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.

Version: May 4, 2025 at 11:11pm (IST).
Available at: 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

List of Symbols

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

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

Some of the useful Greek alphabets

Chapter 1

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

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[1] of G is called the *order* of the group $(G, *)$, and we denote it by the symbol $|G|$. For notational simplicity,

[1] 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

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

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

(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

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

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

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

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 $e' = e$. □

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

$$\begin{aligned} & b'ab = b' \\ \Rightarrow\ & eb = b' \\ \Rightarrow\ & b = b'. \end{aligned}$$

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, and let $a, b, c \in G$.*

1. *If $ab = ac$ then $b = c$.*
2. *If $ac = bc$, then $a = b$.*

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

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 1.1.2. 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) *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) *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 μ_n is a group with respect to the binary operation given by multiplication of complex numbers. Note that μ_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

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

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

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

Now it is easy to see that,

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

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

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

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

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

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

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

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

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

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

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

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

Therefore, $[1] \in \mathbb{Z}_n$ is the multiplicative identity in $\mathbb{Z}_n$. 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

$$\begin{aligned} a_1k_1 + b_1n &= 1 \\ \text{and } \; a_2k_2 + b_2n &= 1. \end{aligned}$$

Multiplying these two equations, we have

$$(a_1a_2)(k_1k_2) + (a_1k_1b_2 + a_2k_2b_1 + b_1b_2)n = 1.$$

Then we have $\gcd(k_1k_2, n) = 1$. Therefore,

$$[k_1] \cdot [k_2] = [k_1k_2] \in \mathbb{Z}_n^\times, \; \forall \, [k_1], [k_2] \in \mathbb{Z}_n^\times.$$

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 $ab \neq ba$).

Example 1.1.7 (Opposite Group)**.** Given a group $(G, *)$, let G^{op} be the pair $(G, *^{\mathrm{op}})$, where $*^{\mathrm{op}}$ is the binary operation on G defined by

$$a *^{\mathrm{op}} b := b * a, \;\; \forall \, a, b \in G.$$

It is easy to check that $G^{\mathrm{op}} := (G, *^{\mathrm{op}})$ is a group, called the *opposite group* of G. Moreover, $G^{\mathrm{op}} = (G, *)$ if and only if G is abelian.

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

Example 1.1.8 (General linear group)**.** Fix a natural number $n \geq 1$, and consider the set $\mathrm{GL}_n(\mathbb{R})$ of all invertible $n \times n$ matrices with entries from $\mathbb{R}$. Note that $\mathrm{GL}_n(\mathbb{R})$ admits a natural binary operation given by matrix multiplication:

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

Note that

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

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

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

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

Example 1.1.9 (Special linear group)**.** Fix an integer $n \geq 2$, and let

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

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

$$\det(AB) = \det(A)\det(B), \tag{1.1.0.1}$$

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

Example 1.1.10 (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:

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

Note that

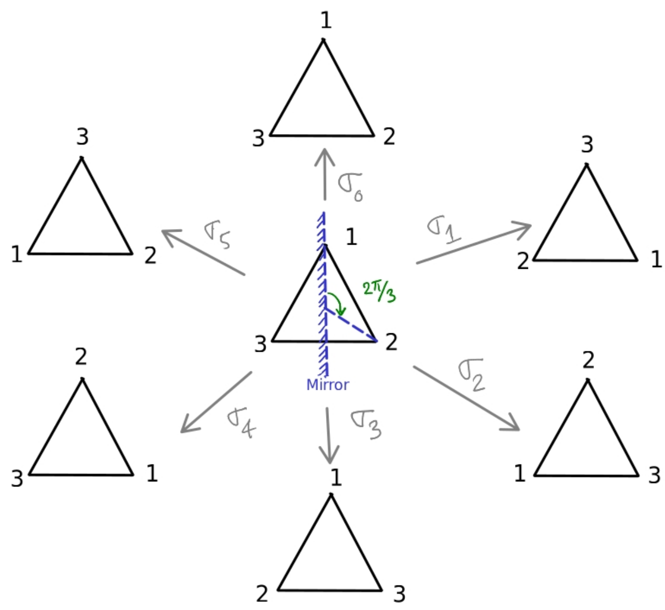
(i) given any $f, g, h \in S(X)$, we have $(f \circ g) \circ h = f \circ (g \circ h)$.

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

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

Thus, $S(X)$ is a group. We shall see in Exercise 1.1.3 that $S(X)$ is non-commutative if X has at least three elements.

Example 1.1.11 (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.



Symmetries of a triangle.

Note that, we have only six possible symmetries of $\triangle$ as follow:

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

Let $S_3 := \{\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$. Note that, each of symmetries are bijective maps from the set $J_3 := \{1, 2, 3\}$ onto itself, and any bijective map from J_3 onto itself is one of the symmetries in S_3. Since composition of bijective maps is bijective, 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 σ_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 1.1.3. 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 1.1.12. Fix an integer $n \geq 2$, and let $J_n := \{k \in \mathbb{N} : k \leq n\}$. Let S_n be the set of all bijective maps from $J_n = \{1, 2, 3, \ldots, n\}$ onto itself. Since the identity map $J_n \to J_n$ is a bijective map, so $S_n \neq \emptyset$. Since the composition of any two bijective maps $\sigma, \tau : J_n \to J_n$ is again a bijective map $\sigma \circ \tau : J_n \to J_n$, we have a binary operation on the set S_n given by sending $(\sigma, \tau) \in S_n \times S_n$ to $\sigma \circ \tau \in S_n$. Note that the set S_n together with this binary operation (composition of bijective maps) is a group of order $n! := n(n-1)\cdots 3 \cdot 2 \cdot 1$. One can easily show that S_n is non-commutative for $n \geq 3$. We shall study this group in details in Chapter §2.

Example 1.1.13. Define a binary operation on $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ by *component-wise addition:*

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

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

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

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

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

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

Exercise 1.1.4. 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:

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

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

Exercise 1.1.5 (Direct product of a finite family of groups)**.** Given a finite family of groups $\{G_1, \ldots, G_n\}$, not necessarily distinct, we define a binary operation on the Cartesian product $G := G_1 \times \cdots \times G_n$ by setting

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

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

(i) Show that G is a group with respect to the above defined binary operation; we call $G = G_1 \times \cdots \times G_n$ the *direct product* of $G_1, \ldots, G_n$.

(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 $0 \leq r \leq n-1$ 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 $0 \leq r \leq n-1$, 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 μ_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 μ_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 1.1.11.

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 $a, b \in H$.

Example 1.2.4. Consider the set $\mathbb{R}^* := \mathbb{R}\setminus\{0\}$ of all non-zero real numbers. Note that $\mathbb{R}^*$ is a group with respect to the multiplication of real numbers. Consider the subset $\mathbb{R}^+ := \{t \in \mathbb{R} : t > 0\}$ of $\mathbb{R}^*$. Since for any $s, t \in \mathbb{R}^+$, $s^{-1}t = t/s > 0$, we see that $\mathbb{R}^+$ is a subgroup of $\mathbb{R}^*$.

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 1.1.5. 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. □

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 $\mathrm{GL}_n(\mathbb{R})$ and $\mathrm{SL}_n(\mathbb{R})$, 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 $Z(G) = \bigcap\limits_{a\in G} C_G(a)$.

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 $\bigcap\limits_{\alpha\in\Lambda} H_\alpha$ is a subgroup of G.*

Proof. Since $e \in H_\alpha$, for all $\alpha \in \Lambda$, we have $e \in \bigcap\limits_{\alpha\in\Lambda} H_\alpha$. Let $a, b \in \bigcap\limits_{\alpha\in\Lambda} H_\alpha$ 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 $ab^{-1} \in \bigcap\limits_{\alpha\in\Lambda} H_\alpha$. Thus $\bigcap\limits_{\alpha\in\Lambda} H_\alpha$ is a subgroup of G. $\square$

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

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

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 $\langle\, S \,\rangle := \bigcap\limits_{H\in\mathcal{C}_S} H$ 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*

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

Proof. Let

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

Clearly $S \subset K \subseteq G$. Taking $n = 2$, $a_1 = a_2 = a \in S$, $e_1 = 1$ and $e_2 = -1$, we have $e = a\,a^{-1} \in K$. Let $a, b \in K$. Then $a = a_1^{e_1} \cdots a_n^{e_n}$ and $b = b_1^{f_1} \cdots b_m^{f_m}$, for some $a_i, b_j \in S$, $e_i, f_j \in \{1, -1\}$, $1 \leq i \leq n$, $1 \leq j \leq m$, and $m, n \in \mathbb{N}$. Then $ab^{-1} = a_1^{e_1} \cdots a_n^{e_n} \cdot (b_1^{f_1} \cdots b_m^{f_m})^{-1} = a_1^{e_1} \cdots a_n^{e_n} \cdot b_m^{-f_m} \cdots b_1^{-f_1} \in K$. Therefore, K is a subgroup of G containing S. Then by Proposition 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, $K \subseteq \bigcap\limits_{H\in\mathscr{C}_S} H = \langle\, S \,\rangle$. $\square$

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 1.2.5. (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 1.1.5, is finitely generated.

Example 1.2.6. 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[2], denoted by $\operatorname{ord}(a)$. The number $\operatorname{ord}(a) := \inf S_a$ 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 $\operatorname{ord}(a) = \infty$.

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 $\operatorname{ord}(a) \mid m$.

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

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

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

Exercise 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 $\operatorname{ord}(ab)$ divides $\operatorname{lcm}(\operatorname{ord}(a), \operatorname{ord}(b))$.

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

[2]By well-ordering principal of $(\mathbb{N}, \leq)$.

Proof. (i) Let $\operatorname{ord}(a) = m$ and $\operatorname{ord}(b) = n$. Then $a^m = e = b^n$. Let $k := \operatorname{lcm}(m, n)$. Then $k = mu = nv$, for some $u, v \in \mathbb{N}$. Since $ab = ba$, we have

$$(ab)^k = a^k b^k = a^{mu} b^{nv} = (a^m)^u (b^n)^v = e \cdot e = e.$$

Therefore, $\operatorname{ord}(ab)$ is finite, and it divides $k = \operatorname{lcm}(m, n)$ by Exercise 1.2.18 (i).

(ii) Assume that $\gcd(m, n) = 1$. Then $k = \operatorname{lcm}(m, n) = mn$. Let $d := \operatorname{ord}(ab)$. Then $e = (ab)^d = a^d b^d$ implies that $a^d = b^{-d}$. Let $c := a^d = b^{-d}$. Since $c^m = (a^d)^m = (a^m)^d = e$, so $\operatorname{ord}(c) \mid m$. Similarly, $\operatorname{ord}(c) \mid n$. Then $\operatorname{ord}(c) \mid \gcd(m, n)$. Since $\gcd(m, n) = 1$, we have $\operatorname{ord}(c) = 1$. This forces $c = e$. Then $a^d = e$ and $b^d = e$, and so $m \mid d$ and $n \mid d$. Therefore, $mn = \operatorname{lcm}(m, n)$ divides $d = \operatorname{ord}(ab)$, and hence $\operatorname{ord}(ab) = mn$ in this case. □

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 $\operatorname{ord}(a) = m$, $\operatorname{ord}(b) = n$ and $\operatorname{ord}(ab) = r$. The proof of this surprising fact requires some advanced techniques, and may appear in an advanced group theory 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 $\mathrm{GL}_2(\mathbb{R})$. Show that $\operatorname{ord}(A) = \operatorname{ord}(B) = 2$ while $\operatorname{ord}(AB) = \infty$. Consequently, the subgroup $\langle A, B \rangle \leq \mathrm{GL}_2(\mathbb{R})$ generated by two order 2 elements of $\mathrm{GL}_2(\mathbb{R})$ is infinite.

Exercise 1.2.21. Let G be an abelian group. Let $H := \{a \in G : \operatorname{ord}(a) \text{ is finite}\}$. 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 σ and τ of S_3 such that $\langle \sigma, \tau \rangle = S_3$.

Exercise 1.2.25 (Derived subgroup)**.** Let G be a group. For given $a, b \in G$, the *commutator* of a with b 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 $[A_{ij}(c), A_{k\ell}(d)]$.

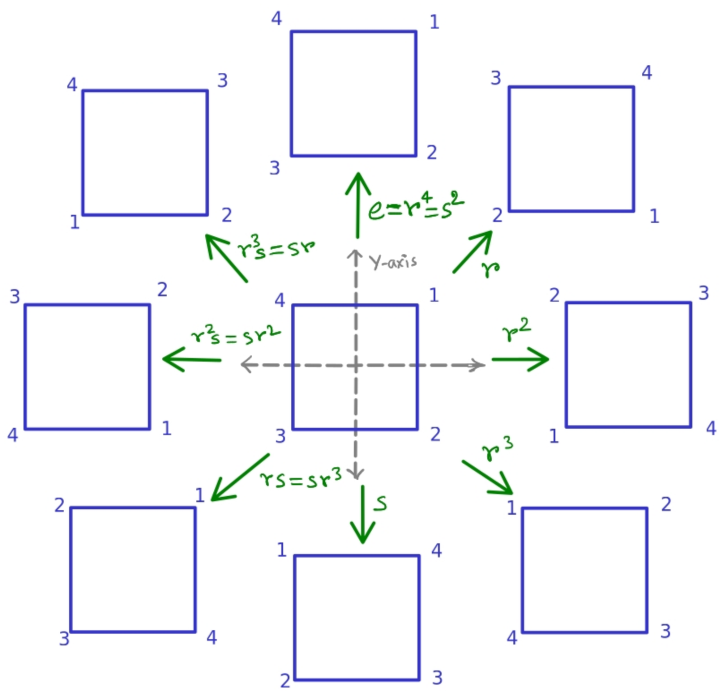
(iii) Show that $\{A_{ij}(c) : 1 \leq i, j \leq n, i \neq j,\ c \in \mathbb{R}\}$ generates $\mathrm{SL}_n(\mathbb{R})$ as a group.

(iv) Show that $\mathrm{SL}_n(\mathbb{R})$ is the derived subgroup of itself.

Example 1.2.7 (The dihedral group D_4)**.** Consider a square $\square$ in the plane $\mathbb{R}^2$ centered at the origin and vertices labeled as $1, 2, 3$ and 4 in the clock-wise direction. Consider the symmetries of this square $\square$ obtained by the following transformations:

(i) Rotations about the center by an angle $2n\pi/4$, where $n \in \mathbb{Z}$, and

(ii) Reflections about the Y-axis.



Symmetries of a square in the plane

Since the above mentioned transformations are given by some bijective maps from the set $J_4 := \{1, 2, 3, 4\}$ onto itself, we may consider them as elements of the symmetric group S_4.

If we denote by r the clock-wise rotation by an angle $2\pi/4$ and denote by s the reflection along the vertical Y-axis, then we have the following identities:

$$\text{ord}(r) = 4, \ \ \text{ord}(s) = 2, \ \ \text{and } sr = r^3 s. \tag{1.2.0.1}$$

Let $D_4 := \langle\, s, r \,\rangle \subseteq S_4$ be the set of all symmetries of the square generated by the above mentioned transformations and their compositions. It follows from the properties of r and s given in (1.2.0.1) that

$$D_4 := \left\{ s^i r^j : i, j \in \mathbb{N} \cup \{0\} \right\} = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}.$$

Thus, D_4 is a subgroup of S_4 consisting of $2 \times 4 = 8$ elements. We call D_4 the *dihedral group* of degree 4. Note that $rs = sr^3 \neq sr$ in D_4. Therefore, D_4 is a non-commutative group.

1.3 Cyclic group

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

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

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

Definition 1.3.1. A group G is said to be *cyclic* if there is an element $a \in G$ such that $G = \langle a \rangle := \{a^n : n \in \mathbb{Z}\}$. An element $a \in G$ satisfying $\langle\, a \,\rangle = G$ is called a *generator* of G.

Remark 1.3.1. Note that, 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. Thus, a cyclic group may have more than one generators.

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

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

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, but the converse is not true. For example, the Klein four-group K_4 in Example 1.1.4 (iv) is abelian but not cyclic.

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 $h = a^n = a^m q \in \langle a^m \rangle$. 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. □

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 $\operatorname{ord}(a)$ 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, $\operatorname{ord}(a)$ is infinite. Conversely, if $\operatorname{ord}(a)$ is infinite, then $a^n \neq e$, for all $n \in \mathbb{Z} \setminus \{0\}$. Since $a^n = a^m$ implies $a^{m-n} = e$, the map $f : \mathbb{Z} \to G$ given by $f(n) = a^n$, $\forall\, n \in \mathbb{Z}$, is injective. Therefore, since $\mathbb{Z}$ is infinite, G must be infinite. □

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

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

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 $\langle a \rangle = G$. □

Exercise 1.3.2. Let $G = \langle a \rangle$ be a finite cyclic group of order $n \in \mathbb{N}$. Show that $\operatorname{ord}(b)$ divides n, for all $b \in G$.

Corollary 1.3.8. *Any non-trivial subgroup of an infinite cyclic group is infinite.*

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. □

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 $\operatorname{ord}(a) = n$ 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 $\operatorname{ord}(a) = n$, we see that d is the least positive integer such that $(a^q)^d = a^{qd} = a^n = e$. Thus, $\operatorname{ord}(a^q) = d$, and so $|H| = d$ 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 $\operatorname{ord}(a^k) = d$. Then $a^{kd} = (a^k)^d = e$. Now by division algorithm there exists unique integers ℓ, 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

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

Since $0 \leq r < q$, we have $0 \leq dr < dq = n$. If $r \neq 0$, it would contradict the fact that $\operatorname{ord}(a) = n$. 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 $K = H$. □

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, $b \in \{a, a^{-1}\}$. □

Exercise 1.3.3. 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 $\phi : \mathbb{N} \to \mathbb{N}$ given by sending $n \in \mathbb{N}$ to the cardinality of the set

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

is called the *Euler phi function*.

Exercise 1.3.4. Let G be a finite cyclic group of order n. Use Exercise 1.3.3 and Corollary 1.3.6 to show that G has $\phi(n)$ number of elements of order n. In particular, if $n = p$ is a prime number, then G has exactly $p - 1$ elements of order p.

Exercise 1.3.5. Give an example of a non-abelian group G such that all of its proper subgroups are cyclic.

Exercise 1.3.6. Show that a non-commutative group always has a non-trivial proper subgroup.

Exercise 1.3.7. Show that a group having at most two non-trivial subgroups is cyclic.

Exercise 1.3.8. Let G be a finite group having exactly one non-trivial proper subgroup. Show that $|G| = p^2$, for some prime number p.

Hint: If H is the unique non-trivial proper subgroup of G, choosing an element $a \in G \setminus H$ note that that G is cyclic, and then by uniqueness of H conclude that $|G|$ has exactly one non-trivial proper integer divisor, and hence $|G|$ must be a square of some prime number. □

Exercise 1.3.9. 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 1.3.10. (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.

Exercise 1.3.11. Let $a, b \in G$ be finite order elements such that $ab = ba$.

(i) If $\langle a \rangle \cap \langle b \rangle = \{e\}$, show that $\operatorname{ord}(ab) = \operatorname{lcm}(\operatorname{ord}(a), \operatorname{ord}(b))$.

(ii) Show that the conclusion in (i) may not hold if $\langle a \rangle \cap \langle b \rangle \neq \{e\}$.

Proof. Let $\operatorname{ord}(a) = m$ and $\operatorname{ord}(b) = n$. Then $\operatorname{ord}(ab) \mid \operatorname{lcm}(m, n)$ by Exercise 1.2.19. To show that $\operatorname{ord}(ab) = \operatorname{lcm}(m, n)$, it suffices to show that $m \mid \operatorname{ord}(ab)$ and $n \mid \operatorname{ord}(ab)$. Let $d = \operatorname{ord}(ab)$. Then $e = (ab)^d = a^d b^d$, since $ab = ba$ in G. Then

$$a^d = b^{-d} \in \langle a \rangle \cap \langle b \rangle = \{e\},$$

and hence $a^d = e = b^d$ in G. Then by Exercise 1.2.18 (i) we have $m \mid d$ and $n \mid d$, and hence $\operatorname{lcm}(m, n) \mid d$, as required. Part (ii) is left as an easy exercise! □

Exercise 1.3.12. Let G be a group, and let $a_1, \ldots, a_r \in G$ elements of finite orders $n_1, \ldots, n_r$, respectively. Suppose that

(i) $a_i a_j = a_j a_i$, for all $i, j \in \{1, \ldots, r\}$, and

(ii) $\langle a_i \rangle \cap \langle \prod_{j \neq i} a_j \rangle = \{e\}$, for all $i \in \{1, \ldots, r\}$.

Show that $\mathrm{ord}(a_1 \cdots a_r) = \mathrm{lcm}(n_1, \ldots, n_r)$.

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 $HK := \{hk \in G : h \in H, k \in K\}$.

Example 1.4.1. Consider the dihedral group $D_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$ described in Example 1.2.7. Note that r and s satisfies $\mathrm{ord}(r) = 4$, $\mathrm{ord}(s) = 2$ and $r^3 s = sr$. Then $srs = r^3 s^2 = r^3 = r^{-1}$. Note that both $H := \{e, s\} \subset D_4$ and $K := \{e, rs\} \subset D_4$ are subgroups of D_4 of order 2, while their product set

$$HK = \{e, s\} \cdot \{e, rs\} = \{e, s, rs, srs\} = \{e, s, rs, r^{-1}\},$$

is not a group because $r^{-1} \in HK$ while $(r^{-1})^{-1} = r \notin HK$.

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 $(hk)^{-1} = h_1 k_1$, for some $h_1 \in H$ and $k_1 \in K$. Then $hk = \big((hk)^{-1}\big)^{-1} = k_1^{-1} h_1^{-1} \in KH$. Therefore, $HK \subseteq KH$, and hence $HK = KH$.

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

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

Therefore, HK is a subgroup of G. □

Corollary 1.4.2. *If H and K are subgroups of a commutative group, then HK is a group.*

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

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

This completes the proof. $\square$

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

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

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

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

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

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

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

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

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

***Remark 2.1.1.** 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*

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

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

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

For example,

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

Exercise 2.1.1. 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

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

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

2.2 Cycles

Fix an integer $n \geq 2$, and consider a permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix} \in S_n$$

as in (2.1.0.1). If $\sigma(k) = k$, for some $k \in J_n$, we may drop the corresponding column from its two-row notation, and rearrange its columns, if required, to get a *reduced expression* of the form

$$\sigma = \begin{pmatrix} k_1 & k_2 & \cdots & k_{r-1} & k_r \\ \sigma(k_1) & \sigma(k_2) & \cdots & \sigma(k_{r-1}) & \sigma(k_r) \end{pmatrix}, \tag{2.2.0.1}$$

where $k_1, \ldots, k_r$ are all distinct elements of J_n that are moved by σ.

If $\sigma(k_i) = k_{i+1}$, for all $i \in \{1, \ldots, r-1\}$ and $\sigma(k_r) = k_1$, then we can express σ in (2.2.0.1) as

$$\sigma = \begin{pmatrix} k_1 & k_2 & \cdots & k_{r-1} & k_r \\ k_2 & k_3 & \cdots & k_r & k_1 \end{pmatrix}; \tag{2.2.0.2}$$

and we call it a *cycle of length* r.

Definition 2.2.1 (Cycle)**.** Let $r \in \mathbb{Z}$ with $2 \leq r \leq n$. An element $\sigma \in S_n$ is called a r*-cycle* or a *cycle of length* r if there exists distinct r elements, say $k_1, \ldots, k_r \in J_n := \{1, \ldots, n\}$ such that $\sigma(k) = k$, for all $k \in J_n \setminus \{k_1, \ldots, k_r\}$ and

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

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

Remark 2.2.1. (i) 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 text books.

(ii) If $\sigma = (k_1 \;\; k_2 \;\; \cdots \;\; k_r) \in S_n$ is a r-cycle, with $2 \leq r \leq n$, it immediately follows from the definition of an r-cycle that $\sigma = (k_2 \;\; k_3 \;\; \cdots \;\; k_r \;\; k_1)$.

(iii) Transpositions are of particular interests. We shall see later (in Corollary 2.2.6) that any $\sigma \in S_n$ can be written as a finite product of either even number of transpositions or odd number of transpositions (see Corollary 2.3.2), and accordingly we call $\sigma \in S_n$ an even permutation or an odd permutation (see Definition 2.3.1).

Definition 2.2.2. Two cycles $\sigma = (k_1 \;\; \cdots \;\; k_r)$ and $\tau = (\ell_1 \;\; \cdots \;\; \ell_s)$ in S_n are said to be *disjoint* if the subsets $\{k_1, \ldots, k_r\}$ and $\{\ell_1, \ldots, \ell_s\}$ of J_n are disjoint.

Proposition 2.2.1. *If σ and τ are disjoint cycles in S_n, then $\sigma \circ \tau = \tau \circ \sigma$.*

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

Interchanging the roles of σ and τ we see that $\tau\sigma(k) = \sigma(k) = \sigma\tau(k)$ holds for the case $k \in \{j_1, \ldots, j_s\}$. Therefore, $\sigma\tau = \tau\sigma$.

With the notation as in (2.2.0.1), in this case the product $\sigma\tau = \tau\sigma$ has the following reduced expression

$$\sigma\tau = \tau\sigma = \begin{pmatrix} i_1 & \cdots & i_{r-1} & i_r & j_1 & \cdots & j_{s-1} & j_s \\ i_2 & \cdots & i_r & i_1 & j_2 & \cdots & j_s & j_1 \end{pmatrix},$$

which can be seen easily. □

Let $\sigma \in S_n$ be a non-identity permutation. Then there exists $k \in J_n$ such that $\sigma(k) \neq k$. Let $\{k_1, \ldots, k_r\} \subseteq J_n$ be such that $\sigma(k_i) \neq k_i$, for all $i = 1, \ldots, r$ and that $\sigma(k) = k$, for all $k \in J_n \setminus \{k_1, \ldots, k_r\}$. Since $\sigma : J_n \to J_n$ is a bijective map, we must have $r \geq 2$. As in (2.2.0.1), we can express σ as

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

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

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

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

$$\text{(2.2.0.4)} \qquad \sigma(k_{i,j}) = \begin{cases} k_{i,j+1}, & \text{if} \quad j \in \{1, \ldots, r_i - 1\}, \\ k_{i,1}, & \text{if} \quad j = r_i, \text{ and} \\ k_{ij}, & \text{if} \quad k_{ij} \in J_n \setminus \{k_1, \ldots, k_r\}. \end{cases}$$

Then σ can be expressed as

$$\begin{aligned} \text{(2.2.0.5)} \qquad \sigma &= \begin{pmatrix} k_{1,1} & \cdots & k_{1,r_1-1} & k_{1,r_1} & \cdots\cdots & k_{m,1} & \cdots & k_{m,r_m-1} & k_{m,r_m} \\ k_{1,2} & \cdots & k_{1,r_1} & k_{1,1} & \cdots\cdots & k_{m,2} & \cdots & k_{m,r_m} & k_{m,1} \end{pmatrix} \\ &= \begin{pmatrix} k_{1,1} & \cdots & k_{1,r_1-1} & k_{1,r_1} \\ k_{1,2} & \cdots & k_{1,r_1} & k_{1,1} \end{pmatrix} \circ \cdots \circ \begin{pmatrix} k_{m,1} & \cdots & k_{m,r_m-1} & k_{m,r_m} \\ k_{m,2} & \cdots & k_{m,r_m} & k_{m,1} \end{pmatrix} \\ &= (k_{1,1} \;\; \cdots \;\; k_{1,r_1-1} \;\; k_{1,r_1}) \circ \cdots \circ (k_{m,1} \;\; \cdots \;\; k_{m,r_m-1} \;\; k_{m,r_m}) \end{aligned}$$

Example 2.2.1. Consider the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 4 & 2 & 5 & 7 & 6 \end{pmatrix} \in S_7.$$

Since $5 \in J_7$ is the only element fixed by σ, removing the corresponding column we may rewrite it as

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 6 & 7 \\ 3 & 1 & 4 & 2 & 7 & 6 \end{pmatrix} \in S_7.$$

Since $1 \overset{\sigma}{\mapsto} 3 \overset{\sigma}{\mapsto} 4 \overset{\sigma}{\mapsto} 2 \overset{\sigma}{\mapsto} 1$ and $6 \overset{\sigma}{\mapsto} 7 \overset{\sigma}{\mapsto} 6$ we see that σ is a product of two cycles

$$\begin{aligned} \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 4 & 2 & 5 & 7 & 6 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \circ \begin{pmatrix} 6 & 7 \\ 7 & 6 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 3 & 4 & 2 \\ 3 & 4 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 6 & 7 \\ 7 & 6 \end{pmatrix} \\ &= (1\ \ 3\ \ 4\ \ 2) \circ (6\ \ 7) \end{aligned}$$

Exercise 2.2.1. Express the following permutations as product of disjoint cycles.

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

(ii) $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 2 & 6 & 1 & 5 & 8 & 9 & 3 & 10 & 7 \end{pmatrix} \in S_{10}.$

Example 2.2.2. 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.

Exercise 2.2.2. Let $\sigma = (k_1\ \ k_2\ \ \cdots\ \ k_r) \in S_n$ be a cycle of length $r \geq 2$ in S_n. Show that $\mathrm{ord}(\sigma) = r$.

Solution: In view of Remark 2.2.1 (ii), it suffices to show that r is the smallest positive integer such that $\sigma^r(k_1) = k_1$. Since

$$\sigma^i(k_1) = k_{1+i} \neq k_1, \ \ \forall\, i \in \{1, \ldots, r-1\},$$

and $\sigma^r(k_1) = \sigma(\sigma^{r-1}(k_1)) = \sigma(k_r) = k_1$, the result follows. □

Exercise 2.2.3. Show that the number of distinct r cycles in S_n is $\dfrac{n!}{r(n-r)!}$.

Solution: Note that, we can choose a r cycle from S_n in

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

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

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

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

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

two r cycles (note that k_1 is fixed!)

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

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

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

This completes the proof. □

Theorem 2.2.2. *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 the subset

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

contains exactly r elements, and so it defines an r-cycle

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

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

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

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

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

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

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

Definition 2.2.3 (Cycle type)**.** Given $\sigma \in S_n$, by Lemma 2.2.2 there exists a unique finite set of pairwise disjoint cycles $\{\sigma_1, \ldots, \sigma_r\}$ in S_n such that $\sigma = \sigma_1 \circ \cdots \circ \sigma_r$. Since disjoint cycles commutes by Proposition 2.2.1, by reindexing σ_j's, if required, we may assume that $n_1 \geq \ldots \geq n_r$, where $n_j = \mathrm{length}(\sigma_j)$, for all $j \in \{1, \ldots, r\}$. Since $\sigma_1, \ldots, \sigma_r$ are pairwise disjoint cycles in S_n, we have $\ell + \sum\limits_{j=1}^{r} n_j = n$, for some non-negative integer ℓ. If $\ell = 0$, then the sequence $(n_1, \ldots, n_r)$ is called the *cycle type* of σ, and if $\ell > 0$, then the sequence $(n_1, \ldots, n_r, f_1, \ldots, f_\ell)$, where $f_1 = \ldots = f_\ell = 1$, is called the cycle type of σ.

Example 2.2.3. (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 σ and τ in S_n are said to be *conjugate* in S_n if there exists $\delta \in S_n$ such that $\tau = \delta \circ \sigma \circ \delta^{-1}$.

Proposition 2.2.3. *Let $\sigma = (k_1 \ \ k_2 \ \ \cdots \ \ k_r) \in S_n$ be a r-cycle. Then for any $\tau \in S_n$ we have*
$$\tau\sigma\tau^{-1} = (\tau(k_1) \ \ \tau(k_2) \ \ \cdots \ \ \tau(k_r)).$$

Proof. Note that we have

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

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

Corollary 2.2.4. *Let $\sigma \in S_n$ is a product of pairwise disjoint cycles $\sigma_1, \ldots, \sigma_r$ in S_n. Suppose that $\sigma_i = (k_{i1} \ \ \cdots \ \ k_{i\ell_i}) \in S_n$, for all $i \in \{1, \ldots, r\}$. 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 σ and $\tau\sigma\tau^{-1}$ have the same cycle type.*

Proof. Use $\tau\sigma\tau^{-1} = (\tau\sigma_1\tau^{-1}) \circ \cdots \circ (\tau\sigma_r\tau^{-1})$ and Proposition 2.2.3. □

Theorem 2.2.5. *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 2.2.4. Conversely suppose that $\sigma, \tau \in S_n$ have the same cycle type, say
$$(n_1, \ldots, n_r, f_1, \ldots, f_\ell),$$
where $n_1 \geq \cdots \geq n_r \geq 2$ and $f_1 = \cdots = f_\ell = 1$, $\ell \geq 0$ and that $n_1 + \cdots + n_r + \ell = n$. Let $\sigma = \sigma_1 \circ \cdots \circ \sigma_r$ and $\tau = \tau_1 \circ \cdots \circ \tau_r$, where σ_i, τ_j are cycles in S_n of lengths n_i and n_j, respectively. Suppose that $\sigma_i = (a_{i1} \ \ \cdots \ \ a_{in_i})$ and $\tau_j = (b_{j1} \ \ \cdots \ \ b_{jn_j})$. 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 $\{a_1, \ldots, a_\ell\}$. Then I_n is a disjoint union of the subsets $\{a_{11}, \ldots, a_{1n_1}\}, \ldots, \{a_{r1}, \ldots, a_{rn_r}\}, \{a_1, \ldots, a_\ell\}$. Similarly if we write the subset $I_n \setminus \{b_{ij} : 1 \leq i \leq r, 1 \leq j \leq n_i\}$ as $\{b_1, \ldots, b_\ell\}$, then I_n is a disjoint union of the subsets $\{b_{11}, \ldots, b_{1n_1}\}, \ldots, \{b_{r1}, \ldots, b_{rn_r}\}, \{b_1, \ldots, b_\ell\}$. Then we define a map $\delta : I_n \to I_n$ by sending a_{ij} to b_{ij}, for all $(i, j) \in \{1, \ldots, r\} \times \{1, \ldots, n_i\}$, and by sending a_k to b_k, for all $k \in \{1, \ldots, \ell\}$, if $\ell > 0$. Clearly δ is a bijective map, and hence is an element of S_n. Then Proposition 2.2.3 ensures that $\delta\sigma_i\delta^{-1} = \tau_i$, for all $i \in \{1, \ldots, r\}$. Then we have

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

This completes the proof. □

Corollary 2.2.6. *For $n \geq 2$, every element of S_n can be written as a product of finitely many transpositions.*

Proof. In view of above Lemma 2.2.2 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. □

Exercise 2.2.4. Let σ and τ be two pairwise disjoint cycles in S_n. Show that $\langle\sigma\rangle \cap \langle\tau\rangle = \{e\}$.

Proof. If $\pi = (k_1\ \ k_2\ \ \cdots\ \ k_r) \in S_n$ is a r-cycle, then for any $k \in J_n \setminus \{k_1, \ldots, k_r\}$ we have $\pi(k) = k$, and hence $\pi^i(k) = k$, $\forall\, i \geq 0$. Therefore, none of the elements in $J_n \setminus \{k_1, \ldots, k_r\}$ appear in the factorization of π^i as a finite product of disjoint cycles in S_n, for all $i \geq 0$. In particular, if $\sigma = (u_1\ \ \cdots\ \ u_r)$ and $\tau = (v_1\ \ \cdots\ \ v_s)$ are two pair-wise disjoint cycles in S_n, then for any $i \in \{1, \ldots, r-1\}$ we have $\sigma^i(v_1) = v_1$ while $\tau^j(v_1) = v_{1+j} \neq v_1$, for all $j \in \{1, \ldots, s-1\}$. Therefore, $\sigma^i \neq \tau^j$, for all $i \in \{1, \ldots, r-1\}$ and $j \in \{1, \ldots, s-1\}$. Since $\mathrm{ord}(\sigma) = r$ and $\mathrm{ord}(\tau) = s$, we see that the cyclic subgroups $\langle\sigma\rangle = \{e, \sigma, \ldots, \sigma^{r-1}\}$ and $\langle\tau\rangle = \{e, \tau, \ldots, \tau^{s-1}\}$ of S_n intersects trivially; i.e., $\langle\sigma\rangle \cap \langle\tau\rangle = \{e\}$. □

Exercise 2.2.5. Let $\sigma_1, \ldots, \sigma_r$ be pairwise disjoint cycles in S_n. Show that

$$\langle\sigma_i\rangle \cap \langle\prod_{j \neq i} \sigma_j\rangle = \{e\}, \ \ \forall\, i \in \{1, \ldots, r\}.$$

Corollary 2.2.7. *Let σ and τ be two pairwise disjoint cycles of lengths r and s, respectively, in $S_n \setminus \{e\}$. Then $\mathrm{ord}(\sigma\tau) = \mathrm{lcm}(r, s)$.*

Proof. Since $\sigma\tau = \tau\sigma$ by Proposition 2.2.1 and since $\langle\sigma\rangle \cap \langle\tau\rangle = \{e\}$ by Exercise 2.2.4, the result follows from Exercise 1.3.11. □

Exercise 2.2.6. Let σ be a non-identity element in S_n. If $\sigma = \sigma_1 \circ \cdots \circ \sigma_r$ is a product of pairwise disjoint cycles in S_n, show that

$$\mathrm{ord}(\sigma) = \mathrm{lcm}(\ell_1, \ldots, \ell_r),$$

where ℓ_i is the length of σ_i, for all $i = 1, \ldots, r$.

Solution: For $r = 2$, it is just Corollay 2.2.7. For $r \geq 3$, use Exercise 2.2.5 and Exercise 1.3.12. □

Exercise 2.2.7. Find the number of elements of order 2 and 3 in S_4.

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 $\chi := \prod\limits_{1 \leq i < j \leq n} (x_i - x_j)$ given by*

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

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

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

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

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

(c) If $\{i, j\} \cap \{p, q\}$ is singleton, we have three indices to consider, namely p, q and t, where $t \in \{i, j\} \setminus \{p, q\}$. So 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 $\sigma((x_p - x_t)(x_t - x_q)) = (x_{\sigma(p)} - x_{\sigma(t)})(x_{\sigma(t)} - x_{\sigma(q)}) = (x_q - x_t)(x_t - x_p) = (x_p - x_t)(x_t - x_q)$.

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

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

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

Corollary 2.3.2. *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 σ_i, τ_j are all transpositions in S_n, then both r and s are either even or odd.*

Proof. Consider the formal product $\chi := \prod\limits_{1 \leq i < j \leq n} (x_i - x_j)$. 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 σ can be written as a product of even (respectively, odd) number of transpositions in S_n.

Note that given a permutation $\sigma \in S_n$, if $\sigma = \sigma_1 \circ \cdots \circ \sigma_r$, where $\sigma_1, \ldots, \sigma_r$ are 2-cycles in S_n, then by Corollary 2.3.2 we see that σ is even if and only if $(-1)^r = 1$. Thus we have a well-defined map $\mathrm{sgn} : S_n \to \{1, -1\}$ given by sending $\sigma \in S_n$ to $(-1)^r$, where r is a number of 2-cycles appearing in the decomposition of σ into a product of 2-cycles in S_n. In other words,

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

The number $\mathrm{sgn}(\sigma)$ 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 σ is a product of five transpositions in S_8, we conclude that σ is odd.

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

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

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

Exercise 2.3.3. Show that S_4 has no element of order ≥ 5.

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 $\tau_1, \ldots, \tau_{2r}$ are transpositions in S_n. Since transpositions are elements of order 2 (see Exercise 2.2.2), they are self inverse in S_n. Now it follows from Exercise 1.1.2 (ii) that

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

Therefore, τ^{-1} is also an even permutation. Since σ and τ^{-1} are even, their product $\sigma \circ \tau^{-1} \in A_n$. Therefore, A_n is a subgroup of S_n by Lemma 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 σ and τ are not disjoint, then we may assume that $j = k$. Then $\sigma \circ \tau = (i\ \ j)(j\ \ \ell) = (i\ \ j\ \ \ell)$ is a 3-cycle. If σ and τ are disjoint, then

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

where the last equality is due to the first case. Hence the result follows. $\square$

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

Solution: Fix a transposition $\pi \in S_n$, for example, one can take $\pi = (1\ \ n) \in S_n$. Note that π being an element of order 2, we have $\pi^{-1} = \pi$. Define a map $\varphi : A_n \to S_n \setminus A_n$ by

$$\varphi(\sigma) = \sigma \circ \pi, \ \ \forall\, \sigma \in A_n.$$

Clearly $\sigma \circ \pi$ is an odd permutation, for any $\sigma \in A_n$. If $\sigma \circ \pi = \sigma' \circ \pi$, for some $\sigma, \sigma' \in A_n$, then applying π from the right-side of the above equation, we have $\sigma = \sigma'$. Therefore, φ is injective. For given $\tau \in S_n \setminus A_n$, note that $\sigma := \tau \circ \pi \in A_n$ and it satisfies $\varphi(\sigma) = \sigma \circ \pi = \tau \circ \pi \circ \pi = \tau$. Therefore, φ is surjective, and hence is a bijective map. Therefore, both A_n and $S_n \setminus A_n$ have the same number of elements. Hence the result follows. □

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* σ *and* τ 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 $\{(1\ \ 2), (1\ \ 2\ \ \cdots\ \ n)\}$, for all $n \geq 3$.

Proof. Let H be the subgroup of S_n generated by $(1\ \ 2)$ and $(1\ \ 2\ \ \cdots\ \ n)$. Since any non-identity element $\sigma \in S_n$ is a product of finitely many transpositions, to show $H = S_n$, it suffices to show that $(i\ \ j) \in H$, for all $i, j \in J_n$ with $i < j$. Since $(i\ \ j) = (1\ \ j)(1\ \ i)(1\ \ j)$, it suffices to show that $(1\ \ i) \in H$, for all $i \in J_n$.

Claim 1: $(i\ \ i+1) \in H$, for all $i \in \{1, \ldots, n-1\}$.

> *Proof of Claim 1:* The case $i = 1$ is trivial, as $(1\ \ 2) \in H$. Suppose that $(i\ \ i+1) \in H$, for some $i \in \{1, \ldots, n\}$. Since $\sigma := (1\ \ 2\ \ \cdots\ \ n)$, then we have $\sigma(i\ \ i+1)\sigma^{-1} = (\sigma(i)\ \ \sigma(i+1)) = (i+1\ \ i+2) \in H$. □

Claim 2: $(1\ \ i) \in H$, for all $i \in \{1, \ldots, n\}$.

> *Proof of Claim 2:* As before, the case $i = 1$ is trivial as $(1\ \ 2) \in H$. Suppose that $(1\ \ i) \in H$, for some $i \in \{1, \ldots, n-1\}$. Since $(i\ \ i+1) \in H$, we have $(1\ \ i+1) = (i\ \ i+1)(1\ \ i)(i\ \ i+1) \in H$. □

This completes the proof. □

Example 2.4.1 (Dihedral group D_n)**.** This is a generalization of the Example 1.2.7. Consider a regular n-gon in the plane $\mathbb{R}^2$ whose vertices are labelled as $1, 2, 3, \ldots, n$ in clockwise order. Let D_n be the set of all symmetries of this regular n-gon given by the following operations and their finite compositions:

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

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

Note that $\operatorname{ord}(a) = n$, $\operatorname{ord}(b) = 2$ 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

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

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

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

Note that each element of D_n is given by a bijection of the set $J_n := \{1, 2, \ldots, n\}$ onto itself, and hence is a permutation on J_n. However, not all permutations of the set J_n corresponds to a symmetry of a regular n-gon as described above (see Exercise 2.4.7 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. Consider the cycles $\sigma = (1\ \ 2)$ and $\tau = (1\ \ 2\ \ 3)$ in S_3.

(i) Show that $\operatorname{ord}(\sigma) = 2$, $\operatorname{ord}(\tau) = 3$ and $\sigma\tau\sigma^{-1} = \tau^2$.

(ii) Conclude that $D_3 = \langle\, \sigma, \tau \,\rangle = \{e, \tau, \tau^2, \sigma, \sigma\tau, \sigma\tau^2\} = S_3$.

Exercise 2.4.7. Show that D_n is a proper subgroup of S_n, for all $n \geq 4$.

Exercise 2.4.8. 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 $f : G \to H$ 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 $c_e : G \to G$, which sends all points of G to the neutral element $e \in G$, is a group homomorphism, called the *trivial group homomorphism* of G.

(ii) Let H be a subgroup of a group G. Then the set theoretic inclusion map $H \hookrightarrow G$ is a group homomorphism. In particular, for any group G, the identity map
$$\mathrm{Id}_G : G \to G, \ \ a \mapsto a$$
is a group homomorphism.

(iii) Fix an integer m, and define a function
$$\varphi_m : \mathbb{Z} \longrightarrow \mathbb{Z}, \ \ n \longmapsto mn, \ \forall\, n \in \mathbb{Z}.$$
Then $\varphi_m(n_1 + n_2) = m(n_1 + n_2) = mn_1 + mn_2 = \varphi_m(n_1) + \varphi_m(n_2)$, for all $n_1, n_2 \in \mathbb{Z}$. Therefore, φ_m is a group homomorphism. Note that, φ_m is always injective, and it is surjective only for $m \in \{1, -1\}$.

(iv) Let $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$, and consider the exponential map
$$f : \mathbb{R} \longrightarrow \mathbb{R}^*, \ \ x \longmapsto e^x, \ \ \forall\, x \in \mathbb{R}.$$
Since $f(a + b) = e^{a+b} = e^a \cdot e^b = f(a) \cdot f(b)$, for all $a, b \in \mathbb{R}$, the map f is a group homomorphism from $(\mathbb{R}, +)$ into $(\mathbb{R}^*, \cdot)$. Verify that f is injective.

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

(vi) Let

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

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

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

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

Verify that ψ is a surjective group homomorphism.

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

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

Therefore, $\mathbf{F}$ is a group homomorphism, known as the *Frobenius endomorphism*.

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

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

Verify that f is a group homomorphism.

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

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

Exercise 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 $\widetilde{\sigma} : J_{n+1} \to J_{n+1}$ defined by

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

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

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

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

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

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

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

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

3.2 Basic properties

Proposition 3.2.1. *Let $f : G \to H$ be a group homomorphism. Let $e_G \in G$ and $e_H \in H$ be the neutral elements of G and H, respectively. Then we have the following.*

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

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

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

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

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

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

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

□

Exercise 3.2.1. Let G and H be two groups, and let $\varphi, \psi : G \to H$ be group homomorphisms. If both φ and ψ are constant maps, show that $\varphi = \psi$.

Proposition 3.2.2. *Let $f : G \to H$ be a group homomorphism.*

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

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

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

(ii) Let $e_G \in G$ and $e_H \in H$ be the neutral elements of G and H, respectively. Since $f(e_G) = e_H$ by Proposition 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.

□

Exercise 3.2.2. Let G be a group. Fix a prime number $p > 0$. Show that any non-trivial group homomorphism from G into $\mathbb{Z}_p$ is surjective.

Exercise 3.2.3. Show that the groups $(\mathbb{Q}, +)$ and $(\mathbb{Q}^\times, \cdot)$ are not isomorphic.

Proposition 3.2.3. *Composition of group homomorphisms is a group homomorphism.*

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

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

Exercise 3.2.4. Let G and H be two groups. Show that the projection maps $\pi_G : G \times H \to G$ and $\pi_H : G \times H \to H$ defined by

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

are surjective group homomorphisms.

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

Proof. Let $\pi_H : H \times K \to H$ and $\pi_K : H \times K \to K$ be the projection maps onto the first and the second factors, respectively (see Exercise 3.2.4). Since both π_H and π_K are group homomorphisms, given any group homomorphism $f : G \to H \times K$, we have $\pi_H \circ f \in \mathrm{Hom}(G, H)$ and $\pi_K \circ f \in \mathrm{Hom}(G, K)$ by Proposition 5.2.2. Thus we get a map $\Phi : \mathrm{Hom}(G, H \times K) \to \mathrm{Hom}(G, H) \times \mathrm{Hom}(G, K)$ defined by

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

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

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

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

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

Therefore, if $\Phi(f) = \Phi(g)$ for some $f, g \in \mathrm{Hom}(G, H \times K)$, 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. □

Definition 3.2.1. A group homomorphism $f : G \to H$ 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 $f : G \to H$ is an isomorphism, we say that *G is isomorphic to H*, and express it as $G \cong H$.

Exercise 3.2.5. Show that $\mathbb{Z}_6$ is not isomorphic to S_3.

Solution: Since $\mathbb{Z}_6$ is abelian, if there were an isomorphism $f : \mathbb{Z}_6 \to S_3$, then $S_3 = f(\mathbb{Z}_6)$ would be abelian by Proposition 3.2.2 (i), which is not true. □

Exercise 3.2.6. Let G be a group. Denote by G^{op} the opposite group of G (see Example 1.1.7). Show that the map $\iota : G \to G^{\mathrm{op}}$ defined by $\iota(a) = a^{-1}$, for all $a \in G$, is an isomorphism of groups.

Proof. Since $\iota(ab) = (ab)^{-1} = b^{-1}a^{-1} = \iota(a) *^{\mathrm{op}} \iota(a)$, for all $a, b \in G$, the map ι is a group homomorphism. Since $\mathrm{Ker}(\iota) = \{a \in G : a^{-1} = e\} = \{e\}$, the map ι is injective. Since for given any $b \in G$, $\iota(b^{-1}) = (b^{-1})^{-1} = b$, the map ι is surjective. Thus $\iota : G \to G^{\mathrm{op}}$ is an isomorphism of groups. □

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

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

3.3 Kernel

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

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

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

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

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

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

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

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

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

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

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

Proposition 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 $f : \mathbb{Z} \to G$ by $f(n) = a^n$, for all $n \in \mathbb{Z}$. Since

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

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

Proposition 3.3.3. *Any finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$.*

Proof. Let $G = \langle\, a \,\rangle = \{a^k : k \in \mathbb{Z}\}$ be a finite cyclic group of order n. Let $r, s \in \mathbb{Z}$ be such that $a^r = a^s$. Without loss of generality we may assume that $r \geq s$. Since $\operatorname{ord}(a) = n$ and $a^{r-s} = e$, we have $r - s = nk$, for some $k \in \mathbb{Z}$. Therefore, the map $f : G \to \mathbb{Z}_n$ defined by

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

is well-defined. Let $x, y \in G$ be given. Then $x = a^r$ and $y = a^s$, for some $r, s \in \mathbb{Z}$. Then

$$\begin{aligned} f(xy) = f(a^r a^s) &= f(a^{r+s}) \\ &= [r+s] \\ &= [r] + [s] \\ &= f(a^r) + f(a^s) = f(x) + f(y). \end{aligned}$$

Therefore, f is a group homomorphism. Since

$$\begin{aligned} \operatorname{Ker}(f) &= \{a^r \in G : [r] = [0]\} \\ &= \{a^r \in G : r = nk, \ \text{ for some } k \in \mathbb{Z}\} = \{e\}, \end{aligned}$$

the map f is injective. Since $|G| = n = |\mathbb{Z}_n|$, the map f is surjective too. Therefore, f is an isomorphism of groups. $\square$

Exercise 3.3.1. Show that there is no surjective group homomorphism from $\mathbb{Z}_6$ to $\mathbb{Z}_4$.

Lemma 3.3.4. *For any integer $n \geq 2$, we have $\sum\limits_{d|n} \phi(d) = n$, where the sum is taken over all integers $d \geq 1$ such that d divides n.*

Proof. Note that $\phi(d)$ is equal to the number of generators of a finite cyclic group of order d (see Exercise 1.3.3). Fix a finite cyclic group G of order n. Note that every element $a \in G$ generates a cyclic subgroup $H_a := \langle a \rangle$ of order $d_a := \operatorname{ord}(a)$, and for each divisor d of n there is a unique cyclic subgroup of G of order d. Since G has n elements, combining these observations the result follows. $\square$

Example 3.3.2. In this example we describe all group homomorphisms from $\mathbb{Z}_n$ into $\mathbb{Z}_m$. Let $f \in \mathrm{Hom}(\mathbb{Z}_n, \mathbb{Z}_m)$ be given. Since $\mathbb{Z}_n$ is a cyclic group generated by $[1] \in \mathbb{Z}_n$, the element $f([1]) \in \mathbb{Z}_m$ completely determine the map f. Since $\mathrm{ord}(f([1])) \mid n$ by Proposition 3.2.1 (iii) and $\mathrm{ord}(f([1])) \mid m$ by Exercise 1.3.2, we see that $\mathrm{ord}(f([1]))$ divides $d := \gcd(m, n)$. Let $r \in \mathbb{N}$ be such that $r \mid d$. Since $r \mid m$, there is a unique subgroup, say H_r of $\mathbb{Z}_m$, with $|H_r| = r$ by Proposition 1.3.9. Since H_r is a cyclic group of order r, it is isomorphic to $\mathbb{Z}_r$ by Proposition 3.3.3. Then by Exercise 1.3.3 the number of generators of H_r is equal to $\phi(r)$, where ϕ is the Euler phi function. Since for each choice of a generator $[b]$ of H_r, sending $[1]$ to $[b] \in H_r$ we get a surjective group homomorphism $\mathbb{Z}_n \to H_r \subseteq \mathbb{Z}_m$, the total number of group homomorphisms from $\mathbb{Z}_n$ into $\mathbb{Z}_m$ is equal to

$$\sum_{r \mid d} \phi(r) = d,$$

where the last equality follows from Lemma 3.3.4.

Exercise 3.3.2. Find all group homomorphisms from $\mathbb{Z}_{10}$ to $\mathbb{Z}_6$.

Exercise 3.3.3. Find all surjective group homomorphisms from $\mathbb{Z}_{20}$ to $\mathbb{Z}_{10}$.

Theorem 3.3.5 (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 (see Example 1.1.10). Define a map

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

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

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

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

3.4 Automorphisms

Definition 3.4.1. An *automorphism* of a group G is a group isomorphism from G onto itself. The set of all automorphisms of G is denoted by $\mathrm{Aut}(G)$.

Example 3.4.1. Let G be a group.

(i) The identity map $\mathrm{Id}_G : G \to G$ is an automorphism of G.

(ii) For any automorphism $f : G \to G$, its inverse map $f^{-1} : G \to G$ is an automorphism of G.

(iii) For given $a \in G$, the *conjugation by a map*,

$$\varphi_a : G \to G, \;\; g \mapsto aga^{-1},$$

is an automorphism of G, called the *inner automorphism of G defined by a*.

(iv) The map $f : \mathbb{Z}_3 \to \mathbb{Z}_3$ defined by $f([0]) = [0]$, $f([1]) = [2]$ and $f([2]) = [1]$ is an automorphism of $\mathbb{Z}_3$.

Proposition 3.4.1. *Given a group G, the set $\mathrm{Aut}(G)$ forms a group with respect to the binary operation given by composition of maps; the group $\mathrm{Aut}(G)$ is known as the automorphism group of G. The subset*

$$\mathrm{Inn}(G) := \{f \in \mathrm{Aut}(G) : f \;\text{ is an inner automorphism of } G\}$$

forms a subgroup of $\mathrm{Aut}(G)$, known as the group of inner automorphisms of G.

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

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

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

Example 3.4.2. The complex conjugation map $z \mapsto \overline{z}$ from the additive group $\mathbb{C}$ into itself is an automorphism of $\mathbb{C}$.

Exercise 3.4.1. Let G be a group. Consider the map $\varphi : G \to \mathrm{Aut}(G)$ that sends $a \in G$ to the inner autormorphism $\varphi_a \in \mathrm{Aut}(G)$, where

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

(i) Show that φ is a group homomorphism with $\mathrm{Ker}(\varphi) = Z(G)$.

(ii) Conclude that $G \cong \mathrm{Inn}(G)$ whenever $Z(G)$ is trivial.

Solution: Since $\varphi_{ab}(c) = (ab)c(ab)^{-1} = a(bcb^{-1})a^{-1} = (\varphi_a \circ \varphi_b)(c)$, for all $c \in G$, we have

$$\varphi_{ab} = \varphi_a \circ \varphi_b, \ \ \forall\, a, b \in G.$$

Therefore, φ is a group homomorphism. Clearly f is surjective. Let $a \in \mathrm{Ker}(\varphi)$ be given. Then $\varphi_a = \mathrm{Id}_G$ implies that

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

and so $a \in Z(G)$. Therefore, $\mathrm{Ker}(\varphi) = Z(G)$. The second assertion is clear. □

Exercise 3.4.2. Show that $Z(S_3)$ is trivial.

Solution: Let $\sigma \in Z(S_3)$ be given. Then

$$\sigma = \tau\sigma\tau^{-1}, \ \forall\, \tau \in S_3.$$

If $\sigma \neq e$, then there exists $i, j \in J_3 := \{1, 2, 3\}$ with $i < j$ such that $\sigma(i) = j$. Since $\sigma : J_3 \to J_3$ is a bijective map, $\sigma(j) \neq j$. Therefore, either $\sigma = (i\ \ j)$ or $\sigma = (i\ \ j\ \ k)$, where $k \in J_3 \setminus \{i, j\}$. If $\sigma = (i\ \ j)$, choosing $\tau = (i\ \ k)$ we see that

$$\tau\sigma\tau^{-1} = (\tau(i)\ \ \tau(j)) = (k\ \ j) \neq \sigma.$$

If $\sigma = (i\ \ j\ \ k)$, choosing $\tau = (i\ \ k)$ we see that

$$\tau\sigma\tau^{-1} = (\tau(i)\ \ \tau(j)\ \ \tau(k)) = (k\ \ j\ \ i) \neq \sigma.$$

Thus we get contradictions in both cases. Therefore, $Z(S_3) = \{e\}$. □

Exercise 3.4.3. Let T be the set of all 2-cycles in S_3. Let $f \in \mathrm{Aut}(S_3)$ be given.

(i) Show that $f(\sigma) \in T$, for all $\sigma \in T$.

(ii) Show that the map $\widetilde{f} : T \to T$ given by $\sigma \mapsto f(\sigma)$, is bijective.

(iii) Show that the map $\psi : \mathrm{Aut}(S_3) \to S_3$ defined by

$$\psi(f) = \widetilde{f}, \ \forall\, f \in \mathrm{Aut}(S_3),$$

is a group homomorphism.

(iv) Show that $\mathrm{Ker}(\psi)$ is trivial.

Exercise 3.4.4. Show that $\mathrm{Aut}(S_3)$ is isomorphic to S_3.

Proof. Consider the group homomorphism $\varphi : S_3 \to \mathrm{Aut}(S_3)$ that sends $\sigma \in S_3$ to the inner automorphism

$$\varphi_\sigma : \tau \mapsto \sigma\tau\sigma^{-1}.$$

Since $Z(S_3)$ is trivial, the homomorphism φ is injective. Since S_3 is finite, to show $\mathrm{Aut}(S_3) \cong S_3$ it suffices to construct an injective group homomorphism $\psi : \mathrm{Aut}(S_3) \to S_3$; for then the composition

$$\psi \circ \varphi : S_3 \xrightarrow{\varphi} \mathrm{Aut}(S_3) \xrightarrow{\psi} S_3$$

would be an injective group homomorphism, and hence is an isomorphism because S_3 is finite. This would force φ to be an isomorphism of groups. Since the image of φ is the subgroup $\mathrm{Inn}(S_2) \subseteq \mathrm{Aut}(S_3)$, it follows from surjectivity of φ that $\mathrm{Inn}(S_3) = \mathrm{Aut}(S_3)$ concluding the proof.

Let $f \in \mathrm{Aut}(S_3)$ be given. Since 2-cycles are the only elements of order 2 in S_3, the isomorphism f sends a 2-cycle to a 2-cycle. Since there are three 2-cycles in S_3, namely $(1\ \ 2), (1\ \ 3)$ and $(2\ \ 3)$, the map f gives rise to a bijection on the set $T := \{(1\ \ 2), (1\ \ 3), (2\ \ 3)\}$, which we denote by $\widetilde{f}$. Thus we get a map

$$\psi : \mathrm{Aut}(S_3) \to S(T) \cong S_3, \quad f \mapsto \widetilde{f}.$$

It is clear from the construction of ψ that

$$\psi(f \circ g) = \psi(f) \circ \psi(g), \quad \forall\, f, g \in \mathrm{Aut}(S_3).$$

Therefore, ψ is a group homomorphism. Let $f \in \mathrm{Ker}(\psi)$ be given. Then $\widetilde{f} = \mathrm{Id}_T$. Since T generates S_3, we must have $f = \mathrm{Id}_{S_3}$. Therefore, $\mathrm{Ker}(\psi)$ is trivial, and hence ψ is injective. □

Exercise 3.4.5. Show that all automorphisms of S_3 are inner automorphisms.

Proposition 3.4.2. *Let G be a cyclic group generated by $a \in G$. A homomorphism $f : G \to G$ is an automorphism of G if and only if $f(a)$ is a generator of G.*

Proof. Let $f : G \to G$ be an automorphism of G. Let $b = f(a)$. Let $x \in G$ be arbitrary. Since f is surjective, there exists $y \in G$ such that $f(y) = x$. Since $G = \langle\, a \rangle$, we have $y = a^n$, for some $n \in \mathbb{Z}$. Then $x = f(y) = f(a^n) = [f(a)]^n = b^n \in \langle\, b\, \rangle$. This shows that $G = \langle\, b\, \rangle$, and hence b is a generator of G. Conversely if $f : G \to G$ is a homomorphism such that $f(a)$ generates G, then f is surjective. If $|G|$ is finite, we must have f is bijective. If G is not finite, then G has only two generators, namely a and a^{-1} by Proposition 1.3.10, and hence f must be either Id_G or the map given by sending $b \in G$ to b^{-1}. In both cases, f is bijective (c.f. Exercise 3.2.6), and hence is in $\mathrm{Aut}(G)$. □

Exercise 3.4.6. Let G be a cyclic group generated by $a \in G$, and let H be any group. Show that a group homomorphism $f : G \to H$ is uniquely determined by $f(a) \in H$ in the sense that if $g : G \to H$ is any group homomorphism satisfying $g(a) = f(a)$, then $f = g$.

Corollary 3.4.3. *For any integer $n \geq 2$, the group $\mathrm{Aut}(\mathbb{Z}_n)$ is isomorphic to $\mathbb{Z}_n^\times$.*

Proof. Since $\mathbb{Z}_n$ is a cyclic group generated by $[1] \in \mathbb{Z}_n$, it follows from Proposition 3.4.2 that $f([1])$ is a generator of $\mathbb{Z}_n$, for all $f \in \mathrm{Aut}(\mathbb{Z}_n)$. Since $\mathbb{Z}_n^\times = \{[a] \in \mathbb{Z}_n : \gcd(a, n) = 1\}$ is the set of all generators of $(\mathbb{Z}_n, +)$ by Proposition 1.3.1, we get a map $\varphi : \mathrm{Aut}(\mathbb{Z}_n) \to \mathbb{Z}_n^\times$ given by

$$\varphi(f) = f([1]), \ \forall\, f \in \mathrm{Aut}(\mathbb{Z}_n).$$

Since $\varphi(f \circ g) = (f \circ g)([1]) = f(g[1]) = f([1]) \cdot g([1])$, we see that φ is a group homomorphism. Since $\mathrm{Ker}(\varphi) = \{f \in \mathrm{Aut}(\mathbb{Z}_n) : f([1]) = [1]\} = \{\mathrm{Id}_{\mathbb{Z}_n}\}$ by Exercise 3.4.6, we see that φ is injective. To show that φ is surjective, let $[a] \in \mathbb{Z}_n^\times$ be given. Then the map $f : \mathbb{Z}_n \to \mathbb{Z}_n$ defined by

$$f([k]) = [ka], \ \ \forall\, k \in \{0, 1, \ldots, n-1\},$$

is a group homomorphism (verify!). Since $f([1]) = [a] \in \mathbb{Z}_n^\times$, it follows from Proposition 3.4.2 that $f \in \mathrm{Aut}(\mathbb{Z}_n)$. Thus $\varphi(f) = f([1]) = [a]$, and hence φ is surjective. This completes the proof. $\square$

Example 3.4.3 (Automorphisms of K_4)**.** Recall that the Klein's four group $K_4 = \{e, a, b, c\}$ is an abelian group generated by two elements, a and b satisfying the following conditions: $a^2 = b^2 = e$ and $ab = ba = c$. To compute $\mathrm{Aut}(K_4)$, note that if $f \in \mathrm{Aut}(K_4)$, then $f(e) = e$ and hence $f\big|_{\{a,b,c\}}$ is a bijection of the subset $\{a, b, c\} \subset K_4$ onto itself, producing an element of S_3. Thus we get a map $\varphi : \mathrm{Aut}(K_4) \to S_3$. Since for given any $f, g \in \mathrm{Aut}(K_4)$, we have

$$\varphi(f \circ g) = (f \circ g)\big|_{\{a,b,c\}} = f\big|_{\{a,b,c\}} \circ g\big|_{\{a,b,c\}} = \varphi(f) \circ \varphi(g),$$

the map φ is a group homomorphism. Since

$$\mathrm{Ker}(\varphi) = \{f \in \mathrm{Aut}(K_4) : f\big|_{\{a,b,c\}} = \mathrm{Id}_{\{a,b,c\}}\} = \{\mathrm{Id}_{K_4}\},$$

it follows that φ is injective. Let $\sigma \in S_3$ be given. Considering σ as a bijective map $\sigma : \{a, b, c\} \to \{a, b, c\}$, we may extend it to a bijective map $\widetilde{\sigma} : K_4 \to K_4$ by setting $\widetilde{\sigma}(e) = e$ and $\widetilde{\sigma}\big|_{\{a,b,c\}} = \sigma$. Since σ is injective and $\sigma(a), \sigma(b), \sigma(c) \in K_4 \setminus \{e\}$, it follows from the cancellation law (see Lemma 1.1.4) that $\sigma(a)\sigma(b) = \sigma(c) = \sigma(b)\sigma(a)$. Since $ab = ba = c$ in K_4, we have $\sigma(b)\sigma(a) = \sigma(c) = \sigma(ab) = \sigma(a)\sigma(b)$. Similarly, one can easily check that $\sigma(c)\sigma(a) = \sigma(b) = \sigma(a)\sigma(b)$ and $\sigma(c)\sigma(b) = \sigma(a) = \sigma(b)\sigma(c)$. Thus $\widetilde{\sigma}$ is a group homomorphism, and hence is an automorphism of K_4. Since $\varphi(\widetilde{\sigma}) = \sigma$ by construction, $\varphi : \mathrm{Aut}(K_4) \to S_3$ is an isomorphism of groups.

Exercise 3.4.7. Show that $\mathrm{Aut}(\mathbb{Q})$ is isomorphic to $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$.

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

(4.1.0.1)
$$\begin{tikzcd} G \arrow[r, "t"] \arrow[d, "\pi"'] & T \\ Q \arrow[ur, dashed, "\exists ! \widetilde{t}"'] & \end{tikzcd}$$

Interesting point is that, without knowing existence of such a pair (Q, q), it follows immediately from the properties (i) and (ii) in Definition 4.1.1 that such a pair (Q, q), 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, π) and (Q', π') are two quotients of G by H, then there exists a unique group isomorphism $\varphi : Q \to Q'$ such that $\varphi \circ \pi = \pi'$.*

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

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

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

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 $\pi : G \to Q$ is a group homomorphism by assumption, given any two elements $a, b \in G$ with $a^{-1}b \in H$ we have $\pi(a^{-1}b) = e_Q$, and hence $\pi(a) = \pi(b)$. In other words, two elements $a, b \in G$ are in the same fiber[1] of the map $\pi : G \to Q$ if $a^{-1}b \in H$. Since the set of all fibers of any set map $f : G \to Q$ gives a partition of G, and hence an equivalence relation on G, the condition (i) suggests us to define a relation ρ_L on G by setting

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

It is easy to check that ρ_L is an equivalence relation on G (verify!). The ρ_L-equivalence class of an element $a \in G$ is the subset

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

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

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

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

[1]The *fiber* of a map $f : X \to Y$ over a point $y \in Y$ is the subset $f^{-1}(y) = \{x \in X : f(x) = y\} \subseteq X$.

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

Proposition 4.2.1. *For each $a \in G$, the map $\varphi_a : H \to aH$ defined by $\varphi_a(h) = ah$, for all $h \in H$, is bijective. Consequently, $|aH| = |bH|$, for all $a, b \in H$.*

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

Exercise 4.2.1. Define a relation ρ_R on G by setting

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

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

(ii) Show that the ρ_R-equivalence class of $a \in G$ 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 $a \in G$.

Let $G/H = \{aH : a \in G\}$ be the set of all distinct left cosets of H in G, and let $H\backslash G = \{Ha : a \in G\}$ be the set of all distinct right cosets of H in G.

Lemma 4.2.2. *Let H be a subgroup of a group G. Then there is a one-to-one correspondence between the set of all left cosets of H in G and the set of all right cosets of H in G. In other words, there is a bijective map $\varphi : G/H \longrightarrow H\backslash G$. Therefore, both the sets G/H and $H\backslash G$ have the same cardinality.*

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

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 4.2.2. 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

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

(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.

Theorem 4.2.3 (Lagrange's Theorem)**.** *Let G be a finite group and H a subgroup of G. Then $|G| = [G : H] \cdot |H|$. In other words, $|H|$ divides $|G|$.*

Proof. Since ρ_L is an equivalence relation on G, 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 $|G/H| = [G : H]$ is the index of H in G. This completes the proof. □

Exercise 4.2.3. 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 4.2.4. *Let G be a finite group of order n. Then for any $a \in G$, $\operatorname{ord}(a)$ 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 4.2.3, $|H|$ divides $|G| = n$. Since $|H| = \operatorname{ord}(a)$, the result follows. To see the second part, note that if $\operatorname{ord}(a) = k$, then $n = km$, for some $m \in \mathbb{N}$, and so $a^n = (a^k)^m = e^m = e$. □

Exercise 4.2.4. 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 $f : G \to G$ defined by $f(a) = a^k$, $\forall\, a \in G$, is injective, and hence is bijective.

Corollary 4.2.5. *Any group of prime order is cyclic.*

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

Corollary 4.2.6 (Euler's Theorem)**.** *Let $n \geq 2$ be an integer. Then for any positive integer a with $\gcd(a, n) = 1$, we have $a^{\phi(n)} \equiv 1$ (mod n), where $\phi(n)$ is the number of elements in the set $\{k \in \mathbb{N} : 1 \leq k < n \text{ and } \gcd(k, n) = 1\}$.*

Proof. Note that, $U_n := \{[a] \in \mathbb{Z}_n : \gcd(a, n) = 1\}$ is a finite subset of $\mathbb{Z}_n$ containing $\phi(n)$ elements. Since U_n is a group with respect to the multiplication operation modulo n, for any $[a] \in U_n$ we have $[a]^{\phi(n)} = [1]$ by Corollary 4.2.4. In other words, $a^{\phi(n)} \equiv 1$ (mod n). $\square$

Corollary 4.2.7 (Fermat's little theorem)**.** *If $p > 0$ is a prime number, then for any positive integer a with $\gcd(a, p) = 1$, we have $a^{p-1} \equiv 1$ (mod p).*

Proof. Since $\phi(p) = |U_p| = p - 1$, the result follows from the Corollary 4.2.6. $\square$

Exercise 4.2.5. Show that $2^{6000} - 1$ is divisible by 7.

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

Exercise 4.2.6. Show that $15^{1000} - 1$ and $105^{1200} - 1$ are divisible by 8.

Exercise 4.2.7. Let G and H be finite groups of order m and n, respectively. If $\gcd(m, n) = 1$, show that any group homomorphism from G into H is trivial. (*Hint:* Use Proposition 3.2.1 (iii), 3.2.2 (i) and Theorem 4.2.3).

Exercise 4.2.8. Let G be a group generated by two elements $a, b \in G$ that satisfy $\mathrm{ord}(a) = \mathrm{ord}(b) = 2$ and $ab = ba$. Show that G is isomorphic to the Klein's four group.

Proposition 4.2.8. *Any group of order 4 is isomorphic to either $\mathbb{Z}_4$ or K_4.*

Proof. Let G be a group of order 4. If G contains an element of order 4, then G is cyclic, and hence is isomorphic to $\mathbb{Z}_4$ by Proposition 3.3.3. Suppose that G has no elements of order 4. Then any non-identity element of G has order 2 by Lagrange's theorem 4.2.3. Let $G = \{e, a, b, c\}$, where a, b and c are distinct elements of order 2. If $ab = e$, then $b = a^{-1} = a$, since $\mathrm{ord}(a) = 2$, which is not possible as $a \neq b$. If $ab = a$ or $ab = b$, then by cancellation property (see Lemma 1.1.4) we have $b = e$ or $a = e$, which contradict our assumptions that $a \neq e \neq b$. Therefore, we must have $ab = c$. Similarly, $ba = c$. Therefore, $G = \{e, a, b, c\}$, where $\mathrm{ord}(a) = \mathrm{ord}(b) = 2$ and $ab = ba = c$, which is exactly the presentation of the Klein's four group (see Example 1.1.4). Therefore, $G \cong K_4$. $\square$

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 $f : G \to T$ such that $H \subseteq \mathrm{Ker}(f)$. Then we have $f(a) = f(b)$ if $a^{-1}b \in H$. The commutativity of the diagram (4.1.0.1) tells us to send $aH \in Q$ to $f(a) \in T$ to define the map $\widetilde{f} : Q \to T$ which needs to be a group homomorphism. Then we should have

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

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

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

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

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

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. □

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. (i) Let H be a subgroup of an abelian group G. Show that H is normal in G.

(ii) Let H 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) Is the subgroup $K := \langle\, (1\ \ 2) \rangle$ of S_3 normal in S_3?

(iv) Show that $Z(G) := \{a \in G : ab = ba,\ \forall\, b \in G\}$ is a normal subgroup of G.

Exercise 4.3.2. 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. □

Exercise 4.3.3. For all $n \geq 3$, show that $[S_n : A_n] = 2$ to conclude that A_n is a normal subgroup of S_n.

Solution: Since $\sigma^{-1}\tau \in A_n$, for all $\sigma, \tau \in S_n \setminus A_n$, we see that $\sigma A_n = \tau A_n$. Therefore, A_n has only two left cosets in S_n, namely A_n and σA_n, where $\sigma \in S_n \setminus A_n$. Therefore, $[S_n : A_n] = 2$, and hence A_n is normal in S_n by Proposition 4.3.2. □

Exercise 4.3.4. Show that S_4 has no normal subgroup of order 3.

Solution: Let H be a subgroup of S_4 of order 3. Then H is cyclic by Corollary 4.2.5, and it contains exactly two elements of order 3 by Exercise 1.3.4. It follows from Theorem 2.2.2 and Exercise 2.2.6 that if $\sigma \in S_4$ has order 3, then σ is a 3-cycle in S_4. Now there are $\frac{4!}{3} = 8$ distinct 3-cycles in S_4 by Exercise 2.2.3, and all of them are conjugates by Proposition 2.2.3. If H is a normal subgroup H of S_4, then it must contains all 3-cycles of S_4 and hence it contains at least 8 elements, which is a contradiction. □

Exercise 4.3.5. Let H be a subgroup of G. Let $\rho = \{(a,b) \in G \times G : a^{-1}b \in H\} \subseteq G \times G$. Note that ρ is an equivalence relation on G. Show that H is a normal subgroup of G if and only if ρ is a subgroup of the direct product group $G \times G$ (see Exercise 1.1.5).

Lemma 4.3.3. *Let $f : G \to H$ be a group homomorphism. Then $\operatorname{Ker}(f)$ is a normal subgroup of G.*

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

Exercise 4.3.6. For $n \geq 2$, show that A_n is a normal subgroup of S_n by constructing a group homomorphism $\varphi : S_n \to \mu_2 = \{1, -1\}$ such that $\operatorname{Ker}(\varphi) = A_n$.

Exercise 4.3.7. Show that $\mathrm{SL}_n(\mathbb{R})$ is a normal subgroup of $\mathrm{GL}_n(\mathbb{R})$, for all $n \geq 1$.

Lemma 4.3.4. *Let $f : G \to H$ be a group homomorphism. If K is a normal subgroup of H, then $f^{-1}(K)$ is a normal subgroup of G.*

Proof. Let K be 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 $aba^{-1} \in f^{-1}(K)$. $\square$

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?

Exercise 4.3.8. Show that any group of order 6 is isomorphic to either $\mathbb{Z}_6$ or S_3.

Solution: Recall that $\mathbb{Z}_6$ and S_3 are groups of order 6 that are not isomorphic to each other by Exercise 3.2.5. Let G be a group of order 6. If G has an element of order 6, then G is cyclic by Corollary 1.3.7, and hence $G \cong \mathbb{Z}_6$ by Proposition 3.3.3. Assume that G has no elements of order 6. Since $|G| = 6$ is even, G contains an element, say a, of order 2 by Exercise 1.2.22. If all non-identity elements of G has order 2, then G is abelian by Exercise 1.2.23. Then for any two distinct elements $x, y \in G \setminus \{e\}$, the subgroup $H = \langle x, y \rangle$ of G is isomorphic to K_4 (verify!), which is not possible by Lagrange's theorem 4.2.3. Therefore, G contains an element, say b, of order 3. Then $K := \langle b \rangle = \{e, b, b^2\}$ is a subgroup of G of index $[G : K] = 2$ by Theorem 4.2.3, and hence is normal in G by Proposition 4.3.2. Since $\operatorname{ord}(a) = 2$, by Lagrange's theorem we have $a \notin K$, and hence $aK \neq K$. Then $K \cap aK = \emptyset$ and that $K \sqcup aK = G$. Thus, $G = \{e, b, b^2, a, ab, ab^2\}$. Since K is normal in G, we have $aba^{-1} \in \{e, b, b^2\} = K$. If $aba^{-1} = e$, then $b = e$, which is not possible as $\operatorname{ord}(b) = 3$. If $aba^{-1} = b$, then $ab = ba$. Then $\operatorname{ord}(ab) = \operatorname{ord}(a) \cdot \operatorname{ord}(b) = 6$ by Exercise 1.2.19, which is not possible since G is not cyclic by assumption. Then we must have $aba^{-1} = b^2$. Thus we see that $G = \langle a, b \rangle = \{e, b, b^2, a, ab, ab^2\}$, where $\operatorname{ord}(a) = 2$, $\operatorname{ord}(b) = 3$ and $aba^{-1} = b^2$. This is exactly the presentation of the group S_3 as the dihedral group of degree 3 (see Exercise 2.4.5 and Exercise 2.4.6). Therefore, $G \cong S_3$. $\square$

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, π) of G by H exists and is unique in the sense that if (Q, π) and (Q', π') are two quotients of G by H, then there exists a unique isomorphism of groups $\varphi : Q \to Q'$ such that $\varphi \circ \pi' = \pi$. We denote Q by G/H.*

Proof. Since H is a normal subgroup of G,

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

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

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

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

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

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

$$\pi : G \longrightarrow Q$$

defined by

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

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

$$\widetilde{t} : G/H \to T, \ \ aH \longmapsto t(a), \tag{4.4.0.1}$$

is well-defined. Since

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

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

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 $\operatorname{Ker}(\pi) = H$.*

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

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

This completes the proof. □

Proposition 4.4.3. *Let H be a normal subgroup of G, and let $\pi : G \to Q$ be a surjective group homomorphism. Then the pair (Q, π) is a quotient group of G by H in the sense of Definition 4.1.1 if and only if $\operatorname{Ker}(\pi) = H$.*

Proof. Suppose that $\operatorname{Ker}(\pi) = H$. Since $\pi(h) = e_Q$, for all $h \in H$, property (i) in Definition 4.1.1 is verified. To verify the universal property (ii), let $\varphi : G \to T$ be a surjective group homomorphism such that $\varphi(h) = e_T$, for all $h \in H$. To define a map $\widetilde{\varphi} : Q \to T$ satisfying $\widetilde{\varphi} \circ \pi = \varphi$, for given $q \in Q$ using surjectivity of π we can choose an element $a \in G$ such that $\pi(a) = q$, and then set

$$\widetilde{\varphi}(q) = \varphi(a) \in T.$$

If $\pi(a) = q = \pi(b)$, for some $a, b \in G$, then π being a group homomorphism we have $\pi(a^{-1}b) = e_Q$, and so $a^{-1}b \in \operatorname{Ker}(\pi) = H$. Since $H \subseteq \operatorname{Ker}(\varphi)$ by assumption, we have $\varphi(a^{-1}b) = e_T$, and hence $\varphi(a) = \varphi(b)$ as φ is a group homomorphism. Thus we get a well-defined map

$$\widetilde{\varphi} : Q \to T$$

such that $\widetilde{\varphi} \circ \pi = \varphi$ by its construction. To show that $\widetilde{\varphi}$ is a group homomorphism, for given $x, y \in Q$ using surjectivity of π we can choose $a, b \in G$ such that $\pi(a) = x$ and $\pi(b) = y$. Then by construction of $\widetilde{\varphi}$ we have

$$\widetilde{\varphi}(x) = \varphi(a) \text{ and } \widetilde{\varphi}(y) = \varphi(b).$$

Now π being a group homomorphism we have $\pi(ab) = \pi(a)\pi(b) = xy$ so that

$$\begin{aligned}\widetilde{\varphi}(xy) &= \varphi(ab)\\ &= \varphi(a)\varphi(b)\\ &= \widetilde{\varphi}(x)\widetilde{\varphi}(y).\end{aligned}$$

It remains to show uniqueness of $\widetilde{\varphi}$. Let $\psi : Q \to T$ be a group homomorphism such that $\psi \circ \pi = \varphi$. Then for given $x \in Q$ choosing an element $a \in G$ with $\pi(a) = x$ we see that

$$\psi(x) = \psi(\pi(a)) = \varphi(a) = \widetilde{\varphi}(x).$$

Therefore, $\psi = \widetilde{\varphi}$ as required.

Conversely suppose that (Q, π) is a quotient of G by H in the sense of Definition 4.1.1. Then $\pi : G \to Q$ is a surjective group homomorphism with $H \subseteq \mathrm{Ker}(\pi)$ by property (i) in Definition 4.1.1. To show that $\mathrm{Ker}(\pi) = H$, we take $T = G/H := \{aH : a \in G\}$, the set of all left cosets of H in G equipped with the binary operation defined by

$$aH \cdot bH := abH,\ \forall\, aH, bH \in G/H.$$

Note that this is a well-defined binary operation on the set G/H making it a group because H is normal in G (see Proposition 4.3.1). The map $\pi_H : G \to G/H$ defined by

$$\pi_H(a) = aH,\ \forall\, a \in G,$$

is a surjective group homomorphism with $\mathrm{Ker}(\pi_H) = H$. Then by universal property (ii) in Definition 4.1.1 of (Q, π), there exists a unique group homomorphism $\widetilde{\pi_H} : Q \to G/H = T$ such that $\widetilde{\pi_H} \circ \pi = \pi_H$.

$$\begin{tikzcd} G \arrow[rr, "\pi_H"] \arrow[dr, "\pi"'] & & G/H =: T \\ & Q \arrow[ur, "\widetilde{\pi_H}"'] & \end{tikzcd}$$

Now if $H \neq \mathrm{Ker}(\pi)$, then there exists an element, say $a \in \mathrm{Ker}(\pi)$, such that $a \notin H$. Then $aH \neq H$ in $G/H = T$, and hence $aH \neq e_T$. But then

$$e_T \neq \pi_H(a) = (\widetilde{\pi_H} \circ \pi)(a) = \widetilde{\pi_H}(e_Q) = e_T,$$

which is a contradiction. Therefore, we must have $H = \mathrm{Ker}(\pi)$. $\square$

Remark 4.4.1. The above Proposition 4.4.3 enable us to formulate an equivalent definition of a *quotient group of G by a normal subgroup $H \trianglelefteq G$* to be a pair (Q, π), where Q is a group and $\pi : G \to Q$ is a surjective group homomorphism with $\mathrm{Ker}(\pi) = H$.

Exercise 4.4.1. Let G be a group. If $G/Z(G)$ 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 $xZ = (aZ)^n = a^n Z$, 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. □

4.5 Another way to quotient groups

In this section we give an equivalent way to define the notion of a quotient group and prove its uniqueness without appealing to its universal property as done in §4.1. Those who find it difficult to digest the definition of quotient group using its universal property, may find this point-of-view a bit easier.

Let G be a group. A *quotient group* of G is a pair (Q, π), where Q is a group and $\pi : G \to Q$ is a surjective group homomorphism. Note that the kernel of π,

$$K := \mathrm{Ker}(\pi) = \{a \in G : \pi(a) = e_Q\},$$

has the following property:

$$aba^{-1} \in K, \ \forall\, a \in G \ \text{ and } \ b \in K. \tag{4.5.0.1}$$

A subgroup K of G satisfying (4.5.0.1) is called a *normal subgroup of* G; in this case, we express it symbolically as $K \trianglelefteq G$.

Definition 4.5.1. A *quotient group of* G *by a normal subgroup* H *of* G is a pair (Q, π), where Q is a group and $\pi : G \to Q$ is a surjective group homomorphism with $\mathrm{Ker}(\pi) = H$.

To construct a quotient (Q, π) of G by a normal subgroup H of G, we consider the set of all left cosets (see §4.2) of H in G,

$$G/H := \{aH : a \in G\},$$

and define a binary operation on G/H by setting

$$aH \cdot bH := (ab)H, \ \forall\, aH, bH \in G/H. \tag{4.5.0.2}$$

Since H is a normal subgroup of G, (4.5.0.2) gives a well-defined binary operation on the set G/H by Proposition 4.3.1. Moreover, the set G/H is a group with respect to the above defined binary operation (c.f. proof of Theorem 4.4.1). Define a map

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

by setting

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

Since $\pi(ab) = (ab)H = (aH)\cdot(bH) = \pi(a)\pi(b)$, for all $a, b \in G$, the map π is a group homomorphism. Since any element of G/H is of the form aH, for some $a \in G$, the map π is surjective. Note that

$$\mathrm{Ker}(\pi) = \{a \in G : aH = H\} = H.$$

Therefore, the pair $(G/H, \pi)$ is a quotient of G by the normal subgroup H according to the Definition 4.5.1.

Lemma 4.5.1. *Let H be a normal subgroup of G. Let $\varphi : G \to T$ be a group homomorphism such that $H \subseteq \mathrm{Ker}(\varphi)$. Then there exists a unique group homomorphism $\widetilde{\varphi} : G/H \to T$ such that $\widetilde{\varphi} \circ \pi = \varphi$.*

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & T \\ G/H \arrow[ur, dashed, "\exists!\widetilde{\varphi}"'] & \end{tikzcd}$$

Proof. Define a map $\widetilde{\varphi} : G/H \to T$ by setting

$$\widetilde{\varphi}(aH) = \varphi(a), \ \forall\, aH \in G/H.$$

Let $a, b \in G$ be such that $aH = bH$. Then $a^{-1}b \in H$. Since $H \subseteq \mathrm{Ker}(\varphi)$, we have $\varphi(a^{-1}b) = e$. Since φ is a group homomorphism, we have $\varphi(a)^{-1}\varphi(b) = e$, and hence $\varphi(a) = \varphi(b)$. Therefore, $\widetilde{\varphi}(aH) = \varphi(a) = \varphi(b) = \widetilde{\varphi}(bH)$, and so $\widetilde{\varphi}$ is a well-defined map. Since

$$\begin{aligned} \widetilde{\varphi}(aH \cdot bH) &= \widetilde{\varphi}(abH) \\ &= \varphi(ab) \\ &= \varphi(a)\varphi(b) \\ &= \widetilde{\varphi}(aH)\widetilde{\varphi}(bH), \ \ \forall\, aH, bH \in G/H, \end{aligned}$$

the map $\widetilde{\varphi}$ is a group homomorphism. Since

$$(\widetilde{\varphi} \circ \pi)(a) = \widetilde{\varphi}(aH) = \varphi(a), \ \ \forall\, a \in G,$$

we have $\widetilde{\varphi} \circ \pi = \varphi$.

It remains to show uniqueness of $\widetilde{\varphi}$. Let $\psi : G/H \to T$ be any group homomorphism such that $\psi \circ \pi = \varphi$. Then for any $aH \in G/H$ we have

$$\psi(aH) = \psi(\pi(a)) = \varphi(a) = \widetilde{\varphi}(aH).$$

Therefore, $\psi = \widetilde{\varphi}$. This completes the proof. $\square$

Corollary 4.5.2 (Uniqueness of quotient group). *Let H be a normal subgroup of a group G. Let $\varphi : G \to Q$ be a surjective group homomorphism with $\mathrm{Ker}(\varphi) = H$. Then there exists a unique isomorphism of groups $\widetilde{\varphi} : G/H \to Q$ such that $\widetilde{\varphi} \circ \pi = \varphi$.*

$$\begin{tikzcd} & G \arrow[dl, "\pi"'] \arrow[dr, "\varphi"] & \\ G/H \arrow[rr, "\widetilde{\varphi}"] & & Q \end{tikzcd}$$

In other words, quotient of G by a normal subgroup H of G exists and is unique unto a unique isomorphism.

Proof. Since $H = \mathrm{Ker}(\varphi)$, by Lemma 4.5.1 we have a unique group homomorphism $\widetilde{\varphi} : G/H \to Q$ such that $\widetilde{\varphi} \circ \pi = \varphi$. Since φ is surjective, so is $\widetilde{\varphi}$ (verify!). To complete the proof, it suffices to show that $\mathrm{Ker}(\widetilde{\varphi})$ is trivial. Let $aH \in \mathrm{Ker}(\widetilde{\varphi})$ be given. Then

$$\varphi(a) = (\widetilde{\varphi} \circ \pi)(a) = \widetilde{\varphi}(aH) = e,$$

and so $a \in \mathrm{Ker}(\varphi) = H$. This implies that $aH = H$. Thus $\mathrm{Ker}(\widetilde{\varphi}) = \{H\}$ is the trivial subgroup of G/H, and hence $\widetilde{\varphi}$ is injective. This completes the proof. □

Remark 4.5.1. To get a group homomorphism from a quotient group G/H to a group G', thanks to Lemma 4.5.1 we just need to define a group homomorphism $\varphi : G \to G'$ such that $H \subseteq \mathrm{Ker}(\varphi)$.

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

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

is the natural quotient homomorphism given by

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

Then as an immediate application of Lemma 4.5.1, we have the following.

Theorem 5.1.1 (First Isomorphism Theorem). *Let $\varphi : G \to H$ be a homomorphism of groups. Then φ induces a unique isomorphism*

$$\widetilde{\varphi} : G/\mathrm{Ker}(\varphi) \to f(G)$$

onto the subgroup $\varphi(G) \subseteq H$ such that $\widetilde{\varphi} \circ \pi = \varphi$, where $\pi : G \to G/\mathrm{Ker}(\varphi)$ is the natural homomorphism onto the quotient group. Moreover, if φ is surjective then $\widetilde{\varphi} : G/\mathrm{Ker}(\varphi) \to H$ is an isomorphism.

Proof. This is essentially Corollary 4.5.2. □

Example 5.1.1. Consider the map $f : \mathbb{R} \to S^1$ defined by

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

Since $f(s+t) = e^{2\pi i(s+t)} = e^{2\pi i s}e^{2\pi i t} = f(s)f(t)$, for all $s, t \in \mathbb{R}$, the map f is a group homomorphism. Since any element of S^1 is of the form $e^{2\pi i t}$, for some $t \in \mathbb{R}$, the map f is surjective. Since

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

by first isomorphism theorem we have $\mathbb{R}/\mathbb{Z} \cong S^1$.

Exercise 5.1.1. For given $n \geq 2$ consider the map $f : \mathbb{C}^* \to \mathbb{C}^*$ defined by

$$f(z) = z^n, \ \forall\, z \in \mathbb{C}^*.$$

Show that f is a surjective group homomorphism with $\mathrm{Ker}(f) = \mu_n$ (see Example 1.1.4 (v)). Conclude that $\mathbb{C}^*/\mu_n \cong C^*$.

Exercise 5.1.2. Show that the map $f : \mathbb{C}^* \to S^1$ defined by

$$f(z) = z/|z|, \ \forall\, z \in \mathbb{C}^*,$$

is a surjective group homomorphism with $\mathrm{Ker}(f) = \mathbb{R}^+ := \{t \in \mathbb{R} : t > 0\}$. Conclude that $\mathbb{C}^*/\mathbb{R}^+ \cong S^1$.

Exercise 5.1.3. Consider the map $f : \mathbb{C}^* \to S^1$ defined by

$$f(z) = z^2/|z|^2, \ \forall\, z \in \mathbb{C}^*.$$

Show that f is a surjective group homomorphism with $\mathrm{Ker}(f) = \mathbb{R}^*$. Conclude that $\mathbb{C}^*/\mathbb{R}^* \cong S^1$.

Exercise 5.1.4. Let $f : G \to Q$ be a surjective group homomorphism with Q finite. Let H be a finite subgroup of G such that $\gcd(|H|, |Q|) = 1$. Show that $H \subseteq \mathrm{Ker}(f)$.

Solution: Since $f(H)$ is a subgroup of the finite group Q, by Lagrange's theorem $|f(H)|$ divides $|Q|$. Since $f\big|_H : H \to f(H)$ is a surjective group homomorphism, by first isomorphism theorem we have $H/\mathrm{Ker}(f\big|_H) \cong f(H)$. Since $|H|$ is finite, we see that $|f(H)|$ divides $|H|$. Therefore, $|f(H)|$ divides $\gcd(|H|, |Q|) = 1$. Therefore, $|f(H)| = 1$, and hence $H \subseteq \mathrm{Ker}(f)$. □

Theorem 5.1.2 (Chinese Reminder Theorem for Groups)**.** *Let H and K be normal subgroups of a group G. Then the following holds.*

(i) $H \cap K$ is a normal subgroup of G.

(ii) $G/(H \cap K)$ is isomorphic to a subgroup of $(G/H) \times (G/K)$.

(iii) If $G = HK$, then $G/(H \cap K) \cong (G/H) \times (G/K)$.

Proof. (i) Let H and K be two normal subgroups of a group G. Consider the map

$$\varphi : G \to (G/H) \times (G/K)$$

defined by

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

Since for all $a, b \in G$ we have

$$\begin{aligned}\varphi(ab) &= ((ab)H, (ab)K)\\ &= (aH \cdot bH, aK \cdot bK)\\ &= (aH, aK) \cdot (bH, bK) = \varphi(a)\varphi(b),\end{aligned}$$

the map φ is a group homomorphism. Since

$$\begin{aligned}\operatorname{Ker}(\varphi) &= \{a \in G : (aH, aK) = (H, K)\}\\ &= \{a \in G : a \in H \text{ and } a \in K\}\\ &= H \cap K,\end{aligned}$$

the subgroup $H \cap K$ is normal in G by Lemma 4.3.3.

(ii) By first isomorphism theorem (Theorem 5.1.1) φ induces a unique injective homomorphism of groups

$$\widetilde{\varphi} : G/(H \cap K) \longrightarrow (G/H) \times (G/K)$$

such that $\widetilde{\varphi} \circ \pi_{H\cap K} = \varphi$, where $\pi_{H\cap K} : G \to G/H \cap K$ is the quotient homomorphism. Therefore, $G/(H \cap K)$ is isomorphic to the subgroup $\widetilde{\varphi}(G/(H \cap K))$ of $G/H \times G/K$.

(iii) Suppose that $G = HK$. To show $\widetilde{\varphi}$ is an isomorphism in this case, it suffices to show that φ is surjective. Let $(aH, bK) \in (G/H) \times (G/K)$ be given. We claim that $aH \cap bK \neq \emptyset$. Since $G = HK$, we have $a = hk$, for some $h \in H$ and $k \in K$. Then we have $ak^{-1} = h \in H$ and so $Ha = Hk$. Similarly, $b \in G = HK$ implies that $b = h'k'$, for some $h' \in H$ and $k' \in K$. Then $h'^{-1}b = k' \in K$ implies that $bK = h'K$. Then $c := h'k \in Hk \cap h'K = Ha \cap bK = aH \cap bK$, where the equality $Ha = aH$ holds because H is normal in G (see Exercise 4.3.2). This proves our claim. Now choosing any $c \in aH \cap bK$ we have $aH = cH$ and $bK = cK$, and hence $\varphi(c) = (cH, cK) = (aH, bK)$ as required. Thus, φ is surjective and hence $\widetilde{\varphi}$ is an isomorphism of groups. □

Exercise 5.1.5. Let G_1 and G_2 be two groups, and let H_1 and H_2 be normal subgroups G_1 and G_2, respectively. Prove or disprove the following statements.

(i) $H_1 \times H_2$ is a normal subgroup of $G_1 \times G_2$, and

(ii) $(G_1 \times G_2)/(H_1 \times H_2) \cong (G_1/H_1) \times (G_2/H_2)$.

Let G be a group. Note that given a normal subgroup N of G, the quotient group G/N of G by N comes with a natural surjective group homomorphism $\pi_N : G \to G/N$ such that $\operatorname{Ker}(\pi_N) = N$ (see Definition 4.1.1 and Corollary 4.4.2). On the other hand, given a group Q and a surjective group homomorphism $\pi : G \to Q$, its kernel $\operatorname{Ker}(\pi)$ is a normal subgroup of G such that $G/\operatorname{Ker}(\pi) \cong Q$ by the First isomorphism theorem (Corollary 5.1.1) for groups. As an immediate consequence, we have the following one-to-one correspondence between the set of all normal subgroups of G and the set of all quotient groups of G.

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

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

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

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

Since

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

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

Proposition 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 $f : \mathbb{Z} \to G$ by

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

Since

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

f is a group homomorphism. Clearly f is surjective because every element of G is of the form a^k, for some $k \in \mathbb{Z}$. Then by first isomorphism theorem G is isomorphic to $\mathbb{Z}/\mathrm{Ker}(f)$. Note that, $\mathrm{Ker}(f) = \{k \in \mathbb{Z} : a^k = e\}$. Since G is a cyclic group of order n generated by a, we have $\mathrm{ord}(a) = n$ (see Corollary 1.3.6). Then we have $\mathrm{Ker}(f) = \{k \in \mathbb{Z} : a^k = e\} = n\mathbb{Z}$. Therefore, $G \cong \mathbb{Z}/n\mathbb{Z}$. Since $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ by Theorem 5.1.4, we have $G \cong \mathbb{Z}_n$. □

Exercise 5.1.6. Show that A_n is the only subgroup of S_n with index 2.

Exercise 5.1.7. Show that $\mathrm{SL}_2(\mathbb{Z}_3)$ and S_4 are two non-isomorphic non-commutative groups of order 24. (*Hint:* Look at their centers!).

Exercise 5.1.8. 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 3.3.5) G is isomorphic to a subgroup, say H, of the symmetric group $S(G)$ via the monomorphism $\varphi : G \to S(G) \cong S_{2n}$ defined by sending $a \in G$ to the bijective map $\varphi_a : G \to G$ 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 φ_a is n, an odd number. So φ_a is an odd permutation. This shows that the subgroup $H := \varphi(G)$ contains an odd permutation. Define a map

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

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 5.1.1) we have

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

Then we have

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

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

5.2 Abelianization

Theorem 5.2.1 (Abelianization)**.** *Let G be a group. Then there exists a pair (G_{ab}, Φ) consisting of an abelian group G_{ab} and a surjective group homomorphism $\Phi : G \to G_{\mathrm{ab}}$ satisfying the following universal property:*

- *given any abelain group H and a group homomorphism $f : G \to H$, there exists a unique group homomorphism $\widetilde{f} : G_{\mathrm{ab}} \to H$ such that $\widetilde{f} \circ \Phi = f$.*

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

The pair (G_{ab}, Φ) is unique in the sense that given any surjective group homomorphism $\psi : G \to A$ with A abelian, if the pair (A, ψ) satisfies the above universal property, then there exists a unique isomorphism of groups $\widetilde{\psi} : G_{\mathrm{ab}} \to A$ such that $\widetilde{\psi} \circ \Phi = \psi$. The group G_{ab} is known as the maximal abelian quotient of G and the pair (G_{ab}, Φ) is called the abelianization of G.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Therefore, $[\sigma,\tau] \in A_n$, for all $\sigma, \tau \in S_n$, and hence $[S_n, S_n] \subseteq A_n$. To show the reverse inclusion, note that A_n is generated by 3-cycles, for all $n \geq 3$ (see Exercise 2.4.1), 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 $A_n \subseteq [S_n, S_n]$ completing the proof. □

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

Exercise 5.2.2. Given any two groups H and K, let $\operatorname{Hom}(H,K)$ 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 $\operatorname{Hom}(S_n, G) \longrightarrow \operatorname{Hom}(\mathbb{Z}_2, G)$.

(ii) Find the number of elements in $\operatorname{Hom}(S_n, \mathbb{Z}_4 \times \mathbb{Z}_6)$.

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 $\varphi_a : G \to G$ defined by

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

is a group homomorphism. Indeed,

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

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

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

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

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

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

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

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

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

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

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

by first isomorphism theorem (see Corollary 5.1.1) 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 $\mathrm{lcm}(m, n) = mn$, and so $H \cap K = mn\mathbb{Z}$. Then by the second isomorphism theorem we have $m\mathbb{Z}/mn\mathbb{Z} = H/(H \cap K) \cong (H + K)/K = \mathbb{Z}/n\mathbb{Z}$. Generalize this to the case when m and n are not necessarily coprime.

Exercise 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) $\phi : G \to G/H$,

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

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

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

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

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

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

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

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

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

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

Then by first isomorphism theorem (Corollary 5.1.1) applied to the group homomorphism $\pi \circ \psi$ we have the required isomorphism $G/H \cong (G/K)/(H/K)$ of groups. ∎

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

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

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

Then there is an inclusion preserving bijective map

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

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

Proof. Define a map $\Phi : \mathcal{A} \to \mathcal{B}$ by sending a subgroup N of G containing $\operatorname{Ker}(f)$ 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 $\operatorname{Ker}(f) = f^{-1}(e) \subseteq f^{-1}(K)$. Thus, $f^{-1}(K) \in \mathcal{A}$. This gives a map

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

It remains to show that Φ and Ψ are inverse to each other. Given $N \in \mathcal{A}$, we have $(\Psi \circ \Phi)(N) = f^{-1}(f(N)) \supseteq N$. If $a \in f^{-1}(f(N))$, then $f(a) = f(b)$, for some $b \in N$. Then $f(ab^{-1}) = f(a)f(b)^{-1} = e_H$ implies $ab^{-1} \in \operatorname{Ker}(f) \subseteq N$, 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 $\Psi \circ \Phi = \operatorname{Id}_{\mathcal{A}}$. Conversely, given $K \in \mathcal{B}$, we have $(\Phi \circ \Psi)(K) = f(f^{-1}(K)) = K$, since f is surjective. Thus $\Phi \circ \Psi = \operatorname{Id}_{\mathcal{B}}$. 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 $\pi : G \to Q$ be a surjective group homomorphism. Let H be a normal subgroup of G and let $\pi_H : H \to Q$ be the restriction of π on H. If $K = H \cap \operatorname{Ker}(\pi)$, show that the induced map $\widetilde{\pi_H} : H/K \to Q$ 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 $\{\pi_\alpha : G \to G_\alpha\}_{\alpha\in\Lambda}$ is a family of group homomorphisms such that given any group H and a family of group homomorphisms $\{f_\alpha : H \to G_\alpha\}_{\alpha\in\Lambda}$ there exists a **unique** group homomorphism $f : H \to G$ such that $\pi_\alpha \circ f = f_\alpha$, for all $\alpha \in \Lambda$.

$$\begin{tikzcd} H \arrow[d, dashed, "\exists ! f"'] \arrow[dr, "f_\alpha"] & \\ G \arrow[r, "\pi_\alpha"] & G_\alpha \end{tikzcd}$$

Theorem 6.1.1 (Existence & Uniqueness of Direct Product of Groups)**.** *The direct product of a family of groups exists and is unique upto a unique isomorphism in the sense that if $(G, \{g_\alpha : G \to G_\alpha\}_{\alpha\in\Lambda})$ and $(H, \{h_\alpha : H \to G_\alpha\}_{\alpha\in\Lambda})$ are direct products of the family of groups $\{G_\alpha : \alpha \in \Lambda\}$, then there exists a unique isomorphism of groups $\phi : G \to H$ such that $h_\alpha \circ \phi = g_\alpha$, for all $\alpha \in \Lambda$. We denote by $\prod\limits_{\alpha\in\Lambda} G_\alpha$ the underlying group of the direct product of the family of groups $\{G_\alpha : \alpha \in \Lambda\}$.*

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

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

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

For a construction, let

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

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

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

by

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

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

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

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) := (a_1b_1, \ldots, a_nb_n), \tag{6.1.0.1}$$

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

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

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

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

Since

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

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

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

$$p_i : G_1 \times \cdots \times G_n \to G_i \tag{6.1.0.2}$$

be the map defined by

$$p_i(a_1, \ldots, a_n) = a_i, \ \forall\, (a_1, \ldots, a_n) \in G_1 \times \cdots \times G_n. \tag{6.1.0.3}$$

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

$$f(h) = (f_1(h), \ldots, f_n(h)), \ \ \forall\, h \in H. \tag{6.1.0.4}$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 $hk = kh$.*

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

Proposition 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 $G_1, \ldots, G_n$, and $H_i := \{(a_1, \ldots, a_n) \in G : a_j = e_j, \ \forall\, j \neq i\}$, for each $i \in I_n$. Then G is an internal direct product of $H_1, \ldots, H_n$, respectively.*

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

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

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

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

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

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

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

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

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

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

Exercise 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*

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

satisfying the following universal property:

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

$$\begin{tikzcd} A_\alpha \arrow[r, "f_\alpha"] \arrow[d, "\iota_\alpha"'] & T \\ A \arrow[ur, "f"'] & \end{tikzcd}$$

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 $\bigoplus\limits_{\alpha\in\Lambda} A_\alpha$.*

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_α additively. Given $\alpha \in \Lambda$, let 0_α be the neutral element of A_α, and $\pi_\alpha : \prod\limits_{\beta\in\Lambda} A_\beta \to A_\alpha$ be the natural projection homomorphism. Given $x \in \prod\limits_{\alpha\in\Lambda} A_\alpha$, let $x_\alpha := \pi_\alpha(x) \in A_\alpha$. Consider the subset

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

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 $\prod\limits_{\alpha\in\Lambda} A_\alpha$. For each $\alpha \in \Lambda$, let $\iota_\alpha : A_\alpha \to A$ 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 ι_α is an injective group homomorphism, for all $\alpha \in \Lambda$. Let T be an abelian group. Let $f_\alpha : A_\alpha \to T$ be a group homomorphism, for each $\alpha \in \Lambda$. Define a map $f : A \to T$ by

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

Note that the above sum is finite. Since $f_\alpha : A_\alpha \to T$ 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 $\{A_1, \ldots, A_n\}$ be a finite collection of abelian groups and let $A_1 \times \cdots \times A_n$ be the direct product. Then for each $i \in \{1, \ldots, n\}$ the natural map

$$\varphi_i : A_i \to A_1 \times \cdots \times A_n$$

defined by sending $a \in A_i$ to the element $\varphi_i(a) \in A_1 \times \cdots \times A_n$ 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 $A_1 \times \cdots \times A_n$. Then by universal property of direct sum (Theorem 6.2.1), there is a unique group homomorphism

$$f : A_1 \oplus \cdots \oplus A_n \to A_1 \times \cdots \times A_n$$

such that $f \circ \iota_i = \varphi_i$, for all $i \in \{1, \ldots, n\}$. Clearly f is injective; in fact, it is the inclusion map. Given any $(a_1, \ldots, a_n) \in A_1 \times \cdots \times A_n$, we have $f(\sum\limits_{i=1}^{n} \iota_i(a_i)) = \sum\limits_{i=1}^{n} \varphi_i(a_i) = (a_1, \ldots, a_n)$. Therefore, f is surjective, and hence is an isomorphism. Thus, for a finite index set Λ, we have $\bigoplus\limits_{\alpha \in \Lambda} A_\alpha = \prod\limits_{\alpha \in \Lambda} A_\alpha$.

Remark 6.2.1. If we remove *abelian* hypothesis from A_α'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.

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

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

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

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

satisfying the following conditions:

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

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

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

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

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

satisfying the following conditions:

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

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

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

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

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

defined by

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

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

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

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

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

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

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

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

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

$$f_\sigma : G \to S(X) \tag{7.1.0.1}$$

that sends $a \in G$ to the map

$$f_\sigma(a) : X \to X,\ x \mapsto \sigma(a, x). \tag{7.1.0.2}$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Since

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

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

Example 7.1.3. Recall that Cayley's theorem (Theorem 3.3.5) says that any group G is isomorphic to a subgroup of the permutation group $S(G)$ on G. This can be explained using group action as follow. Consider the left translation map

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

defined by

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

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

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

Then f_σ is a group homomorphism with

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

is trivial, and hence σ is a faithful action.

7.2 Orbits and isotropy subgroups

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

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

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

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

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

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

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

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

Proposition 7.2.1. *Let $\sigma : G \times X \to X$ be a left G-action on X. For each $x \in X$ the subset*

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

is a subgroup of G, called the stabilizer or the isotropy subgroup of x, and sometimes it is also denoted by $\mathrm{Stab}_G(x)$.

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

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

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

$$\begin{tikzcd} G \times X \arrow[r, "\sigma"] \arrow[d, "\pi_H \times \mathrm{Id}_X"'] & X \arrow[d, equal] \\ (G/H) \times X \arrow[r, "\widetilde{\sigma}"] & X \end{tikzcd}$$

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

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

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

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

$$f_{\widetilde{\sigma}} : G/H \to S(X)$$

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

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

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

Exercise 7.2.2. Let $\sigma : G \times X \to X$ be a left G-action on X. Given $x \in X$ and $a \in G$, show that $G_y = aG_xa^{-1}$, where $y = \sigma(a, x) \in X$. Deduce that if σ is a transitive G-action on X, show that $\mathrm{Ker}(f_\sigma) = \bigcap\limits_{a \in G} aG_xa^{-1}$.

Exercise 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 $\bigcap\limits_{\sigma \in G} \sigma G_x \sigma^{-1} = \{e\}$.

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 $\varphi : G \to S(X)$ such that* $\mathrm{Ker}(\varphi) \subseteq H$.

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

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

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

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

that sends $a \in G$ to the map

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

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

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

Exercise 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. □

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 $f : G \to S(X)$ be the map that sends $a \in G$ to

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

Then f is a group homomorphism. Then $K := \mathrm{Ker}(f) \subseteq H$ by Corollary 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 5.1.1). Then by Lagrange's theorem $pk = |G/K|$ divides $|S_p| = p!$. Then k divides $(p-1)!$.

Since k is a divisor of n and p is the smallest prime divisor of n, unless $k = 1$, any prime divisor of k must be greater than or equal to p. But since k divides $(p-1)!$, any prime divisor of k is less than p. Thus we get a contradiction unless $k = 1$. Therefore, $[H : K] = k = 1$, and so $H = K = \mathrm{Ker}(f)$. Thus H is a normal subgroup of G. $\square$

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 7.2.6. 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 7.2.7. 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 $\sigma : G \times X \to X$ be a left G-action on X. Fix $x \in X$, and let $G/G_x = \{aG_x : a \in G\}$ be the set of all distinct left cosets of G_x in G. Then the map $\varphi : G/G_x \to \mathrm{Orb}_G(x)$ defined by $\varphi(aG_x) = \sigma(a, x)$, $\forall\, a \in G$, is a well-defined bijective map. Consequently, $[G : G_x] = |\mathrm{Orb}_G(x)|$.*

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

Corollary 7.2.7 (Class Equation)**.** *Let $\sigma : G \times X \to X$ be a left G-action on a non-empty finite set X, and let $\mathcal{O}$ be a subset of X containing exactly one element from each G-orbits in X. Then we have*

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

Proof. Since $X = \bigsqcup_{x \in \mathcal{O}} \mathrm{Orb}_G(x)$, the result follows from Proposition 7.2.6. $\square$

Exercise 7.2.8. 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 7.2.9. Fix $n \in \mathbb{N}$. Show that the map $\sigma : \mathrm{GL}_n(\mathbb{R}) \times \mathbb{R}^n \to \mathbb{R}^n$ defined by

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

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

Exercise 7.2.10. Let $\sigma : G \times G \to G$ be the left G-action on itself given by

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

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

Theorem 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 $\{x_1, \ldots, x_n\}$ be the subset of X consisting of exactly one element from each of the G-orbits in X. Note that two elements x and y of X are in the same G-orbit if and only if $\mathrm{Orb}_G(x) = \mathrm{Orb}_G(y)$. Since $|G|/|G_x| = [G : G_x] = |\mathrm{Orb}_G(x)|$, we conclude that $|G_x| = |G_y|$ whenever x and y are in the same G-orbit. Then we have

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

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

7.3 Class equation for conjugacy action

Let G be a group. Consider the map

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

Note that σ is a left action of G on itself, known as the conjugation action. Given $a \in G$, its σ-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) $$\mathrm{Orb}_G(a) = \{gag^{-1} : g \in G\}$$

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 $(n_1, \ldots, n_r)$ such that $n_1 \geq \cdots \geq n_r$ and $\sum\limits_{j=1}^{r} n_j = n$.

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 $\mathcal{C} = \{C_1, \ldots, C_k\}$ 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 $t : \mathcal{C} \to \mathcal{P}_n$ 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 2.2.5, the map t is well-defined and injective. Given a partition $(n_1, \ldots, n_r)$ of n, we have a permutation $\sigma = (1 \ \cdots \ n_1) \circ \cdots \circ (n_1 + \cdots + n_{r-1} + 1 \ \cdots \ n_1 + \cdots + n_r) \in S_n$ whose cycle type is precisely $(n_1, \ldots, n_r)$. 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) $$\sigma : G \times \mathcal{P}(G) \to \mathcal{P}(G), \ \ (a, S) \mapsto aSa^{-1},$$

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

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

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

(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 σ commutes with $e, \sigma, \ldots, \sigma^{r-1}$, and with all $\tau \in S_n$ whose cycles are disjoint from that of σ (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 $\{a_1, \ldots, a_n\}$ be the subset of G consisting of exactly one element from each conjugacy class that are not contained in $Z(G)$. Then we have*

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

Proof. Follows from Corollary 7.2.7 by taking $X = G$ and σ to be the conjugation action of G on itself. □

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

Corollary 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 4.2.3). 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. □

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 $m := \operatorname{ord}(a)$. Then $1 < m < n$. If $p \mid m$, then by induction hypothesis H has an element, say b, of order p, and we are done. Assume that $p \nmid m$. Since G is abelian, H is a normal subgroup of G. Then p divides the order of the quotient group G/H. Since $|G/H| = n/m < n$, by induction hypothesis G/H has an element, say $bH \in G/H$, of order p. Then $b^pH = (bH)^p = H$ in G/H, and so $b^p \in H$. Since $H = \langle a \rangle$ is a cyclic group of order m, we have $(b^m)^p = (b^p)^m = e$. Then $\operatorname{ord}(b^m) \mid p$. Since p is a prime number, either $b^m = e$ or $\operatorname{ord}(b^m) = p$. If $b^m = e$, then $(bH)^m = b^mH = eH = H$, and so $p = \operatorname{ord}(bH) \mid m$. This contradicts our assumption that $p \nmid m$. Therefore, $b^m \neq e$, and hence $\operatorname{ord}(b^m) = p$. □

Theorem 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

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

where $\{a_1, \ldots, a_r\}$ is the subset of G consisting of exactly one element from each G-orbits of that does not intersect $Z(G)$. Since $a \in Z(G)$ if and only if $C_G(a) = G$, we see that $|C_G(a_i)| < n$, for all $i \in \{1, \ldots, r\}$. If $p \mid |C_G(a_i)|$, for some $i \in \{1, \ldots, r\}$, then by induction hypothesis $C_G(a_i) \subseteq G$ has an element of order p, and we are done. Suppose that $p \nmid |C_G(a_i)|$, $\forall\, i \in \{1, \ldots, r\}$. Since $p \mid n = |G|$ and $|G| = |C_G(a_i)|[G : C_G(a_i)]$, we see that $p \mid [G : C_G(a_i)]$, $\forall\, i \in \{1, \ldots, r\}$. Since $Z(G)$ is a subgroup of G, $|Z(G)| \geq 1$. Then from class equation above, we see that p divides $|Z(G)|$. Since $Z(G)$ is abelian, it contains an element of order p by Proposition 7.3.5. This completes the proof. □

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

Corollary 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. □

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 $\mathrm{ord}(m/p^n)$ 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 $a \in G$, $\mathrm{ord}(a) \mid p^n$ by Lagrange's theorem (Theorem 4.2.3), and hence $\mathrm{ord}(a) = p^r$, for some $r \in \{1, \ldots, n\}$, 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. □

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

Proof. Follows from the definition. □

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 $P = P_0 \leq P_1 \leq \cdots$, the subset $P := \bigcup\limits_{n\geq 0} P_n$ is a p-subgroup of G (verify!), and hence is an element of $\mathcal{P}$. Then by Zorne's lemma $\mathcal{P}$ has a maximal element, say $P_{\max} \in \mathcal{P}$. This completes the proof. □

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 $Z(G) \neq \{e\}$. □

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 4.2.5. 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. □

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 $|X| \equiv |X_0|$ (mod 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 $[G : G_x] = |\mathrm{Orb}_G(x)| > 1$, 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 $|X_0| \neq 0$ (mod p), and hence the second part follows. □

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

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

Note that σ 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. □

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 4.2.3). 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 $d := \mathrm{lcm}(m, n)$.

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 $d := \mathrm{lcm}(m, n)$ 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, $|Z(G)| = p$. □

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 4.2.4 we have $a^n = e$, $\forall\, a \in K$, and hence $K \subseteq H$. Since $|K| = n$, by Lagrange's theorem we have $n \mid |H|$. □

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. □

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 2.2.3 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 π is odd, then we replace π 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 σ, they commutes, 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 $I_n := \{1, \ldots, n\}$. If $r = 2$, then σ must be a transposition, which is not possible since then σ would be odd while $H \subseteq A_n$. Therefore, $r \geq 3$. If we can show that $r = 3$, then σ must be a 3-cycle and we are done.

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

Step 1: Suppose that σ_j is a transposition, for all $j \in \{1, \ldots, k\}$. 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 σ_1 and σ_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 τ 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 σ 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 σ, which is a contradiction. Therefore, at least one σ_i must be a cycle of length ≥ 3. Since disjoint cycles commutes, we may assume that $\sigma_1 = (a\ \ b\ \ c\ \ \cdots)$ is a cycle of length ≥ 3.

Step 2: If $r = 4$, then either σ 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 σ, 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 σ, which is a contradiction. Therefore, we must have $r = 3$, and hence σ 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 $\bigcap\limits_{N \in \mathcal{N}} N$ 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 $D_8 = \langle\, r, s : \mathrm{ord}(r) = 4, \mathrm{ord}(s) = 2, sr = r^{-1}s\rangle$, and identify the associated quotient groups.

Q7. Fix an integer $n \geq 3$, and let $D_{2n} = \langle\, r, s : \mathrm{ord}(r) = n, \mathrm{ord}(s) = 2, sr = r^{-1}s\rangle$ be the dihedral group of degree n and order $2n$.

(i) Show that

$$Z(D_{2n}) = \begin{cases} \{e\}, & \text{if } n \text{ is odd, and} \\ \{e, r^k\}, & \text{if } n = 2k \text{ is even.} \end{cases}$$

(ii) 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 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 $\operatorname{lcm}(m, n) \leq [G : H \cap K] \leq mn$. 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 $f : \mathbb{Z} \to G$ 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 $\varphi : \mathbb{Z}_n \to G$ such that $\varphi([1]) = a$.

Q26. Fix an integer $n \geq 2$. Given an integer k, let $f_k : \mathbb{Z}_n \to \mathbb{Z}_n$ 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 $f_k \in \mathrm{Aut}(\mathbb{Z}_n)$ 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 $f : \mathbb{Z}_n^\times \to \mathrm{Aut}(\mathbb{Z}_n)$ 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 $\mathrm{Aut}(\mathbb{Z}_n)$.

(vii) Conclude that $\mathrm{Aut}(\mathbb{Z}_n)$ is an abelian group of order $\phi(n)$, where ϕ 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 $f : G \to G$ 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 $f : \mathbb{Z}_m \to \mathbb{Z}_n$.

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 $F_p : G \to G$ given by $z \mapsto z^p$, is a surjective group homomorphism.

(iii) Find $\operatorname{Ker}(F_p)$.

(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 $\pi : G \to S(G)$ be the *left regular representation of* G (i.e., π 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 $\operatorname{ord}(a) = n$ 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 $\operatorname{ord}(a)$ is even and $|G|/\operatorname{ord}(a)$ 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 $f \in \operatorname{Aut}(G)$. 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 $G \to S_3$). 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 $\mathrm{Hom}(G, H)$ the set of all group homomorphisms from G into H.

(i) Find the number of elements of the set $\mathrm{Hom}(\mathbb{Z} \times \mathbb{Z}, \mathbb{Z}_n)$, for all $n \in \mathbb{N}$.

(ii) Let G be an abelian groups of order n. Let $r \in \mathbb{N}$. Are the sets $\mathrm{Hom}(\mathbb{Z}^{\oplus r}, \mathbb{Z}_n)$ and $\mathrm{Hom}(\mathbb{Z}^{\oplus r}, G)$ 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

$$\mathrm{Hom}(G, H) \times \mathrm{Hom}(G, K) \longrightarrow \mathrm{Hom}(G, H \times K).$$

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 $|N_{S_p}(P)| = p(p-1)$.