and isotropy subgroups

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

$$(7.2.0.1) \quad x \sim_\sigma y \text{ if } y = \sigma(a, x), \text{ for some } a \in G.$$

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

$$(7.2.0.2) \quad \text{Orb}_G(x) := \{\sigma(a, x) : a \in G\} \subseteq X,$$

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

- (i)  $x \in \text{Orb}_G(x)$ ,  $\forall x \in X$ , and
- (ii) given  $x, y \in X$ , either  $\text{Orb}_G(x) = \text{Orb}_G(y)$  or  $\text{Orb}_G(x) \cap \text{Orb}_G(y) = \emptyset$ .

Therefore,  $X$  is a disjoint union of distinct  $G$ -orbits of elements of  $X$ . A  $G$ -action  $\sigma : G \times X \rightarrow X$  is said to be *transitive* if  $\text{Orb}_G(x) = \text{Orb}_G(y)$ , for all  $x, y \in X$ . Therefore,  $\sigma$  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 7.2.1.** *Let  $\sigma : G \times X \rightarrow X$  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  $x$ , and sometimes it is also denoted by  $\text{Stab}_G(x)$ .*

*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  $G$ .  $\square$

**Exercise 7.2.1.** Let  $\sigma : G \times X \rightarrow X$  be a left  $G$ -action on  $X$ . If  $f_\sigma : G \rightarrow S(X)$  is the group homomorphism induced by  $\sigma$ , then show that  $\text{Ker}(f_\sigma) = \bigcap_{x \in X} G_x$ , where  $G_x$  is the isotropy subgroup of  $x \in X$ .

**Corollary 7.2.2.** *Let  $X$  be a non-empty set equipped with a left  $G$ -action  $\sigma : G \times X \rightarrow X$ . Let  $H$  be a normal subgroup of  $G$ . Then the  $G$ -action  $\sigma$  induces a left  $G/H$ -action*

$\tilde{\sigma} : (G/H) \times X \rightarrow X$  making the following diagram commutative

$$\begin{array}{ccc} G \times X & \xrightarrow{\sigma} & X \\ \pi_H \times \text{Id}_X \downarrow & & \parallel \\ (G/H) \times X & \xrightarrow{\tilde{\sigma}} & X \end{array}$$

if and only if  $H \subseteq \bigcap_{x \in X} G_x$ , where  $G_x := \{g \in G : \sigma(g, x) = x\}$ ,  $\forall x \in X$ .

*Proof.* Let  $f_\sigma : G \rightarrow S(X)$  be the permutation representation of  $G$  in  $S(X)$  associated to the  $G$ -action  $\sigma$  on  $X$ . Note that  $\text{Ker}(f_\sigma) = \bigcap_{x \in X} G_x$ .

Let  $H$  be a normal subgroup of  $G$ . Let  $\pi_H : G \rightarrow G/H$  be the associated quotient group homomorphism. Suppose that  $H \subseteq \bigcap_{x \in X} G_x = \text{Ker}(f_\sigma)$ . Then by universal property of quotient, there exists a unique group homomorphism  $\tilde{f}_\sigma : G/H \rightarrow S(X)$  such that  $\tilde{f}_\sigma \circ \pi_H = f_\sigma$ . Then  $\tilde{f}_\sigma$  induces a left  $G/H$ -action  $\tilde{\sigma} : (G/H) \times X \rightarrow X$  which sends  $(aH, x) \in (G/H) \times X$  to  $\tilde{\sigma}(aH, x) := \tilde{f}_\sigma(aH)(x) = f_\sigma(a)(x) = \sigma(a, x) \in X$ .

Conversely, suppose that  $\tilde{\sigma} : (G/H) \times X \rightarrow X$  be a left  $G/H$ -action on  $X$  making the above diagram commutative. Let

$$f_{\tilde{\sigma}} : G/H \rightarrow S(X)$$

be the permutation representation of  $G/H$  into  $S(X)$  associated to  $\tilde{\sigma}$ . Then  $\sigma$  can be recovered from the group homomorphism

$$G \xrightarrow{\pi_H} G/H \xrightarrow{f_{\tilde{\sigma}}} S(X)$$

using the construction given in Lemma 7.1.1. From this, we have  $H \subseteq \text{Ker}(f_\sigma)$ .  $\square$

**Exercise 7.2.2.** Let  $\sigma : G \times X \rightarrow X$  be a left  $G$ -action on  $X$ . Given  $x \in X$  and  $a \in G$ , show that  $G_y = aG_x a^{-1}$ , where  $y = \sigma(a, x) \in X$ . Deduce that if  $\sigma$  is a transitive  $G$ -action on  $X$ , show that  $\text{Ker}(f_\sigma) = \bigcap_{a \in G} aG_x a^{-1}$ .

**Exercise 7.2.3.** 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  $\bigcap_{\sigma \in G} \sigma G_x \sigma^{-1} = \{e\}$ .

**Corollary 7.2.3 (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  $\varphi : G \rightarrow S(X)$  such that  $\text{Ker}(\varphi) \subseteq H$ .

*Proof.* Consider the map  $\sigma : G \times X \rightarrow X$  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,  $\sigma$  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,  $\sigma$  is a left  $G$ -action on  $X$ . Then  $\sigma$  give rise to the group homomorphism

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

that sends  $a \in G$  to the map

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

Since  $\text{Ker}(f_\sigma) \subseteq G_x$ , for all  $x \in X$  by Exercise 7.2.1, 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  $\text{Ker}(f_\sigma) \subseteq H$ . □

**Exercise 7.2.4.** Let  $H$  be a subgroup of  $G$ , and let  $X$  be the set of all left cosets of  $H$  in  $G$ . Let  $\sigma : G \times X \rightarrow X$  be the left  $G$ -action on  $X$  defined by  $\sigma(a, bH) = (ab)H$ ,  $\forall a, b \in G$ . Show that  $\sigma$  is a transitive action.

**Exercise 7.2.5.** 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 7.2.4** (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 7.2.3. □

**Exercise 7.2.6.** 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  $n$ .

*Solution:* By Cayley's theorem (Theorem 3.3.4)  $G$  is isomorphic to a subgroup, say  $H$ , of the symmetric group  $S(G)$  via the monomorphism  $\varphi : G \rightarrow S(G) \cong S_{2n}$  defined by sending  $a \in G$  to the bijective map  $\varphi_a : G \rightarrow G$  that sends  $b \in G$  to  $ab$ , for all  $b \in G$ . Since 2 divides  $|G| = 2n$ ,  $G$  has an element, say  $a \in G$ , of order 2 by Exercise 1.2.22. Since for any  $b \in G$  we have  $\varphi_a(b) = ab$  and  $\varphi_a(ab) = a^2b = eb = b$ , we see that  $\varphi_a \in S(G)$  is a product of transpositions of the form  $(b \ ab)$ . Since  $|G| = 2n$ , the number of transpositions appearing in the factorization of  $\varphi_a$  is  $n$ , an odd number. So  $\varphi_a$  is an odd permutation. This shows that the subgroup  $H := \varphi(G)$  contains an odd permutation. Define a map

$$f : H \rightarrow \{-1, 1\}$$

by sending  $\sigma \in H$  to

$$f(\sigma) := \begin{cases} 1, & \text{if } \sigma \text{ is an even permutation,} \\ -1, & \text{if } \sigma \text{ is an odd permutation.} \end{cases}$$

Note that  $f$  is a surjective group homomorphism, and hence by first isomorphism theorem (Theorem 5.1.2) we have

$$H/\text{Ker}(f) \cong \{-1, 1\}.$$

Then we have

$$2 = |\{-1, 1\}| = |H/\text{Ker}(f)| = \frac{|H|}{|\text{Ker}(f)|} = \frac{2n}{|\text{Ker}(f)|}.$$

Therefore,  $\text{Ker}(f)$  is a normal subgroup of  $H$  of order  $|\text{Ker}(f)| = n$ . Since  $G \cong H$  via  $\varphi$ , taking inverse image of  $\text{Ker}(f) \subseteq H$  along the isomorphism  $\varphi$  we get a required normal subgroup of  $G$  of order  $n$ .  $\square$

**Corollary 7.2.5.** *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  $f : G \rightarrow S(X)$  be the map that sends  $a \in G$  to

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

Then  $f$  is a group homomorphism. Then  $K := \text{Ker}(f) \subseteq H$  by Corollary 7.2.3, 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 5.1.2). 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  $H = K = \text{Ker}(f)$ . Thus  $H$  is a normal subgroup of  $G$ .  $\square$

**Warning:** The above Corollary 7.2.5 does not ensure existence of a subgroup  $H$  of  $G$  of index smallest prime factor of  $|G|$ .

**Exercise 7.2.7.** 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 7.2.8.** 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 7.2.6.** *Let  $\sigma : G \times X \rightarrow X$  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  $\varphi : G/G_x \rightarrow \text{Orb}_G(x)$  defined by  $\varphi(aG_x) = \sigma(a, x)$ ,  $\forall a \in G$ , is a well-defined bijective map. Consequently,  $[G : G_x] = |\text{Orb}_G(x)|$ .*

*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  $\varphi$  is well-defined. To show that  $\varphi$  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  $\varphi$  is injective. To show  $\varphi$  is surjective, note that  $\sigma(a, x) = \varphi(aG_x)$ , for all  $a \in G$ . Therefore,  $\varphi$  is bijective.  $\square$

**Corollary 7.2.7 (Class Equation).** *Let  $\sigma : G \times X \rightarrow X$  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  $X = \bigsqcup_{x \in \mathcal{O}} \text{Orb}_G(x)$ , the result follows from Proposition 7.2.6.  $\square$

**Exercise 7.2.9.** 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 7.2.10.** Fix  $n \in \mathbb{N}$ . Show that the map  $\sigma : \text{GL}_n(\mathbb{R}) \times \mathbb{R}^n \rightarrow \mathbb{R}^n$  defined by

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

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

**Exercise 7.2.11.** Let  $\sigma : G \times G \rightarrow G$  be the left  $G$ -action on itself given by

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

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

**Theorem 7.2.8 (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  $|T| = \sum_{a \in G} F(a)$ . Also  $|T| = \sum_{x \in X} |G_x|$ , where  $G_x$  is the stabilizer of  $x \in X$ . Let  $\{x_1, \dots, x_n\}$  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  $\text{Orb}_G(x) = \text{Orb}_G(y)$ . Since  $|G|/|G_x| = [G : G_x] = |\text{Orb}_G(x)|$ , we conclude that  $|G_x| = |G_y|$  whenever  $x$  and  $y$  are in the same  $G$ -orbit. Then we have

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

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

### 7.3 Class equation for conjugacy action

Let  $G$  be a group. Consider the map

$$(7.3.0.1) \quad \sigma : G \times G \rightarrow G, (a, b) \mapsto aba^{-1}.$$

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

$$G_a = \{g \in G : gag^{-1} = a\} = \{g \in G : ga = ag\}.$$

is a subgroup of  $G$ , called the *centralizer* or the *normalizer* of  $a$  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  $a \in G$ , its  $G$ -orbit

$$(7.3.0.2) \quad \text{Orb}_G(a) = \{gag^{-1} : g \in G\}$$

consists of all conjugates of  $a$  in  $G$ , and is called the *conjugacy class* of  $a$  in  $G$ .

**Definition 7.3.1.** A partition of an integer  $n \geq 1$  is a finite sequence of positive integers  $(n_1, \dots, n_r)$  such that  $n_1 \geq \dots \geq n_r$  and  $\sum_{j=1}^r n_j = n$ .

**Exercise 7.3.1.** Fix an integer  $n \geq 2$ . Show that the number of conjugacy classes in  $S_n$  is the number of partitions of  $n$ .

*Solution:* Let  $\mathcal{C} = \{C_1, \dots, C_k\}$  be the set of all distinct conjugacy classes in  $S_n$ . Let  $\mathcal{P}_n$  be the set of all partitions of  $n$ . Define a map  $t : \mathcal{C} \rightarrow \mathcal{P}_n$  by sending  $C_i \in \mathcal{C}$  to the cycle type of an element of  $C_i$ , for all  $i$ . Since two elements of  $S_n$  are conjugate in  $S_n$  if and only if they have the same cycle type by Theorem 2.2.6, the map  $t$  is well-defined and injective. Given a partition  $(n_1, \dots, n_r)$  of  $n$ , we have a permutation  $\sigma = (1 \ \dots \ n_1) \circ \dots \circ (n_1 + \dots + n_{r-1} + 1 \ \dots \ n_1 + \dots + n_r) \in S_n$  whose cycle type is precisely  $(n_1, \dots, n_r)$ . Therefore,  $t$  is surjective, and hence is bijective, as required.  $\square$

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

$$(7.3.0.3) \quad \sigma : G \times \mathcal{P}(G) \rightarrow \mathcal{P}(G), \quad (a, S) \mapsto aSa^{-1},$$

where

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

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

$$(7.3.0.4) \quad N_G(S) := \{a \in G : aSa^{-1} = S\}$$

for the conjugation action in (7.3.0.3), is a subgroup of  $G$ , known as the *normalizer* of  $S$  in  $G$ . Then we have the following.

**Corollary 7.3.1.** *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 7.2.6.  $\square$

**Exercise 7.3.2.** Let  $\sigma = (k_1 \ \dots \ k_r) \in S_n$  be a  $r$ -cycle in  $S_n$ . Let  $I_n \setminus \sigma := I_n \setminus \{k_1, \dots, k_r\} \subset I_n$ , and let

$$S(I_n \setminus \sigma) := \left\{ \tau \in S_n : \tau|_{\{k_1, \dots, k_r\}} = \text{Id}_{\{k_1, \dots, k_r\}} \right\}.$$

- (i) Show that  $S(I_n \setminus \sigma)$  is a subgroup of  $S_n$ .
- (ii) Show that  $|C_{S_n}(\sigma)| = r(n - r)!$ .
- (iii) Deduce that  $C_{S_n}(\sigma) = \{\sigma^i \tau \in S_n : \tau \in S(I_n \setminus \sigma)\}$ . (*Hint:* Note that  $\sigma$  commutes with  $e, \sigma, \dots, \sigma^{r-1}$ , and with all  $\tau \in S_n$  whose cycles are disjoint from that of  $\sigma$  (precisely elements of  $S(I_n \setminus \sigma)$ ). Then use part (ii).)
- (iv) Compute  $C_{S_7}(\sigma)$ , where  $\sigma = (1 \ 2 \ 3) \in S_7$ .

**Exercise 7.3.3.** Let  $G$  be a group and  $S$  a non-empty subset of  $G$ . If  $H$  is the subgroup of  $G$  generated by  $S$ , show that  $N_G(S) \leq N_G(H)$ .

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 7.3.2** (Class Equation). *Let  $G$  be a finite group, and let  $\{a_1, \dots, a_n\}$  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 7.2.7 by taking  $X = G$  and  $\sigma$  to be the conjugation action of  $G$  on itself.  $\square$

**Corollary 7.3.3.** *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 7.3.2) for the conjugacy action of  $G$  on itself gives

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

where  $\{a_1, \dots, a_n\}$  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  $|Z(G)| = p^n - \sum_{i=1}^r p^{n_i}$  is divisible by  $p$ . Therefore,  $Z(G) \neq \{e\}$ .  $\square$

**Corollary 7.3.4.** *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 7.3.3, we see that  $G/Z(G)$  has order  $p$  or  $1$ , and hence is cyclic. Then  $G$  is abelian by Exercise 4.4.1. 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 4.2.2). 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 1.4.1 with

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



by Lemma 1.4.3, we have  $G = HK$ . Then  $G \cong H \times K$  by Theorem 6.1.7.  $\square$

**Proposition 7.3.5.** *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 1.3.9. Assume that  $H := \langle a \rangle$  is a proper non-trivial subgroup of  $G$ . Let  $m := \text{ord}(a)$ . 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  $b^p H = (bH)^p = H$  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  $\text{ord}(b^m) \mid p$ . Since  $p$  is a prime number, either  $b^m = e$  or  $\text{ord}(b^m) = p$ . If  $b^m = e$ , then  $(bH)^m = b^m H = eH = H$ , and so  $p = \text{ord}(bH) \mid m$ . This contradicts our assumption that  $p \nmid m$ . Therefore,  $b^m \neq e$ , and hence  $\text{ord}(b^m) = p$ .  $\square$

**Theorem 7.3.6 (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

$$(7.3.0.5) \quad |G| = |Z(G)| + \sum_{i=1}^r [G : C_G(a_i)],$$

where  $\{a_1, \dots, a_r\}$  is the subset of  $G$  consisting of exactly one element from each  $G$ -orbit 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  $i \in \{1, \dots, r\}$ . If  $p \mid |C_G(a_i)|$ , for some  $i \in \{1, \dots, r\}$ , then by induction hypothesis  $C_G(a_i) \subseteq G$  has an element of order  $p$ , and we are done. Suppose that  $p \nmid |C_G(a_i)|$ ,  $\forall i \in \{1, \dots, r\}$ . Since  $p \mid n = |G|$  and  $|G| = |C_G(a_i)|[G : C_G(a_i)]$ , we see that  $p \mid [G : C_G(a_i)]$ ,  $\forall i \in \{1, \dots, r\}$ . 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 7.3.5. This completes the proof.  $\square$

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

**Corollary 7.3.7.** *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 7.3.6)  $G$  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 5.5.1. Since  $|K| = |S| \cdot |H| = kp = m$ , that  $K$  is a required subgroup of  $G$  of order  $m$ . This completes the proof.  $\square$

## 7.4 $p$ -groups

**Definition 7.4.1 ( $p$ -group).** Let  $p \in \mathbb{N}$  be a prime number. A group  $G$  is said to be a  $p$ -group if every element of  $G$  has order equal to a power of  $p$ . A subgroup  $H$  of  $G$  is called a  $p$ -subgroup of  $G$  if  $H$  is a  $p$ -group.

**Example 7.4.1.**  $D_4$  and  $K_4$  are 2-groups.

**Example 7.4.2.** Given a prime number  $p > 0$ , let

$$\mathbb{Z}_{(p)} := \left\{ \frac{m}{p^n} \in \mathbb{Q} : m, n \in \mathbb{Z} \right\}.$$

Clearly  $\mathbb{Z}_{(p)}$  is a non-empty subset of  $\mathbb{Q}$ . Since given  $m/p^n, k/p^\ell \in \mathbb{Z}_{(p)}$ , we have

$$\frac{m}{p^n} - \frac{k}{p^\ell} = \frac{mp^\ell - np^n}{p^{n+\ell}} \in \mathbb{Z}_{(p)},$$

we conclude that  $\mathbb{Z}_{(p)}$  is a subgroup of  $\mathbb{Q}$ . Note that  $\text{ord}(m/p^n)$  is a power of  $p$ , and hence  $\mathbb{Z}_{(p)}$  is a  $p$ -group.

**Proposition 7.4.1.** A finite group  $G$  is a  $p$ -group if and only if  $|G| = p^n$ , for some  $n \in \mathbb{N}$ .

*Proof.* If  $|G| = p^n$ , for some  $n \in \mathbb{N}$ , then given  $a \in G$ ,  $\text{ord}(a) \mid p^n$  by Lagrange's theorem (Theorem 4.2.2), and hence  $\text{ord}(a) = p^r$ , for some  $r \in \{1, \dots, n\}$ , since  $p$  is a prime number.

Conversely suppose that  $G$  is a finite  $p$ -group. If  $|G| \neq p^n$ , for all  $n \in \mathbb{N} \cup \{0\}$ , then there exists a prime number  $q \neq p$  such that  $q \mid |G|$ . Then by Cauchy's

theorem  $G$  has an element of order  $q$ , which is not of the form  $p^n$ , for any  $n \in \mathbb{N}$ . This contradicts our assumption that  $G$  is a  $p$ -group. This completes the proof.  $\square$

**Lemma 7.4.2.** *Subgroup of a  $p$ -group is a  $p$ -group.*

*Proof.* Follows from the definition.  $\square$

**Lemma 7.4.3.** *Let  $G$  be a group (not necessarily finite), and  $p > 0$  a prime number. Then any  $p$ -subgroup of  $G$  is contained in a maximal  $p$ -subgroup of  $G$ .*

*Proof.* Let  $P$  be a  $p$ -subgroup of  $G$ . Let  $\mathcal{P}$  be the set of all  $p$ -subgroups of  $G$  containing  $P$ . Given  $P, Q \in \mathcal{P}$  we define  $P \leq Q$  if  $P \subseteq Q$ . Clearly this is a partial order relation on  $\mathcal{P}$ . Given a chain  $(P_n)_{n \geq 0}$  of elements from  $\mathcal{P}$  with  $P = P_0 \leq P_1 \leq \dots$ , the subset  $P := \bigcup_{n \geq 0} P_n$  is a  $p$ -subgroup of  $G$  (verify!), and hence is an element of  $\mathcal{P}$ . Then by Zorn's lemma  $\mathcal{P}$  has a maximal element, say  $P_{\max} \in \mathcal{P}$ . This completes the proof.  $\square$

**Proposition 7.4.4.** *Any finite non-trivial  $p$ -group have non-trivial center.*

*Proof.* Let  $G$  be a  $p$ -group of order  $p^n$ , for some prime number  $p > 0$  and positive integer  $n > 0$ . Then the class equation for the conjugacy action of  $G$  on itself gives

$$|G| = |Z(G)| + \sum_{a \in \mathcal{O} \setminus Z(G)} [G : C_G(a)],$$

where  $\mathcal{O}$  is a subset of  $G$  consisting of exactly one element from each  $G$ -orbits. Since  $C_G(a) = G$  if and only if  $a \in Z(G)$ , we see that  $[G : C_G(a)] > 1$  for all  $a \in \mathcal{O} \setminus Z(G)$ . Since  $|G| = p^n$ , it follows from Lagrange's theorem that  $p$  divides  $[G : C_G(a)]$ ,  $\forall a \in \mathcal{O} \setminus Z(G)$ . Then from the class equation above we see that  $p$  divides  $|Z(G)|$ . Since  $|Z(G)| \geq 1$ , it follows that  $Z(G) \neq \{e\}$ .  $\square$

**Corollary 7.4.5.** *Let  $p > 0$  be a prime number. Then every group of order  $p^2$  is abelian.*

*Proof.* Let  $G$  be a group of order  $p^2$ . Then by Proposition 7.4.4 above,  $Z(G) \neq \{e\}$ . Then  $|Z(G)| \in \{p, p^2\}$  by Lagrange's theorem. If  $|Z(G)| = p$ , then the quotient group  $G/Z(G)$  has order  $p$ , and hence is cyclic by Corollary 4.2.4. Then  $G$  is abelian by Exercise 4.4.1, which is a contradiction. Therefore,  $|Z(G)| = p^2 = |G|$ , and hence  $G = Z(G)$ . Therefore,  $G$  is abelian.  $\square$

**Lemma 7.4.6.** *Let  $G$  be a group of order  $p^n$ , where  $p > 0$  is a prime number and  $n \in \mathbb{N}$ . Let  $X$  be a non-empty finite set admitting a left  $G$ -action. Let*

$$X_0 := \{x \in X : ax = x, \forall a \in G\}$$

*be the subset of  $X$  consisting of elements with singleton  $G$ -orbits. Then  $|X| \equiv |X_0| \pmod{p}$ . In particular, if  $p \nmid |X|$ , there exists  $x \in X$  with singleton  $G$ -orbit.*

*Proof.* The class equation for the left  $G$ -action on  $X$  gives

$$|X| = |X_0| + \sum_{x \in \mathcal{O} \setminus X_0} [G : G_x],$$

where  $\mathcal{O}$  is the subset of  $X$  consisting of exactly one element from each  $G$ -orbits of  $X$ . Since  $[G : G_x] = |\text{Orb}_G(x)| > 1$ , for all  $x \in \mathcal{O} \setminus X_0$ , and  $|G| = p^n$ , we conclude that  $p$  divides  $[G : G_x]$ , for all  $x \in \mathcal{O} \setminus X_0$ . Then the result follows by reducing the class equation above modulo  $p$ . If  $p \nmid |X|$ , then  $|X_0| \not\equiv 0 \pmod{p}$ , and hence the second part follows.  $\square$

**Corollary 7.4.7.** *Let  $G$  be a finite group having a subgroup  $H$  of order  $p^n$ , where  $p > 0$  is a prime number and  $n \in \mathbb{N}$ . Then  $[G : H] \equiv_p [N_G(H) : H]$ . In particular, if  $p \mid [G : H]$ , then  $N_G(H) \neq H$ .*

*Solution:* Take  $X = \{aH : a \in G\}$  to be the set of all left cosets of  $H$  in  $G$ . Then  $H$  acts on  $X$  by

$$\sigma : H \times X \rightarrow X, \quad (h, aH) \mapsto (ha)H.$$

Note that  $\sigma$  is a well-defined map and is a left  $H$ -action on  $X$ . Moreover the subset of  $X$  consisting of singleton  $H$ -orbits is given by

$$\begin{aligned} X_0 &= \{aH \in X : \sigma(h, aH) = aH, \forall h \in H\} \\ &= \{aH \in X : a^{-1}ha \in H, \forall h \in H\} \\ &= \{aH \in X : a \in N_G(H)\}, \end{aligned}$$

we have  $|X_0| = [N_G(H) : H]$ . Since  $|X| = [G : H]$ , the result follows from Lemma 7.4.6.  $\square$

## 7.5 Simple Groups

**Definition 7.5.1.** A group is said to be *simple* if it has no non-trivial proper normal subgroup.

**Example 7.5.1.** Any group of prime order is simple (c.f. Lagrange's theorem).

**Lemma 7.5.1.** *A finite abelian group  $G$  is simple if and only if  $|G|$  is a prime number.*

*Proof.* If  $|G| = p$ , for some prime number, then its only subgroups are  $\{e\}$  and  $G$ , and hence  $G$  is simple in this case. To see the converse, note that if  $|G|$  is composite, then  $|G| = pk$ , for some prime number  $p$  and an integer  $k > 1$ . Then by Cauchy's theorem (Theorem 7.3.6)  $G$  has an element, say  $a \in G$ , of order  $p$ . Since  $G$  is abelian, the cyclic subgroup  $H := \langle a \rangle$  of  $G$  is normal in  $G$ . Since  $1 < |H| = p < |G|$ , it follows that  $H$  is a non-trivial proper normal subgroup of  $G$ . Thus  $G$  is not simple.  $\square$

**Exercise 7.5.1.** Let  $G$  be a finite group of order  $pq$ , where  $p$  and  $q$  are primes (not necessarily distinct). Show that  $G$  is not simple.

*Solution:* If  $p = q$ , then  $|G| = p^2$ , and so  $G$  is abelian by Corollary 7.4.5. Then  $G$  is not simple by Lemma 7.5.1. If  $p \neq q$ , without loss of generality we assume that  $p > q$ . Then by Cauchy's theorem  $G$  has a subgroup, say  $H$ , of order  $p$ . To show  $G$  is not simple, it suffices to show that  $H$  is normal. If possible suppose that there exists  $a \in G$  such that  $aHa^{-1} \neq H$ . Since both  $H$  and  $K_a := aHa^{-1}$  are subgroups of  $G$  of order  $p$ , their intersection  $H \cap K_a$  is a subgroup (see Lemma 1.2.3) of order 1 or  $p$  by Lagrange's theorem (Theorem 4.2.2). Since  $H \neq K_a$  by assumption,  $|H \cap K_a| = 1$ . Then the subset  $HK_a \subseteq G$  has cardinality

$$|HK_a| = \frac{|H| \cdot |K_a|}{|H \cap K_a|} = p^2 > pq = |G|,$$

which is a contradiction. Therefore,  $aHa^{-1} = H$ ,  $\forall a \in G$ , and hence  $H$  is normal in  $G$ .  $\square$

**Exercise 7.5.2.** Let  $G$  be an abelian group having finite subgroups  $H$  and  $K$  of orders  $m$  and  $n$ , respectively. Show that  $G$  has a subgroup of order  $d := \text{lcm}(m, n)$ .

*Solution.* Since  $G$  is abelian, both  $H$  and  $K$  are normal in  $G$ , and hence  $HK$  is a subgroup of  $G$  of order at most  $|H| \cdot |K| = mn$ . Since  $H$  and  $K$  are subgroups of  $HK$ , by Lagrange's theorem both  $m$  and  $n$  divides  $|HK|$ , and hence  $d := \text{lcm}(m, n)$  divides  $|HK|$ . Since  $G$  is abelian, so is its subgroup  $HK$ . Then by Corollary 7.3.7  $HK$  has a subgroup, say  $V$  of order  $d$ . Since  $V$  is also a subgroup of  $G$ , we are done.  $\square$

**Exercise 7.5.3.** Let  $G$  be a non-abelian group of order  $p^3$ , where  $p$  is a prime number. Show that  $|Z(G)| = p$ .

*Solution:* Since  $G$  has order  $p^3$ , it has non-trivial center. Since  $G$  is non-abelian, so  $Z(G) \neq G$ . Then by Lagrange's theorem  $Z(G)$  has order  $p$  or  $p^2$ . If  $|Z(G)| = p^2$ , then  $G/Z(G)$  has order  $p$ , and hence is a cyclic group. Then  $G$  is abelian by Exercise 4.4.1, which is a contradiction. Therefore,  $|Z(G)| = p$ .  $\square$

**Exercise 7.5.4.** Let  $G$  be a finite abelian group. Let  $n \in \mathbb{N}$  be such that  $n \mid |G|$ . Show that the number of solutions of the equation  $x^n = e$  in  $G$  is a multiple of  $n$ .

*Solution:* The set of all solutions of  $x^n = e$  in  $G$  is given by

$$H := \{a \in G : a^n = e\}.$$

Since  $e^n = e$ , we see that  $H \neq \emptyset$ . Let  $a, b \in H$  be given. Since  $G$  is abelian, we have  $(a^{-1}b)^n = (a^n)^{-1}b^n = e^{-1}e = e$ , and so  $a^{-1}b \in H$ . Therefore,  $H$  is

a subgroup of  $G$ . Since  $G$  is a finite abelian group and  $n \mid |G|$ , by Corollary 7.3.7  $G$  has a subgroup, say  $K$  of order  $n$ . Then by Corollary 4.2.3 we have  $a^n = e$ ,  $\forall a \in K$ , and hence  $K \subseteq H$ . Since  $|K| = n$ , by Lagrange's theorem we have  $n \mid |H|$ .  $\square$

**Exercise 7.5.5.** Let  $G$  be a group of order  $p^n$ , where  $p > 0$  is a prime number and  $n \in \mathbb{N}$ . Let  $H$  be a subgroup of  $G$  of order  $p^{n-1}$ . Show that  $H$  is normal in  $G$ .

*Solution:* Follows from Corollary 7.2.5.  $\square$

**Exercise 7.5.6.** Show that  $N := \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \subset A_4$  is the unique subgroup of order 4 in  $A_4$ , and hence is normal in  $A_4$ . Conclude that  $A_4$  is not simple.

Next we show that  $A_n$  is simple, for all  $n \geq 5$ . We begin with some useful observations.

**Lemma 7.5.2.** Fix an integer  $n \geq 5$ , and let  $H$  be a normal subgroup of  $A_n$ . If  $H$  contains a 3-cycle, then  $H = A_n$ .

*Proof.* Suppose that  $H$  contains a 3-cycle, say  $\sigma = (a\ b\ c) \in H$ . Since  $A_n$  is generated by 3-cycles, it suffices to show that any 3-cycle is contained in  $H$ . Let  $\tau = (u\ v\ w)$  be any 3-cycle. Let  $\pi \in S_n$  be such that

$$\pi(a) = u, \pi(b) = v \text{ and } \pi(c) = w.$$

Then by Proposition 2.2.1 we have

$$\pi\sigma\pi^{-1} = (\pi(a)\ \pi(b)\ \pi(c)) = (u\ v\ w) = \tau.$$

Since  $H$  is a normal subgroup of  $A_n$ , it follows that  $\tau \in H$  whenever  $\pi \in A_n$ .

If  $\pi$  is odd, then we replace  $\pi$  with  $\pi\delta$ , where  $\delta = (d\ f) \in S_n$  for some  $d, f \in I_n \setminus \{a, b, c\}$  with  $d \neq f$ , and we can always do this because of our assumption  $n \geq 5$ . Since the 2-cycle  $\delta = \delta^{-1}$  is disjoint from  $\sigma$ , they commute, and so  $(\pi\delta)\sigma(\pi\delta)^{-1} = \pi\sigma\pi^{-1} = \tau$ , as required. This completes the proof.  $\square$

**Corollary 7.5.3.** Fix an integer  $n \geq 5$ , and let  $H$  be a normal subgroup of  $A_n$ . If  $H$  contains a product of two disjoint transpositions, then  $H = A_n$ .

*Proof.* Let  $(a\ b)$  and  $(c\ d)$  be two disjoint transpositions in  $S_n$  such that  $(a\ b) \circ (c\ d) \in H$ . To show that  $H = A_n$ , in view of Lemma 7.5.2, it suffices to show that  $H$  contains a 3-cycle. Since  $n \geq 5$ , we can choose an element  $f \in I_n \setminus \{a, b, c, d\}$ . Then the 3-cycle  $\pi := (c\ d\ f) \in A_n$ . Since  $H$  is normal in  $A_n$ , we have  $\pi \circ (a\ b) \circ (c\ d) \circ \pi^{-1} \in H$ . But

$$\begin{aligned} \pi \circ (a\ b) \circ (c\ d) \circ \pi^{-1} &= (c\ d\ f) \circ (a\ b) \circ (c\ d) \circ (c\ f\ d) \\ &= (a\ b) \circ (d\ f). \end{aligned}$$

Since  $H$  is a group containing  $(a\ b) \circ (c\ d)$  and  $(a\ b) \circ (d\ f)$ , we have

$$\pi = (c\ d\ f) = (a\ b) \circ (c\ d) \circ (a\ b) \circ (d\ f) \in H,$$

as required. This completes the proof.  $\square$

**Theorem 7.5.4.** *The alternating group  $A_n$  is simple, for all  $n \geq 5$ .*

*Proof.* Let  $H$  be a non-trivial normal subgroup of  $A_n$ . To show  $A_n$  is simple, thanks to Lemma 7.5.2, it suffices to show that  $H$  contains a 3-cycle.

Let  $\sigma \in H \setminus \{e\}$  be a permutation that moves the smallest number of elements, say  $r$ , of  $I_n := \{1, \dots, n\}$ . If  $r = 2$ , then  $\sigma$  must be a transposition, which is not possible since then  $\sigma$  would be odd while  $H \subseteq A_n$ . Therefore,  $r \geq 3$ . If we can show that  $r = 3$ , then  $\sigma$  must be a 3-cycle and we are done.

Suppose on the contrary that  $r > 3$ . Write  $\sigma$  as a product of finite number of disjoint cycles, say  $\sigma = \sigma_1 \circ \dots \circ \sigma_k$ , where  $\sigma_j$  is a cycle in  $S_n$ , for all  $j \in \{1, \dots, k\}$ .

**Step 1:** Suppose that  $\sigma_j$  is a transposition, for all  $j \in \{1, \dots, k\}$ . Then  $k \geq 2$ , for otherwise  $\sigma = \sigma_1$  would be odd, a contradiction. Let  $\sigma_1 = (a\ b)$  and  $\sigma_2 = (c\ d)$  in  $S_n$ . Since  $\sigma_1$  and  $\sigma_2$  are disjoint cycles and  $n \geq 5$ , there exists an element  $f \in I_n \setminus \{a, b, c, d\}$ . Let  $\tau := (c\ d\ f) \in S_n$ . Since  $\tau$  is even,  $\tau \in A_n$ . Since  $\sigma \in H$  and  $H$  is normal in  $A_n$ , we have  $\tau\sigma\tau^{-1} \in H$ . Since  $H$  is a group,

$$\sigma' := [\sigma^{-1}, \tau] = \sigma^{-1}\tau\sigma\tau^{-1} \in H.$$

Since  $\sigma$  permutes  $a$  and  $b$ , we see that  $\sigma'(a) = a$  and  $\sigma'(b) = b$ . If  $u \in I_n \setminus \{a, b, c, d, f\}$  is such that  $\sigma(u) = u$ , then  $\sigma'(u) = (\sigma^{-1}\tau\sigma\tau^{-1})(u) = u$ . Since  $\sigma'(f) = c$ , we have  $\sigma' \neq e$ . Therefore,  $\sigma' \in H \setminus \{e\}$  moves fewer elements of  $I_n$  than  $\sigma$ , which is a contradiction. Therefore, at least one  $\sigma_i$  must be a cycle of length  $\geq 3$ . Since disjoint cycles commutes, we may assume that  $\sigma_1 = (a\ b\ c\ \dots)$  is a cycle of length  $\geq 3$ .

**Step 2:** If  $r = 4$ , then either  $\sigma$  is a product of two disjoint transpositions or is a 4-cycle. The first possibility is ruled out by step 1 and the second possibility is ruled out since a 4-cycle is odd and  $\sigma \in H \subseteq A_n$ . Therefore,  $r \geq 5$ .

**Step 3:** Since  $n \geq 5$ , we can choose  $d, f \in I_n \setminus \{a, b, c\}$  with  $d \neq f$ . Let  $\tau = (c\ d\ f) \in A_n$ . As before,  $H$  being a normal subgroup of  $A_n$  containing  $\sigma$ , we have  $\sigma' := \sigma^{-1}\tau\sigma\tau^{-1} \in H$ . Since  $\sigma'(b) \neq b$ , we have  $\sigma' \neq e$ . Given any  $u \in I_n \setminus \{a, b, c, d, f\}$ , if  $\sigma(u) = u$ , then  $\sigma'(u) = (\sigma^{-1}\tau\sigma\tau^{-1})(u) = u$ . Moreover  $\sigma(a) \neq a$  while  $\sigma'(a) = a$ . Therefore,  $\sigma' \in H \setminus \{e\}$  moves fewer elements of  $I_n$  than  $\sigma$ , which is a contradiction. Therefore, we must have  $r = 3$ , and hence  $\sigma$  must be a 3-cycle. Hence the result follows.  $\square$





## Chapter 8

### Miscellaneous Exercises

Let  $G$  be a group.

- Q1. Given a subset  $A \subseteq G$ , we define  $N_G(A) := \{a \in G : a^{-1}Aa = A\}$ . Show that
- (i)  $N_G(A)$  is a subgroup of  $G$ .
  - (ii) If  $H$  is a subgroup of  $G$ , show that  $H \leq N_G(H)$ .
  - (iii) If  $H$  is a subgroup of  $G$ , show that  $N_G(H)$  is the largest subgroup of  $G$  in which  $H$  is normal.
  - (iv) Show by an example that  $A$  need not be a subset of  $N_G(A)$ .
- Q2. Given a subset  $A$  of  $G$ , let  $C_G(A) := \{a \in G : aba^{-1} = b, \forall b \in A\}$ .
- (i) Show that  $C_G(A)$  is a subgroup of  $G$ .
  - (ii) If  $H$  is a subgroup of  $G$ , show that  $H \leq C_G(H)$  if and only if  $H$  is abelian.
- Q3. If  $\mathcal{N}$  is a family of normal subgroups of  $G$ , show that  $\bigcap_{N \in \mathcal{N}} N$  is normal in  $G$ .
- Q4. If  $N$  is a normal subgroup of  $G$ , show that  $H \cap N$  is normal in  $H$ , for any subgroup  $H$  of  $G$ .
- Q5. Let  $N$  be a finite subgroup of  $G$ . Suppose that  $N = \langle S \rangle$  and  $G = \langle T \rangle$ , for some subsets  $S$  and  $T$  of  $G$ . Show that  $N$  is normal in  $G$  if and only if  $tSt^{-1} \subseteq N$ , for all  $t \in T$ .
- Q6. Find all normal subgroups of the dihedral group  $D_8 = \langle r, s : \text{ord}(r) = 4, \text{ord}(s) = 2, sr = r^{-1}s \rangle$ , and identify the associated quotient groups.
- Q7. Fix an integer  $n \geq 3$ , and let  $D_{2n} = \langle r, s : \text{ord}(r) = n, \text{ord}(s) = 2, sr = r^{-1}s \rangle$  be the dihedral group of degree  $n$  and order  $2n$ .

(a) Show that

$$Z(D_{2n}) = \begin{cases} \{e\}, & \text{if } n \text{ is odd, and} \\ \{e, r^k\}, & \text{if } n = 2k \text{ is even.} \end{cases}$$

(b) If  $k \in \mathbb{N}$  divides  $n$ , show that  $\langle r^k \rangle$  is a normal subgroup of  $D_{2n}$ , and the associated quotient group  $D_{2n}/\langle r^k \rangle$  is isomorphic to  $D_{2k}$ .

Q8. Let  $G$  and  $H$  be groups.

- (i) Show that  $\{(a, e_H) : a \in G\}$  is a normal subgroup of  $G \times H$  and the associated quotient group is isomorphic to  $H$ .
- (ii) If  $G$  is abelian, show that the diagonal  $\Delta_G := \{(a, a) : a \in G\}$  of  $G$  is a normal subgroup of  $G \times G$ , and the associated quotient group is isomorphic to  $G$ .
- (iii) Show that the diagonal subgroup  $\Delta_{S_3} \subseteq S_3 \times S_3$  is not normal in  $S_3 \times S_3$ .

Q9. Let  $H$  and  $K$  be subgroups of  $G$  with  $H \leq K$ . Show that  $[G : H] = [G : K][K : H]$ .

Q10. Let  $G$  be a finite group. Let  $H$  and  $N$  be subgroups of  $G$  with  $N$  normal in  $G$ . If  $\gcd(|H|, [G : N]) = 1$ , show that  $H$  is a subgroup of  $N$ .

Q11. Let  $N$  be a normal subgroup of a finite group  $G$ . If  $\gcd(|N|, [G : N]) = 1$ , show that  $N$  is the unique subgroup of order  $|N|$  in  $G$ .

Q12. Let  $H$  be a normal subgroup of  $G$ . Given any subgroup  $K$  of  $G$ , show that  $H \cap K$  is normal in  $HK$ .

Q13. Show that  $\mathbb{Q}$  has no proper subgroup of finite index. Deduce that  $\mathbb{Q}/\mathbb{Z}$  has no proper subgroup of finite index.

Q14. Let  $H$  and  $K$  be subgroups of  $G$  with  $[G : H] = m < \infty$  and  $[G : K] = n < \infty$ . Show that  $\text{lcm}(m, n) \leq [G : H \cap K] \leq mn$ . Deduce that  $[G : H \cap K] = [G : H][G : K]$  whenever  $\gcd(m, n) = 1$ .

Q15. Show that  $S_4$  cannot have normal subgroups of orders 8 and 3.

Q16. Find the last two digits of  $3^{3^{100}}$ .

Q17. Let  $H$  and  $K$  be subgroups of  $G$ . If  $H \subseteq N_G(K)$ , then show that

- (i)  $HK$  is a subgroup of  $G$ ,
- (ii)  $K$  is normal in  $HK$ ,
- (iii)  $H \cap K$  is normal in  $H$ , and
- (iv)  $H/(H \cap K) \cong HK/K$ .

- Q18. If  $H$  is a normal subgroup of  $G$  with  $[G : H] = p$ , a prime number, show that for any subgroup  $K$  of  $G$ , either
- (i)  $K$  is a subgroup of  $H$ , or
  - (ii)  $G = HK$  and  $[K : H \cap K] = p$ .
- Q19. Let  $H$  and  $K$  be normal subgroups of  $G$  such that  $G = HK$ . Show that  $G/(H \cap K) \cong (G/H) \times (G/K)$ .
- Q20. Let  $G$  be a finite group of order  $p^r m$ , where  $p > 0$  is a prime number,  $r, m \in \mathbb{N}$  and  $\gcd(p, m) = 1$ . Let  $P$  be a subgroup of order  $p^r$ . Let  $N$  be a normal subgroup of  $G$  of order  $p^s n$ , where  $\gcd(p, n) = 1$ . Show that  $|P \cap N| = p^s$  and  $|PN/N| = p^{r-s}$ . Conclude that intersection of a Sylow  $p$ -subgroup of  $G$  with a normal subgroup  $N$  of  $G$  is a Sylow  $p$ -subgroup of  $N$ .
- Q21. A subgroup  $H$  of a finite group  $G$  is said to be a *Hall subgroup of  $G$*  if its index in  $G$  is relatively prime to its order; i.e., if  $\gcd([G : H], |H|) = 1$ .  
If  $H$  is a Hall subgroup of  $G$  and  $N$  is a normal subgroup of  $G$ , show that  $H \cap N$  is a Hall subgroup of  $N$  and  $HN/N$  is a Hall subgroup of  $G/N$ .
- Q22. A non-trivial abelian group  $G$  is said to be *divisible* if for each  $a \in G$  and non-zero integer  $n \in \mathbb{Z} \setminus \{0\}$ , there exists an element  $b \in G$  such that  $b^n = a$ ; i.e., each element of  $G$  has a  $n$ -th root in  $G$ , for all  $n \in \mathbb{Z} \setminus \{0\}$ . Prove the following.
- (i) Show that  $(\mathbb{Q}, +)$  is a divisible group.
  - (ii) Show that any non-trivial divisible group is infinite.
  - (iii) Show by an example that subgroup of a divisible group need not be divisible.
  - (iv) If  $G$  and  $H$  are non-trivial abelian groups, show that  $G \times H$  is divisible if and only if both  $G$  and  $H$  are divisible.
  - (v) Show that quotient of a divisible group by a proper subgroup is divisible.
- Q23. Find all generators and subgroups of  $\mathbb{Z}_{48}$ .
- Q24. Let  $G$  be a group. Given an element  $a \in G$ , show that there is a unique group homomorphism  $f : \mathbb{Z} \rightarrow G$  such that  $f(1) = a$ .
- Q25. Let  $G$  be a group. Let  $a \in G$  be such that  $a^n = e$ , for some integer  $n \geq 0$ , show that there is a unique group homomorphism  $\varphi : \mathbb{Z}_n \rightarrow G$  such that  $\varphi([1]) = a$ .
- Q26. Fix an integer  $n \geq 2$ . Given an integer  $k$ , let  $f_k : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$  be the map defined by  $f_k(x) = x^k$ ,  $\forall x \in \mathbb{Z}_n$ .

- (i) Show that  $f_k$  is a well-defined map.
  - (ii) Show that  $f_k \in \text{Aut}(\mathbb{Z}_n)$  if and only if  $\gcd(n, k) = 1$ .
  - (iii) Show that  $f_k = f_\ell$  if and only if  $\ell \equiv k \pmod{n}$ .
  - (iv) Show that every group automorphism of  $\mathbb{Z}_n$  is of the form  $f_k$ , for some  $k \in \mathbb{Z}$ .
  - (v) Show that  $f_k \circ f_\ell = f_{k\ell}$ ,  $\forall k, \ell \in \mathbb{Z}$ .
  - (vi) Deduce that the map  $f : \mathbb{Z}_n^\times \rightarrow \text{Aut}(\mathbb{Z}_n)$  defined by  $f(k) = f_k$ ,  $\forall k \in \mathbb{Z}_n^\times$ , is an isomorphism of  $\mathbb{Z}_n^\times := U_n$  onto the automorphism group  $\text{Aut}(\mathbb{Z}_n)$ .
  - (vii) Conclude that  $\text{Aut}(\mathbb{Z}_n)$  is an abelian group of order  $\phi(n)$ , where  $\phi$  denotes the Euler phi function.
- Q27. Fix an integer  $n \geq 3$ . Show that the multiplicative group  $G := (\mathbb{Z}/2^n\mathbb{Z})^\times$  has two distinct subgroups of order 2. Conclude that  $G$  is not cyclic.
- Q28. Let  $G$  be a finite group of order  $n$ . Let  $k \in \mathbb{N}$  with  $\gcd(n, k) = 1$ . Use Lagrange's theorem and Cauchy's theorem to show that the map  $f : G \rightarrow G$  defined by  $f(a) = a^k$ ,  $\forall a \in G$ , is surjective.
- Q29. Let  $m, n \geq 2$  be two integers. Find all group homomorphism  $f : \mathbb{Z}_m \rightarrow \mathbb{Z}_n$ .
- Q30. Let  $G$  be a group. Show that there is a one-to-one correspondence between the set of all group homomorphisms from  $\mathbb{Z}_m$  into  $G$  with the set of all solutions of the equations  $x^m = e_G$  in  $G$ .
- Q31. Find the number of group homomorphisms from  $\mathbb{Z}_n$  into  $\mathbb{Z}_m \times \mathbb{Z}_k$ .
- Q32. Find the number of all group homomorphisms from  $S_3$  into  $\mathbb{Z}_n \times \mathbb{Z}_m$ . (Hint: Use abelianization of  $S_3$ .)
- Q33. Let  $G$  be a group and  $H$  an abelian subgroup of  $G$ . Show that the subgroup  $\langle H, Z(G) \rangle$  is abelian. Give an example of a group  $G$  and an abelian subgroup  $H$  of  $G$  such that the subgroup  $\langle H, C_G(H) \rangle$  is not abelian, where  $C_G(H) = \{a \in G : a^{-1}ha = h, \forall h \in H\}$  is the *centralizer* of  $H$  in  $G$ .
- Q34. Show that the subgroup generated by any two distinct elements of order 2 in  $S_3$  is  $S_3$ .
- Q35. Show that any finitely generated subgroup of  $(\mathbb{Q}, +)$  is cyclic. Conclude that  $\mathbb{Q}$  is not finitely generated.
- Q36. Show that the subgroup of  $(\mathbb{Q}^*, \cdot)$  generated by the subset  $\{1/p \in \mathbb{Q}^+ : p \text{ is a prime number}\}$  is  $\mathbb{Q}^+$ , the multiplicative group of positive rational numbers.
- Q37. Show that any group of order 4 is isomorphic to either  $\mathbb{Z}_4$  or  $K_4$ .

Q38. Show that any group of order 6 is isomorphic to either  $\mathbb{Z}_6$  or  $S_3$ .

Q39. Let  $p > 0$  be a prime number, and let

$$G = \{z \in \mathbb{C}^* : z^{p^n} = 1, \text{ for some } n \in \mathbb{N} \cup \{0\}\}.$$

Prove the following.

- (i)  $G$  is a subgroup of  $\mathbb{C}^*$ .
  - (ii) The map  $F_p : G \rightarrow G$  given by  $z \mapsto z^p$ , is a surjective group homomorphism.
  - (iii) Find  $\text{Ker}(F_p)$ .
  - (iv) Show that  $G$  is isomorphic to a *proper quotient group* (i.e., quotient by a non-trivial normal subgroup) of itself.
- Q40. Let  $G$  be the additive group  $(\mathbb{R}, +)$ . Show that  $G$  is isomorphic to the product group  $G \times G$ . (*Hint:* Note that both  $\mathbb{R}$  and  $\mathbb{R} \times \mathbb{R}$  are  $\mathbb{Q}$ -vector spaces). Show that this fails for  $G = (\mathbb{Z}, +)$ .
- Q41. Let  $G$  be a finite group and let  $S(G)$  be the permutation group on  $G$ . Let  $\pi : G \rightarrow S(G)$  be the *left regular representation* of  $G$  (i.e.,  $\pi$  is the group homomorphism defined by sending  $a \in G$  to the permutation  $\sigma_a \in S(G)$  that sends  $b \in G$  to  $ab \in G$ ).
- (i) If  $a \in G$  with  $\text{ord}(a) = n$  and  $|G| = mn$ , show that  $\pi(a)$  is a product of  $m$  number of  $n$ -cycles.
  - (ii) Deduce that  $\pi(a)$  is an odd permutation if and only if  $\text{ord}(a)$  is even and  $|G|/\text{ord}(a)$  is odd.
  - (iii) If  $\pi(G)$  contains an odd permutation, show that  $G$  has a subgroup of index 2.
- Q42. If  $G$  is a finite group of order  $2n$ , where  $n$  is odd, show that  $G$  has a subgroup of index 2. (*Hint:* Use Cauchy's theorem and the previous exercise).
- Q43. Let  $G$  be finite group of order  $n$ , where  $n$  is not a prime number. If  $G$  has a subgroup of order  $r$ , for each positive integer  $r$  that divides  $n$ , show that  $G$  is not a simple group.
- Q44. Let  $G$  be a group. A subgroup  $H$  of  $G$  is said to be a *characteristic subgroup* of  $G$  if  $f(H) \subseteq H$ , for all  $f \in \text{Aut}(G)$ . Prove the following.
- (i) Characteristic subgroups are normal.
  - (ii) If  $H$  is the unique subgroup of a given finite order in  $G$ , then  $H$  is a characteristic subgroup of  $G$ .
  - (iii) If  $K$  is a characteristic subgroup of  $H$  and  $H$  is normal in  $G$ , show that  $K$  is normal in  $G$ .

- Q45. Compute the conjugacy class and the stabilizer of  $\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 7 & 1 & 6 & 4 \end{pmatrix} \in S_7$ .
- Q46. Let  $H$  be a subgroup of  $G$  with finite index  $[G : H] = n$ . Show that there is a normal subgroup  $K$  of  $G$  with  $K \subseteq H$  and  $[G : K] \leq n!$ .
- Q47. Show that every non-abelian group of order 6 has a non-normal subgroup of order 2. (*Hint*: Produce an injective group homomorphism  $G \rightarrow S_3$ ). Use this to show that, upto isomorphism, there are only two groups of order 6, namely  $S_3$  and  $\mathbb{Z}_6$ .
- Q48. Given any two groups  $G$  and  $H$ , we denote by  $\text{Hom}(G, H)$  the set of all group homomorphisms from  $G$  into  $H$ .
- (i) Find the number of elements of the set  $\text{Hom}(\mathbb{Z} \times \mathbb{Z}, \mathbb{Z}_n)$ , for all  $n \in \mathbb{N}$ .
  - (ii) Let  $G$  be an abelian groups of order  $n$ . Let  $r \in \mathbb{N}$ . Are the sets  $\text{Hom}(\mathbb{Z}^{\oplus r}, \mathbb{Z}_n)$  and  $\text{Hom}(\mathbb{Z}^{\oplus r}, G)$  have the same cardinality?
  - (iii) Find the number of group homomorphisms from  $\mathbb{Z} \times \mathbb{Z}$  to  $S_3$ . How many of them are surjective?
- Q49. Given any three groups  $G, H$  and  $K$ , show that there is a natural bijective map
- $$\text{Hom}(G, H) \times \text{Hom}(G, K) \longrightarrow \text{Hom}(G, H \times K).$$
- Q50. Let  $G$  be a finite group of order  $pq$ , where  $p, q$  are prime numbers with  $p \leq q$  and  $p \nmid (q - 1)$ . Show that  $G$  is abelian. If  $p < q$  and  $p \nmid (q - 1)$ , what can you say about  $G$ ?
- Q51. Let  $p > 0$  be a prime number. Let  $P$  be a non-trivial  $p$ -subgroup of  $S_p$ . Show that  $|N_{S_p}(P)| = p(p - 1)$ .