Contents

Chapter 1

Groups

1.1 Introduction

The fundamental notions of set, mapping, binary operation, and binary relation are essential for the study of an algebraic system. An algebraic structure or algebraic system, is a nonempty set in which at least one equivalence relation (equality) and one or more binary operations are defined. The simplest structures occur when there is only one binary operation, as in the case with the algebraic system known as group. The concept of a group is of fundamental importance in the study of algebra. Ideally the goal in studying groups is to classify all groups up to isomorphism, which in practice means finding necessary and sufficient conditions for two groups to be isomorphic.

1.2 Semigroups, Monoids and Groups

Let G be a nonempty set. A *binary operation* on G is a function $G \times G \longrightarrow G$. There are several commonly used notations for the image of (a, b) under a binary operation:

- *multiplicative notation:* ab
- *additive notation:* $a + b$
- $a \cdot b$, $a * b$ etc.

For convenience we shall generally use the multiplicative notation throughout this chapter and refer to ab as the *product* of a and b.

Definition 1.2.1.

i) A *semigroup* is a nonempty set G together with a binary operation on G which is
   - associative: $a(bc) = (ab)c$ for all $a, b \in G$;

ii) a *monoid* is a semigroup G which contains a
   - two sided identity element $e \in G$ such that $ae = ea = a$ for all $a \in G$.

iii) A *group* is a monoid G such that

- for every $a \in G$ there exists a two sided inverse element $a^{-1} \in G$ such that $a^{-1}a = aa^{-1} = e$.

iv) A semigroup G is said to be *abelian* or *commutative* if its binary operation is commutative, that is, $ab = ba$ for all $a, b \in G$.

Example 1.2.2.

1. Let G be the set of complex numbers given by $G = \{1, i, -1, -i\}$, where $i = \sqrt{-1}$, and consider the operation of multiplication of complex numbers in G, see Table 1.1.

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Table 1.1

In this table, we see that:

- G is closed w.r.t. multiplication.
- Multiplication in G is associative, since multiplication has these properties in the set of all complex numbers.
- 1 is the identity element, and that all elements have inverses. Thus, $(G, \cdot)$ is a group by definition.

2. It is easy to verify that each of the following set is a group:
   (i) $(\mathbb{Z}_n, +)$ where $\mathbb{Z}_n = \{\overline{0}, \ldots, \overline{n-1}\}$ is the set of congruence modulo n.
   (ii) $G = \{a, b, c, d\}$ where $(G, \cdot)$ is defined as in Table 1.2.

Definition 1.2.3. Let G be a group.

- The *order* of the group G is the cardinal number $|G|$.
- G is said to be *finite (resp. infinite)* if $|G|$ is finite (resp. infinite).

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Table 1.2

Theorem 1.2.4. *If G is a monoid, then the identity element e is unique. If G is a group, then*

(i) *$c \in G$ and $cc = c \Rightarrow c = e$;*

(ii) *for all $a, b, c \in G$ $ab = ac \Rightarrow b = c$ and $ba = ca \Rightarrow b = c$ (left and right cancellation);*

(iii) *for each $a \in G$, the inverse element a^{-1} is unique;*

(iv) *for each $a \in G$, $(a^{-1})^{-1} = a$;*

(v) *for $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$;*

(vi) *for $a, b \in G$, the equations $ax = b$ and $ya = b$ have unique solutions in G: $x = a^{-1}b$ and $y = ba^{-1}$.*

Proof. (i) If $e' \in G$ is also a two-sided identity, then $e = ee' = e'$.

$$\begin{aligned} cc = c &\Rightarrow c^{-1}(cc) = c^{-1}c \\ &\Rightarrow (c^{-1}c)c = c^{-1}c \\ &\Rightarrow ec = e \\ &\Rightarrow c = e. \end{aligned}$$

(ii)

$$\begin{aligned} ab = ac &\Rightarrow a^{-1}(ab) = a^{-1}(ac) \\ &\Rightarrow (a^{-1}a)b = (a^{-1}a)c \\ &\Rightarrow eb = ec \\ &\Rightarrow b = c \end{aligned}$$

Similarly, $ba = ca \Rightarrow b = c$.

(iii) Let $b \in G$ be an inverse of $a \in G$. Then $ba = e = a^{-1}a$ which implies $b = a^{-1}$ by part (ii).

(iv)

$$\begin{aligned}\left(a^{-1}\right)^{-1} &= \left(a^{-1}\right)^{-1} e \\ &= \left(a^{-1}\right)^{-1} \left(a^{-1}a\right) \\ &= \left(\left(a^{-1}\right)^{-1} a^{-1}\right) a \\ &= ea \\ &= a.\end{aligned}$$

(v)

$$\begin{aligned}(ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1} \\ &= e \\ &= (ab)(ab)^{-1} \\ &\Rightarrow (ab)^{-1} = b^{-1}a^{-1} \text{ by part (ii).}\end{aligned}$$

(vi) Since $a(a^{-1}b) = (aa^{-1})b = eb = b$ and $(ba^{-1})a = b(a^{-1}a) = be = b$, $x = a^{-1}b$ and $y = ba^{-1}$ are solutions of $ax = b$ and $ya = b$. Uniqueness (Exercise!)

□

Proposition 1.2.5. *Let G be a semigroup. Then G is a group if and only if the following conditions hold:*

i) *there exists an element $e \in G$ such that $ea = a$ for all $a \in G$ (left identity element)*

ii) *for each $a \in G$, there exists an element $a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse)*

Proof. ($\Rightarrow$) If G is a group, then by Definition 1.2.1 both conditions *i)* and *ii)* hold.

($\Leftarrow$) We show that e (resp. a^{-1}) is a right identity (resp. inverse). To see this, if $a \in G$, then by part *ii)*

$$\begin{aligned}\left(aa^{-1}\right)\left(aa^{-1}\right) &= a\left(aa^{-1}\right)a^{-1} \\ &= a\left(ea^{-1}\right) = aa^{-1} \\ &\Rightarrow aa^{-1} = e \text{ by Theorem 1.2.4 } (i) \text{ which implies } a^{-1}\end{aligned}$$

is a right inverse.

Moreover, since $ae = a\left(a^{-1}a\right) = \left(aa^{-1}\right)a = ea = a$ for all $a \in G$, e is a right identity. Thus, G is a group by Definition 1.2.1. □

Remark 1.2.6. An analogous result holds for "right inverse" and "right identity".

Proposition 1.2.7. *A semigroup G is a group if and only if, for any elements a and b in G, the equations $ax = b$ and $ya = b$ have solutions in G.*

Proof. ($\Rightarrow$) If G is a group, then we have $a^{-1}b$ and ba^{-1} are elements of G such that

$$a\left(a^{-1}b\right) = \left(aa^{-1}\right)b = eb = b,$$

$$\left(ba^{-1}\right)a = b\left(a^{-1}a\right) = be = b.$$

Thus the equations $ax = b$ and $ya = b$ have solutions in G.

($\Leftarrow$) Suppose that these equations have solutions in G. Let a be an arbitrary element in G. Then, there exists $e \in G$ such that $ae = a$ since $ax = a$ is solvable in G. For all elements $b \in G$, we show that $be = b$. To show this, let $b \in G$. Then, choose an element $g \in G$ such that $ga = b$ since $ya = b$ is solvable in G. Now, $be = (ga)e = ga = b$ which implies e is a right identity in G. Also, since $ax = e$ is solvable in G, we have, for each $a \in G$, an element $a' \in G$ such that $aa' = e$. By Proposition 1.2.5, G is a group. □

Example 1.2.8.

- $(\mathbb{Z}, +), (\mathbb{Q}, +)$ and $(\mathbb{R}, +)$ are infinite abelian groups.
- $(\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot)$ and $(\mathbb{R}, \cdot)$ are monoids.
- $(2\mathbb{Z}, \cdot)$ is a semigroup.

Example 1.2.9. Consider the square with vertices consecutively numbered 1,2,3,4 center at the origin of the x-y plane, and sides parallel to the axes. Let

$$D_4^* = \{R, R^2, R^3, I, T_x, T_y, T_{1,3}, T_{2,4}\}$$

be the set of transformations of the square where

R is a counterclockwise rotation about the center of 90°,
R^2 is a counterclockwise rotation of 180°,
R^3 is a counterclockwise rotation of 270°,
I is a rotation of 360° = 0°,
T_x is a reflection about the diagonal through vertices 1 and 3, and
T_y is a reflection about the diagonal through vertices 2 and 4

Note that each $U \in D_4^*$ is a bijection of the square onto itself. Define the binary operation in D_4^* to be the composition of functions: for $U, V \in D_4^*, U \circ V$ is the transformation V followed by the transformation U. D_4^* is a nonabelian group of order 8 called the *group of symmetries of the square.*

Theorem 1.2.10. *Let $R(\sim)$ be an equivalence relation on a monoid G such that $a_1 \sim a_2$ and $b_1 \sim b_2$ implies $a_1 b_1 \sim a_2 b_2$ for all $a_i, b_i \in G$. Then the set G/R of all equivalence classes of G under R is a monoid under the binary operation defined by $\overline{a}\,\overline{b} = \overline{ab}$, where $\overline{x}$ denotes the equivalence class of $x \in G$. If G is an abelian group, then so is G/R.*

Proof. If $\overline{a_1} = \overline{a_2}$ and $\overline{b_1} = \overline{b_2}$ $(a_i, b_i \in G)$, then $a_1 \sim a_2$ and $b_1 \sim b_2$ by definition of equivalence relation. This implies $a_1 b_1 \sim a_2 b_2$ by hypothesis which also implies $\overline{a_1 b_1} = \overline{a_2 b_2}$ by definition of equivalence relation. Therefore, the binary operation in G/R is well-defined, that is, independent of the choice of equivalent class representatives.

Associativity:

$$\overline{a}\left(\overline{b}\overline{c}\right) = \overline{a}\left(\overline{bc}\right) = \overline{a(bc)} = \overline{(ab)c} = \left(\overline{ab}\right)\overline{c} = \left(\overline{a}\overline{b}\right)\overline{c}.$$

Identity element:

$$\overline{a}\,\overline{e} = \overline{ae} = \overline{a} = \overline{ea} = \overline{e}\,\overline{a}$$

Therefore, G/R is a monoid. Finally, if G is an abelian group, clearly G/R is also an abelian group. □

Remark 1.2.11. If p is prime, then $(\mathbb{Z}_p \setminus \{p\}, \cdot)$ is a group of order $p - 1$.

Definition 1.2.12. Given any sequence of elements of a semigroup G, $\{a_1, a_2 \ldots\}$ define inductively a meaningful product of $a_1, a_2, \ldots$ (in this order) as follows:

- If $n = 1$, the only meaningful product is a_1.
- If $n > 1$, then a meaningful product is defined to be any product of the form $(a_1, \ldots, a_m)(a_{m+1}, \ldots, a_n)$ where $m < n$ and $(a_1, \ldots, a_m)$ and $(a_{m+1}, \ldots, a_n)$ are meaningful products of m and $n - m$ elements respectively.

Theorem 1.2.13 (Generalized Associative Law)**.** *If G is a semigroup and $a_1, \ldots, a_n \in G$, then any two meaningful products of $a_1, \ldots, a_n$ in this order are equal.*

Corollary 1.2.14 (Generalized Commutative Law)**.** *If G is a commutative semigroup and $a_1, \ldots, a_n \in G$, then for any permutation $i_1, \ldots, i_n$ of $1, 2, \ldots, n$, $a_{i_1} \cdots a_{i_n} = a_1 \cdots a_n$ in this order are equal.*

Definition 1.2.15. Let G be a semigroup, $a \in G$ and $n \in \mathbb{N}^*$. The element $a^n \in G$ is defined to be the standard n product $\prod_{i=1}^{n} a_i$ with $a_i = a$ for $1 \leq i \leq n$. If G is a monoid, a^0 is defined to be the identity element e. If G is a group, then for each $n \in \mathbb{N}^*$, a^{-n} is defined to be $(a^{-1})^n \in G$.

1.3 Homomorphisms and Subgroups

Definition 1.3.1. Let G and H be semigroups. A function $f : G \to H$ is a homomorphism provided

$$f(ab) = f(a)f(b)$$

for all $a, b \in G$. Moreover, if

(1) f is injective as a map of sets, it is called a *monomorphism.*

(2) f is surjective, then it is called an *epimorphism.*

(3) f is bijective, then it is called an *isomorphism.* In this case, G and H are said to be isomorphic (written $G \cong H$).

(4) A homomorphism $f : G \to G$ is called an *endomorphism* of G.

(5) An isomorphism $f : G \to G$ is called an *automorphism* of G.

Remark 1.3.2. Let $f : G \to H$ is a homomorphism of groups. Then

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

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

Proof. $e_G e_G = e_G \Rightarrow f(e_G e_G) = f(e_G)e_H \Rightarrow f(e_G)f(e_G) = f(e_G)e_H \Rightarrow f(e_G) = e_H$ by left cancellation law.

$f(a)f(a^{-1}) = f(aa^{-1}) = f(e_G) = e_H = f(a)f(a)^{-1} \Rightarrow f(a^{-1}) = f(a)^{-1}$ by left cancellation. □

Example 1.3.3.

(a) The map $f : \mathbb{Z} \to \mathbb{Z}_m$ defined by $f(x) = \overline{x}$ is an epimorphism of additive groups.

(b) Let $1 < m, k \in \mathbb{N}^*$. The map $g : \mathbb{Z}_m \to \mathbb{Z}_{mk}$ defined by $f(\overline{x}) = \overline{kx}$ is a monomorphism.

(c) Let $G = \{A \in \mathbb{R}^{2\times 2} \mid det(A) \neq 0\}$ and $H = \mathbb{R}^*$. Define a map $f : G \to H$ by $f(A) = \det(A)$. Show that f is a group homomorphism.

Definition 1.3.4. Let $f : G \to H$ be a homomorphism of groups.

(i) The *kernel* of f (denoted by Kerf) is $\{a \in G \mid f(a) = e_H\}$.

(ii) If A is a subset of G, then

$$f(A) = \{b \in H \mid b = f(a) \text{ for some } a \in A\}$$

is the image of A. $f(G)$ is called the *image* of f and denoted by Imf.

(iii) If B is a subset of H,

$$f^{-1}(B) = \{a \in G \mid f(a) \in B\}$$

is the inverse image of B.

Theorem 1.3.5. *Let $f : G \to H$ be a homomorphism of groups. Then*

i) f is a monomorphism iff $Kerf = \{e_G\}$.

ii) f is an isomorphism iff there is a homomorphism $f^{-1} : H \to G$ such that $ff^{-1} = 1_H$ and $f^{-1}f = 1_G$.

Proof. i) Let $a \in \text{Ker}f$. Then $f(a) = e_H = f(e_G)$. Since f is monomorphism, $a = e_G$. Suppose $f(a) = f(b)$. Then $f(ab^{-1}) = e_H$ which implies $ab^{-1} \in \text{Ker}f = \{e_G\}$. Thus, $a = b$ and, hence, f is a monomorphism.

ii) By given, there is a map of sets $f^{-1} : H \to G$ such that $f^{-1}f = 1_G$ and $ff^{-1} = 1_H$. Let $a, b \in H$. Since f is an isomorphism, there exists $a', b' \in G$ such that $f(a') = a$ and $f(b') = b$. Now $f^{-1}(ab) = f^{-1}(f(a')f(b')) = f^{-1}(f(a'b')) = f^{-1}f(a'b') = a'b' = f^{-1}(a)f^{-1}(b)$. Thus, f^{-1} is a homomorphism of groups. The converse is obvious. □

Definition 1.3.6. Let G be a group and H a nonempty subset that is closed under the product in G. If H is itself a group under the product in G, then H is said to be a subgroup of G. This is denoted by $H < G$.

Example 1.3.7. Let G be a group. Then $G < G$ and $\{e_G\} < G$.

Let H be a subgroup of a group G such that $H \neq G$ and $H \neq \{e_G\}$. Then H is called a proper subgroup of G.

a) $n\mathbb{Z} < \mathbb{Z}$ for some fixed integer n.

b) $\{0, 3\}$ and $\{0, 2, 4\} < \mathbb{Z}_6$ under addition.

c) Let $f : G \to H$ be a group homomorphism. Then
   - $\mathrm{Ker} f < G$.
   - Let A be a subset of G. $A < G \Rightarrow f(A) < H$; in particular, $\mathrm{Im} f < H$.
   - Let B be a subset of H. $B < H \Rightarrow f^{-1}(B) < G$.

Theorem 1.3.8. *Let H be a nonempty subset of a group G. Then H is a subgroup of G iff $ab^{-1} \in H$ for all $a, b \in H$.*

Proof. ($\Leftarrow$) There exists $a \in H$ and hence $aa^{-1} \in H$. Thus for any $b \in H$, $b^{-1} = eb^{-1} \in H$. If $a, b \in H$, then $b^{-1} \in H$ and hence $ab = a(b^{-1})^{-1} \in H$ which implies H is closed. The product in H is associative since G is a group. Thus, $H < G$. The other direction is clear. □

Corollary 1.3.9. *If G is a group and $\{H_i \mid i \in I\}$ is a nonempty family of subgroups, then $\cap_{i \in I} H_i$ is a subgroup of G.*

Definition 1.3.10. Let G be a group and X a subset of G. Let $\{H_i \mid i \in I\}$ is a nonempty family of subgroups of G which contain X. Then $\cap_{i \in I} H_i$ is called the subgroup of G generated by the set X and denoted $\langle X \rangle$.

The elements of X are the generators of the subgroup $\langle X \rangle$, which may also be generated other subsets (that is, we may have $\langle X \rangle = \langle Y \rangle$ with $X \neq Y$). If $X = \{a_1, \ldots, a_n\}$, we write $\langle a_1, \ldots, a_n \rangle$ in place of $\langle X \rangle$.

Definition 1.3.11. If $G = \langle a_1, \ldots, a_n \rangle$, $(a_i \in G)$, G is said to be finitely generated. If $a \in G$, the subgroup $\langle a \rangle$ is called the *cyclic subgroup* generated by a.

Example 1.3.12.

i) $(\mathbb{Z}, +)$ is an infinite cyclic group with generator 1 since by additive notation, $m \cdot 1 = m$ for all $m \in \mathbb{Z}$.

ii) The trivial subgroup $\langle e \rangle$ of any group is cyclic.

iii) the multiplicative subgroup $\langle i \rangle$ in $\mathbb{C}$ is cyclic of order 4.

iv) for each m the additive group $\mathbb{Z}_m$ is cyclic of order m with generator $1 \in \mathbb{Z}_m$.

Theorem 1.3.13. *If G is a group and X is a nonempty subset of G, then the subgroup $\langle X \rangle$ generated by X consists of all finite products $a_1^{n_1} \cdots a_t^{n_t}$ ($a_i \in X$ and $n_i \in \mathbb{Z}$). In particular, for every $a \in G$, $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.*

If $\{H_i \mid i \in I\}$ is a family of subgroups of a group G, then $\cup_{i\in I} H_i$ is not a subgroup of G in general. The subgroup $\langle \cup_{i\in I} H_i \rangle$ generated by the set $\cup_{i\in I} H_i$ is called the subgroup generated by the groups $\{H_i \mid i \in I\}$. If H and K are subgroups, the subgroup $\langle H \cup K \rangle$ generated by H and K is called the join of H and K and is denoted by $H \vee K$ (additive notation: $H + K$).

1.4 Cyclic Groups

The structure of cyclic groups is relatively simple. We shall completely characterize all cyclic groups (up to isomorphism).

Theorem 1.4.1. *Every subgroup H of the additive group Z is cyclic. Either $H = \langle 0 \rangle$ or $H = \langle m \rangle$, where m is the least positive integer in H. If $H \neq \langle 0 \rangle$, then H is infinite.*

Proof. If $H = \langle 0 \rangle$, then clearly H is cyclic. $H \neq \langle 0 \rangle$ implies $\langle m \rangle = \{km \mid k \in \mathbb{Z}\}$. Since $m \in H$, we have $\langle m \rangle \subset H$. Conversely, if $h \in H$, then $h = mq + r$ with $q, r \in \mathbb{Z}$ such that $0 \leq r < m$ (Division algorithm). Since $r = h - mq \in H$, the minimality of m implies $r = 0$ and, hence, $h = mq \in \langle m \rangle$ which implies $H \subset \langle m \rangle$.

If $H \neq \{0\}$, then it is clear that $H = \langle m \rangle$ is infinite. □

Theorem 1.4.2. *Every infinite cyclic group is isomorphic to the additive group $\mathbb{Z}$ and every finite cyclic group of order m is isomorphic to the additive group $\mathbb{Z}_m$.*

Proof. If $G = \langle a \rangle$ is a cyclic group, then the map

$$\alpha : \mathbb{Z} \to G, k \mapsto a^k$$

is an epimorphism. If $\mathrm{Ker}\alpha = 0$, then $\mathbb{Z} \cong G$ by Theorem 1.3.5. Otherwise $\mathrm{Ker}\alpha$ is a nontrivial subgroup of $\mathbb{Z}$ and hence $\mathrm{Ker}\alpha = \langle m \rangle$ where m is the least positive integer such that $a^m = e$. Now for all $r, s \in \mathbb{Z}$,

$$\begin{aligned} a^r = a^s \Leftrightarrow a^{r-s} = e \Leftrightarrow r - s \in \mathrm{Ker}\,\alpha = \langle m \rangle \\ \Leftrightarrow m|(r-s) \Leftrightarrow \overline{r} = \overline{s} \text{ in } \mathbb{Z}_m \end{aligned}$$

where $\overline{k}$ is the congruence class of $k \in \mathbb{Z}$.

Therefore, the map $\beta : \mathbb{Z}_m \to G, \overline{k} \mapsto a^k$ is a well-defined epimorphism. Since $\beta(\overline{k}) = e \Leftrightarrow a^k = e \Leftrightarrow \overline{k} = \overline{0}$ in $\mathbb{Z}_m$ which implies β is a monomorphism. □

Definition 1.4.3. Let G be a group and $a \in G$. The order of a is the order of the cyclic subgroup $\langle a \rangle$ and is denoted by $|a|$.

Theorem 1.4.4. *Let G be a group and $a \in G$. If a has infinite order, then*

i) $a^k = e \Leftrightarrow k = 0$.

ii) *the elements* a^k $(k \in \mathbb{Z})$ *are all distinct.*

If a *has a finite order* $m > 0$, *then*

iii) m *is the least positive integer such that* $a^m = e$.

iv) $a^k = e \Leftrightarrow m|k$.

v) $a^r = a^s \Leftrightarrow r \equiv s \bmod m$.

vi) $\langle a \rangle$ *consists of the distinct elements* $a, a^2, \ldots, a^{m-1}, a^m = e$.

vii) *for each* k *such that* $k|m$, $|a^k| = \frac{m}{k}$.

Proof. Let $H = \langle a \rangle < G$. Consider the map

$$\alpha : \mathbb{Z} \to H, k \mapsto a^k.$$

i) Since $|H| = \infty$, then $\mathrm{Ker}\alpha = \{0\}$ by Theorem 1.4.2. Thus $a^k = e \Rightarrow k \in \mathrm{Ker}\,\alpha = \{0\} \Rightarrow k = 0$. If $k = 0$, then $a^k = e$.

ii) if $a^k = a^m$ for some $k, m \in \mathbb{Z}$, $a^{k-m} = e \Rightarrow k - m = 0$ by (i).

iii) Since $|H| < \infty$, $\mathrm{Ker}\alpha = \langle m \rangle$ where m is the least positive integer such that $a^m = e$ by Theorem 1.4.2.

iv) Given $a^m = e$. If $a^k = e$, then

$$\begin{aligned} a^k = a^m \Leftrightarrow a^{k-m} = e \Leftrightarrow k - m \in \mathrm{Ker}\,\alpha = \langle m \rangle \\ \Leftrightarrow m|(k-m) \Leftrightarrow m|k. \end{aligned}$$

Conversely, if $m|k$, then $k = mq$ for some $q \in \mathbb{Z}$. Then

$$a^k = a^{mq} = (a^m)^q = e^q = e.$$

v) $a^r = a^s \Leftrightarrow a^{r-s} = e \Leftrightarrow m|(r-s)$ by (iv). Thus $a^r = a^s \Leftrightarrow r \equiv s \bmod m$.

vi)

$$\begin{aligned} \langle a \rangle &= \{a^k \mid k \text{ is an integer } \} \text{ but } k = mq + r \text{ with } 0 \leq r < m \\ &= \{a^r \mid 0 \leq r < m\} \\ &= \{a, a^2, \ldots, a^{m-1}, a^m = e\}. \end{aligned}$$

viii) $\left(a^k\right)^{\frac{m}{k}} = a^m = e$ and $(a^k)^r \neq e$ for all $0 < r < \frac{m}{k}$. Since otherwise $a^{kr} = e$ with $kr < k(\frac{m}{k}) = m$ contradicting (iii). Therefore, $|a^k| = \frac{m}{k}$.

□

Theorem 1.4.5. *Every homomorphic image and every subgroup of a cyclic group G is cyclic. In particular, if H is a non trivial subgroup of $G = \langle a \rangle$ and m is the least positive integer such that $a^m \in H$, then $H = \langle a^m \rangle$.*

Proof. Let $f : G \to K$ be homomorphism of groups. Then

$$\begin{aligned} \text{Im}f &= \{k \in K \mid f(g) = k \text{ for some } g \in G = \langle a \rangle\} \\ &= \{k \in K \mid f(a^n) = k \text{ for some integer } n\} \\ &= \{k \in K \mid f(a)^n = k \text{ and since } f \text{ is a group hsm}\} \\ &= \{f(a)^n \mid n \text{ is an integer}\} \\ &= \langle f(a) \rangle. \end{aligned}$$

Since $a^m \in H, \langle a^m \rangle \subset H$. Conversely, $h \in H \Rightarrow h \in G$ and, hence, $h = a^n \in H$ for some integer n. By Division algorithm, there exist integers q and r such that $n = mq + r$ with $0 \leq r < m$. Now,

$$a^n = a^{mq}a^r \Rightarrow a^r = a^{n-mq} \in H \Rightarrow r = 0$$

by the minimality of m. Thus $h = a^n = a^{mq} = (a^m)^q \in \langle a^m \rangle$. Hence, $H = \langle a^m \rangle$. □

Note that two distinct elements in a group may generate the same cyclic subgroup.

Theorem 1.4.6. *Let $G = \langle a \rangle$ be a cyclic group. If G is infinite, then a and a^{-1} are the only generators of G.*

Proof. Given that $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. Since G is infinite, $a^n \neq a^m$ for all $m \neq n \in \mathbb{Z}$ by Theorem 1.4.4(ii). In particular, $a \neq a^{-1}$. Thus

$$G = \langle a \rangle = \langle a^{-1} \rangle = \left\{ \left(a^{-1}\right)^{-n} \,\middle|\, -n \in \mathbb{Z} \right\}.$$

Are they the only generators? Suppose that b is any generators of G. Then $\langle b \rangle = \langle a \rangle$ and hence $a = b^n$ and $b = a^m$ for some m and n in $\mathbb{Z}$. Since $a = b^n = (a^m)^n = a^{mn} \Rightarrow mn = 1$. Since $m, n \in \mathbb{Z}$, we must have $m = n = 1$ or $m = n = -1$. Thus $b = a$ or $b = a^{-1}$. □

Theorem 1.4.7. *Let G be a group and $a \in G$ such that $|a| = m < \infty$. Then for any $0 \leq r < m$,*

$$|a^r| = \frac{m}{(m, r)}$$

where (m, r) is the gcd of m and r.

Proof. Let $0 \leq r < m$ be fixed and $d = (m, r)$. Then there exists integers s and t such that $d = sm + tr$. Set $b := a^r$. Since d divides both m and r, $\frac{m}{d}$ and $\frac{m}{r}$ are coprime. Now

$$b^{\frac{m}{d}} = (a^r)^{\frac{m}{d}} = a^{\frac{rm}{d}} = (a^m)^{\frac{r}{d}} = e.$$

On the other hand, for any integer q,

$$\begin{aligned} b^q = e &\Rightarrow (a^r)^q = e \Rightarrow a^{rq} = e \Rightarrow |a| \text{ divides } rq \text{ by Theorem 1.4.4(iv)} \\ &\Rightarrow m|rq \Rightarrow \frac{m}{d}\Big|\frac{r}{d}q \\ &\Rightarrow \frac{m}{d}\Big|q \text{ since } \left(\frac{m}{d}, \frac{r}{d}\right) = 1. \end{aligned}$$

Therefore, $\frac{m}{d}$ is the least positive integer k such that $b^k = e$. Thus $|a^r| = |b| = \frac{m}{d} = \frac{m}{(m,r)}$. □

Let $d \in \mathbb{Z}_+$ such that $d|m$. Then $|a^d| = \frac{m}{(m,d)} = \frac{m}{d}$.

Theorem 1.4.8. *Let G be a finite cyclic group of order m and $a \in G$ such that $G = \langle a \rangle$. For any a^r is a generator of G if and only if $(r, m) = 1$.*

Proof. Let $1 \leq k < m$. Then by Theorem 1.4.7, a^k is a generator of G if and only if

$$m = |a^r| = \frac{m}{(m, r)} \Leftrightarrow (m, r) = 1.$$

□

Example 1.4.9.

1) $(\mathbb{Z}, +)$ is a cyclic group with 1 and -1 as the only generators.

2) $(\mathbb{Z}_n, +_n)$ is a finite cyclic group with $\phi(n)$ generators where $\phi(n) = |\{m < n \mid (m, n) = 1\}|$. Here ϕ is a function $\phi : \mathbb{Z}_+ \to \mathbb{Z}_+$, called the Euler-Totient function.

3) There are exactly two generators in each of the groups $(\mathbb{Z}_3, +_3), (\mathbb{Z}_4, +_4)$ and $(\mathbb{Z}_6, +_6)$ since $\phi(3) = \phi(4) = \phi(6) = 2$.

4) Compute the order of 16 in $(\mathbb{Z}_{24}, +_{24})$. **Solution:** $\mathbb{Z}_{24} = \langle 1 \rangle$ and $|1| = 24$ in $\mathbb{Z}_{24}$. But
$$|16| = \frac{24}{(16, 24)} = \frac{24}{8} = 3$$
by Theorem 1.4.7.

5 Determine all the generators of $36\mathbb{Z} + 24\mathbb{Z}$. The $36\mathbb{Z} + 24\mathbb{Z} = 12\mathbb{Z}$ (see Exercise 1.4.10 2) below) is an infinite cyclic group generated by 12. Thus 12 and -12 are the only generators of $36\mathbb{Z} + 24\mathbb{Z}$.

Exercise 1.4.10.

1) Let p be a prime number. Determine the number of generators of the group $G = (\mathbb{Z}_p, +_p)$.

2) For any positive integers a and b, prove that (left as an exercise)

$$a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b)\mathbb{Z} \text{ and } a\mathbb{Z} \cap b\mathbb{Z} = \operatorname{lcm}(a, b)\mathbb{Z}.$$

For the following section we need the following definition:

Definition 1.4.11. Let A be a non-empty set. A relation R on $A \times A$ is an *equivalence relation* on A provided R is:

$$\textbf{reflexive: } (a, a) \in R \text{ for all } a \in A; \tag{1.1}$$

$$\textbf{symmetric: } (a, b) \in R \Rightarrow (b, a) \in R; \tag{1.2}$$

$$\textbf{symmetric: } (a, b) \in R \text{ and } (b, c) \in R \Rightarrow (a, c) \in R\,. \tag{1.3}$$

If R is an equivalence relation on A and $(a, b) \in R$, we say that a is equivalent to b under R and write $a \sim b$ or aRb. For instance, instead of writing $(a, b) \in R$ we write as $a \sim b$.

Definition 1.4.12. Let $R(\sim)$ be an equivalence relation on A. If $a \in A$, the *equivalence class* of a (denoted $\overline{a}$) is the class of all those elements of A that are equivalent to a, that is, $\overline{a} = \{b \in A \mid b \sim a\}$. The class of all equivalence equivalence classes is denoted by A/R and called the *quotient class* of A by R.

and, hence, we have the following remark:

Remark 1.4.13. Let $R(\sim)$ be an equivalence relation on A. Then

(i) $\overline{a} \neq \emptyset$ for every $a \in A$;

(ii) if A is a set, $\cup_{a \in A} \overline{a} = A = \cup_{\overline{a} \in A/R} \overline{a}$;

(iii) $\overline{a} = \overline{b} \Leftrightarrow a \sim b$, and

(iv) For $a, b \in A$, either $\overline{a} \cap \overline{b} = \emptyset$ or $\overline{a} = \overline{b}$.

Proof. (i) and (ii) Since R is reflexive, $a \in \overline{a}$ for every $a \in A$, $\overline{a} \neq \emptyset$ and, hence, (ii) holds. (iii) For if $\overline{a} = \overline{b}$, then $a \in \overline{a} \Rightarrow a \in \overline{b} \Rightarrow a \sim b$. Conversely, if $a \sim b$ and $c \in \overline{a}$, then $c \sim a$ and $a \sim b \Rightarrow c \sim b \Rightarrow c \in \overline{b}$; a symmetric argument shows that $\overline{b} \subseteq \overline{a}$ and therefore $\overline{a} = \overline{b}$. (iii) is clear. (iv) If $\overline{a} \cap \overline{b} \neq \emptyset$, then there is an element $c \in \overline{a} \cap \overline{b}$. Hence, by definition $a \sim c$ and $c \sim b$ which implies $a \sim b$ and, hence, $\overline{a} = \overline{b}$ by the fact in (ii). □

1.5 Cosets and Counting

In this section, we discuss the notion of *cosets*. This section introduces us the first significant theorems relating the structure of a finite group G with the number theoretic properties of its order $|G|$. To begin with, let us extend the concept of congruence modulo m in the group $\mathbb{Z}$. Before introducing this, we recall the reader the concept of congruence modulo m in the group $\mathbb{Z}$ in the following remark:

Remark 1.5.1.

$$\begin{aligned} a \equiv b \bmod m &\Leftrightarrow m \mid a - b \\ &\Leftrightarrow a - b = mq \in \langle m \rangle = \{mk \mid k \in \mathbb{Z}\}. \end{aligned}$$

In the following definition, we extend the concept of congruence modulo m in the group $\mathbb{Z}$.

Definition 1.5.2. Let H be a subgroup of a group G and $a, b \in G$.

a) a is a right congruent to b modulo H, denoted $a \equiv_r b \bmod H$ if $ab^{-1} \in H$.

b) a is a left congruent to b modulo H, denoted $a \equiv_l b \bmod H$ if $a^{-1}b \in H$.

Remark 1.5.3.

- If G is abelian, then right and left congruence modulo H coincide (since $ab^{-1} \in H \Leftrightarrow (ab^{-1})^{-1} \in H$ and $(ab^{-1})^{-1} = ba^{-1} = a^{-1}b$).
- There exist non abelian groups G and subgroups H such that right and left congruence coincide but this is not true in general. (give a counter example)

Theorem 1.5.4. *Let H be a subgroup of a group G.*

i) Right (resp. left) congruent modulo H is an equivalence relation on G.

ii) The equivalence class of $a \in G$ under right (resp. left) congruence modulo H is the set $Ha = \{ha \mid h \in H\}$ (resp. $aH = \{ah \mid h \in H\}$).

iii) $|Ha| = |H| = |aH|$ *for all* $a \in G$.

Proof. We prove the theorem for right congruence and right cosets. Analogous arguments apply to left congruence.

i) Let $a, b, c \in G$. Then $a \equiv a \bmod H$ since $aa^{-1} = e \in H$; hence $\equiv$ is reflexive. Since

$$\begin{aligned} a \equiv_r b \bmod H &\Rightarrow ab^{-1} \in H \\ &\Rightarrow \left(ab^{-1}\right)^{-1} \in H \\ &\Rightarrow ba^{-1} \in H \ ; \quad \text{since } \left(ab^{-1}\right)^{-1} = ba^{-1} \\ &\Rightarrow b \equiv_r a \bmod H. \end{aligned}$$

$\therefore \ \equiv_r$ is symmetric.

i) If $a \equiv_r b \bmod H$ and $b \equiv_r c \bmod H$, we have $ab^{-1} \in H$ and $bc^{-1} \in H$. Then $ac^{-1} = (ab^{-1})(bc^{-1}) \in H$ which implies $a \equiv_r c \bmod H$. Therefore, $\equiv_r$ is transitive. Thus, right congruence modulo H is an equivalence relation.

ii) The equivalence class of $a \in G$ under right congruence is

$$\begin{aligned} \{x \in G \mid x \equiv_r \bmod H\} &= \{x \in G \mid xa^{-1} \in H\} \\ &= \{x \in G \mid xa^{-1} = h \in H\} \\ &= \{x \in G \mid x = ha; h \in H\} \\ &= \{ha \in H \mid h \in H\} \\ &= Ha. \end{aligned}$$

iii) The map $\alpha : Ha \to H$ given by $\alpha(ha) = h$ is easily seen to be a bijective.

□

Corollary 1.5.5. *Let* H *be a subgroup of a group* G.

a) G *is union of the right (resp. left) cosets of* H *in* G.

b) Two right (resp. left) cosets of H *in* G *are either disjoint or equal.*

c) For all $a, b \in G$, $Ha = Hb \Leftrightarrow ab^{-1} \in H$ *and* $aH = bH \Leftrightarrow a^{-1}b \in H$.

d) If R_H *is the set of distinct right cosets of* H *in* G *and* L_H *is the set of distinct left cosets of* H *in* G, *then* $|R_H| = |L_H|$.

Proof. a) - c) are immediate consequences of Remark 1.4.13. d) The map $R_H \to L_H$ given by $Ha \mapsto a^{-1}H$ is a bijection since $Ha = Hb \Leftrightarrow ab^{-1} \in H \Leftrightarrow (a^{-1})^{-1} b^{-1} \in H \Leftrightarrow a^{-1}H = b^{-1}H$. □

Additive Notation: If H is a subgroup of a group G, then right congruence modulo H is defined by $a \equiv_r b \bmod H \Leftrightarrow a - b \in H$. The equivalence class of $a \in G$ is the right coset $H + a = \{h + a \mid h \in H\}$.

Definition 1.5.6. Let H be a subgroup of a group G. The *index of H in G*, denoted $[G : H]$, is the cardinal number of the set of distinct right (resp. left) cosets of H in G.

Remark 1.5.7.

† If $G = \mathbb{Z}$ and $H = m\mathbb{Z}$, then $[G : H] = m$. Here G and H are infinite groups however the index $[G : H]$ is not.

† If $H = \langle e \rangle$, then $Ha = \{a\}$ for every $a \in G$ and $[G : H] = |G|$.

Theorem 1.5.8. *If K, H, G are groups with $K < H < G$, then $[G : K] = [G : H][H : K]$. If any of two of these indices are finite, then so is the third.*

Proof. By Corollary 1.5.5 $G = \cup_{i \in I} Ha_i$ with $a_i \in G, |I| = [G : H]$ and the cosets Ha_i mutually disjoint (that is, $Ha_i = Ha_j \Leftrightarrow i = j$). Similarly, $H = \cup_{j \in J} Kb_j$ with $b_j \in H, |J| = [H : K]$ and the cosets Kb_j mutually disjoint. Therefore,

$$G = \cup_{i \in I} Ha_i = \cup_{i \in I} \left(\cup_{j \in J} Kb_j\right) a_i = \cup_{(i,j) \in (I \times J)} Kb_j a_i \,.$$

It suffieces to show that the cosets $Kb_j a_i$ are mutually disjoint. For then by Corollary 1.5.5, we must have

$$[G : K] = |I \times J| = |I||J| = [G : H][H : K] \,.$$

To show this, if $Kb_j a_i = Kb_r a_t$, then $b_j a_i = k b_r a_t$ $(k \in K)$. Since $b_j, b_r, k \in H$, we have $Ha_i = Hb_j a_i = Hkb_r a_t = Ha_t \Rightarrow i = t$ and $b_j = kb_r$. Thus $Kb_j = Kkb_r = Kb_r \Rightarrow j = r$. Therefore, the cosets $Kb_j a_i$ are mutually disjoint. The last statement of the theorem is easy to show. □

Corollary 1.5.9 (Lagrange)**.** *If H is a subgroup of a group G, then $|G| = [G : H]|H|$. In particular, if G is finite, the order $|a|$ of $a \in G$ divides $|G|$.*

Proof. Let $K = \langle e \rangle$. Then by the above theorem $|G| = [G : K] = [G : H][H : K] = [G : H]|H|$. In particular, if $H = \langle a \rangle$, then $|H|$ divides $|G|$. □

Proposition 1.5.10. *If H and K are subgroups of a group G, then $[H : H \cap K] \leq [G : K]$. If $[G : K]$ is finite, then $[H : H \cap K] \leq [G : K]$ if and only if $G = KH$.*

Proof. Let A be the set of all right cosets of $H \cap K$ in H. Let B be the set of all right cosets of K in G. Consider the map

$$\phi : A \longrightarrow B$$
$$(H \cap K)h \mapsto Kh.$$

Since $(H \cap K)h_1 = (H \cap K)h_2 \Rightarrow h_1 h_2^{-1} \in H \cap K \subset K$, we have $Kh_1 = Kh_2$. Thus ϕ is well-defined. Let us show that the map ϕ is injective.

$$\phi\left((H \cap K)h_1\right) = \phi\left((H \cap K)h_2\right) \Rightarrow Kh_1 = Kh_2 \Rightarrow h_1 h_2^{-1} \in K\,.$$

But since $h_1, h_2 \in H < G$, we have

$$h_1 h_2^{-1} \in H \Rightarrow h_1 h_2^{-1} \in H \cap K \Rightarrow (H \cap K)h_1 = (H \cap K)h_2\,.$$

Then $[H : H \cap K] = |A| \leq |B| = [G : K]$. If G is finite, then we show that

a) $[H : H \cap K] = [G : K]$ if and only if ϕ is surjective.

b) ϕ is surjective if and only if $G = KH$.

To see this, $|A| = [H : H \cap K] = [G : K] = |B|$ if and only if ϕ is bijective. Since ϕ is already injective, the statement is true if ϕ is surjective. But the map ϕ is surjective if and only if $KH = \phi(A) = B$ and $B = KH$ if and only if $G = KH$. □

Remark 1.5.11. We can also rewrite the above proposition as follows: If H and K are subgroups of a group G, then $[K : H \cap K] \leq [G : H]$. If $[G : H]$ is finite, then $[K : H \cap K] = [G : H]$ if and only if $G = HK$.

Proposition 1.5.12. *Let H and K be subgroups of finite index of a group G. Then $[G : H \cap K]$ is finite and $[G : H \cap K] \leq [G : H][G : K]$. Furthermore, $[G : H \cap K] = [G : H][G : K]$ if and only if $G = HK$.*

Proof. $[G : H]$ and $[G : K]$ are finite and

$$H{\cap}K < H, K < G \Rightarrow [G : H{\cap}K] = [G : H][H : H{\cap}K] \text{ and } [G : H{\cap}K] = [G : K][K : H{\cap}K]\,.$$

By Proposition 1.5.10, we have

$$[H : H \cap K] \leq [G : K] < \infty \Rightarrow [H : H \cap K] \text{ is also finite}\,.$$

Similarly, $[K : H \cap K]$ is finite, see Remark 1.5.11. But

$$[G : H \cap K] = [G : H][H : H \cap K] \leq [G : H][G : K]$$

since $[H : H \cap K] \leq [G : K] \Rightarrow [G : H \cap K]$ is finite. Furthermore, note that in Remark 1.5.11 it is stated that $[K : H \cap K] = [G : H]$ if and only if $G = HK$. We thus have

$$[G : K][G : H] = [G : K][K : H \cap K] = [G : H \cap K] \Leftrightarrow G = HK$$

□

1.6 Normality, Quotient Groups and Homomorphisms

Subgroups N os a group G such that left and right congruence modulo N coincide paly an important role in determining both the structure of a group G and the nature of homomorphisms with domain G.

Theorem 1.6.1. *If N is a subgroup og a group G, then the following conditions are equivalent:*

(i) Left and right congruence modulo N coincide (that is, define the same equivalence relation on G).

(ii) every left coset of N in G is a right coset of N in G.

(iii) $aN = Na$ for all $a \in G$.

(iv) for each $a \in G$, $aNa^{-1} \subseteq N$, where $aNa^{-1} = \{ana^{-1} \mid n \in N\}$.

(v) for each $a \in G, aNa^{-1} = N$.

Proof. (i) $\Leftrightarrow$ (iii) Two equivalence relations R and S are identical if and only if the equivalence class of each element under R is equal to its equivalence class unser S. In this case, the equivalence classes are the left and right cosets respectively of N. (ii) $\Rightarrow$ (iii) If $aN = Nb$ for some $b \in G$, then $a \in Nb \cap Na \Rightarrow Nb = Na$ since two right cosets are either disjoint or equal. (iii) $\Rightarrow$ (iv) Let $x \in aNa^{-1}$. Then $x = ana^{-1}$ for some $n \in N$. But $x = ana^{-1} = naa^{-1} = n \in N$ since $an = na$. (iv) $\Rightarrow$ (v) By given, $a^{-1}Na \subseteq N$ since $a^{-1} \in G$. Then $n = a(a^{-1}na)a^{-1} \in aNa^{-1}$ since $a^{-1}na \in N$. (v) $\Rightarrow$ (ii) is immediate. □

Definition 1.6.2. A subgroup N of a group G which satisfies the equivalent conditions of Theorem 1.6.1 is said to be *normal* in G (or a *normal subgroup* of G) and is denoted by $N \triangleleft G$.

Remark 1.6.3.

(a) If G is a group with subgroups N and M such that $N \triangleleft M$ and $M \triangleleft G$, it doea not follow that $N \triangleleft G$.

(b) If N is normal in G, then it is normal in every subgroup of G containing N.

Proof. Left as an exercise. □

Recall that the join

$$H \vee K = \left\{ \prod_{i=1}^{r} h_i k_i \;\middle|\; h_i \in H, k_i \in K \right\}$$

of two subgroups is the subgroup $\langle H \cup K \rangle$ generated by H and K.

Theorem 1.6.4. *Let K and N be subgroups of a group G with N normal in G. Then*

i) $N \cap K \triangleleft K$

ii) $N \triangleleft N \vee K$

iii) $NK = N \vee K = KN$

iv) $K \triangleleft G$ *and* $K \cap N = \langle e \rangle \Rightarrow nk = kn$ *for all* $k \in K$ *and* $n \in N$.

Proof. i) If $n \in N \cap K$ and $a \in K$, then $ana^{-1} \in N$ since $N \triangleleft G$ and $ana^{-1} \in K$ since $K < G$. Thus $a(N \cap K)a^{-1} \subseteq N \cap K$ and $N \cap K \triangleleft K$. ii) Since $N < N \vee K$ and $N \triangleleft G$, we have $N \triangleleft N \vee K$. iii) Let $x \in N \vee K$. Then $x = n_1 k_1 \cdots n_r k_r$ with $n_i \in N, k_i \in K$. Since $N \triangleleft G$, $n_i k_j = k_j n_i', n_i' \in N$, x can be rewritten as $x = n(k_1 \cdots k_r)$ for some $n \in N$. This implies that $N \vee K \subseteq NK$. Since the other inclusion is obvious, we have $N \vee K = NK$. iv) Let $k \in K$ and $n \in N$. Then $nkn^{-1} \in K$ since $K \triangleleft G$ and $kn^{-1}k^{-1} \in N$ since $N \triangleleft G$. Hence $(nkh^{-1})\, k^{-1} = n\,(kn^{-1}k^{-1}) \in N \cap K = \langle e \rangle \Rightarrow nk = kn$. □

Theorem 1.6.5. *If N is a normal subgroup of a group G and G/N is the set of all (left) cosets of N in G, then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.*

Proof. Since the cosets aN, bN, abN are the equivalence classes of $a, b, ab \in G$, respectively, under the equivalence relation of congruence modulo N, if suffices by Theorem 1.2.10 to show that congruence modulo N is a congruence relation, that is,

$$a_1 \equiv b \bmod N \text{ and } b_1 \equiv b \bmod N \Rightarrow a_1 b_1 \equiv ab \bmod N\,.$$

By assumption, $a_1 a^{-1} = n_1 \in N$ and $b_1 b^{-1} = n_2 \in N$. Hence $(a_1 b_1)(ab)1{-}1 = a_1 b_1 b^{-1} a^{-1} = a_1 n_2 a^{-1}$. Since N is normal in G, $a_1 N = N a_1 \Rightarrow a_1 n_2 = n_3 a_1$ for some $n_3 \in N$. Consequently,

$$(a_1 b_1)(ab)1{-}1 = n_3 a_1 a^{-1} = n_3 n_1 \in N \Rightarrow a_1 b_1 \equiv ab \bmod N\,.$$

□

Definition 1.6.6. If N ia a normal subgroup of a group G, then the group G/N, as int he above theorem, is called the *quotient group* or *factor group* of G by N. If G is written additively, then the group operation in G/N is given by (a+N)+(b+N) = (a+b)+ N.

Remark 1.6.7. If $m > 1$ is a (fixed) integer and $k \in \mathbb{Z}$, then Remark 1.5.1 shows that the equivalence class of k under the congruence modulo m is precisely the coset of $\langle m \rangle$ in $\mathbb{Z}$ which contains k, that is, as sets, $\mathbb{Z}_m = \mathbb{Z}/\langle m \rangle$. Theorem 1.2.10 and Theorem 1.6.5 show that the group operations coincide, whence $\mathbb{Z}_m = \mathbb{Z}/\langle m \rangle$ as groups.

1.6.1 Relationships between Normal subgroups, Quotient groups and Homomorphisms

In this subsection we explore the relationships between normal subgroups, quotient groups and Homomorphisms. We begin with following theorem:

Theorem 1.6.8. *If $f : G \to H$ is a homomorphism of groups, then the kernel of f,*

$$\ker f = \{a \in G \mid f(a) = e_H\}$$

is a normal subgroup of G. Conversely, if N is a normal subgroup of G, then the map $\pi : G \to G/N$, $a \mapsto aN$ is an epimorphism with kernel N.

Proof. Let $x \in \ker f$ and $a \in G$. Then

$$\begin{aligned} f(axa^{-1}) &= f(a)f(x)f(a^{-1}) = f(a)f(a)^{-1} = e_H \\ &\Rightarrow axa^{-1} \in \ker f \Rightarrow a \ker f a^{-1} \subseteq \ker f \\ &\Rightarrow \ker f \triangleleft G\,. \end{aligned}$$

The map π is clearly surjective and since $\pi(ab) = abN = (aN)(bN) = \pi(a)\pi(b)$, this map is an epimorphism. Now

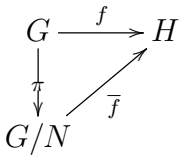
$$\begin{aligned} \ker\pi &= \{a \in G \mid \pi(a) = eN = N\} \\ &= \{a \in G \mid aN = N\} \\ &= \{a \in G \mid a \in N\} = N\,. \end{aligned}$$

□

Definition 1.6.9. The map $\pi : G \to G/N$ is called the *canonical epimorphism* or *projection.*

Hereafter unless stated otherwise $G \to G/N \quad (N \triangleleft G)$ always denotes the canonical epimorphism.

Theorem 1.6.10. *If $f : G \to H$ is a homomorphism of groups and N is a normal subgroup of G contained in the kernel of f, there is a unique homomorphism $\overline{f} : G/N \to H$ such that $\overline{f}(aN) = f(a)$ for all $a \in G$, that is, the diagram*



is commutative. Moreover,

i) $\mathrm{Im}f = \mathrm{Im}\overline{f}$

ii) $\ker\overline{f} = \ker f/N$ *and*

iii) $\overline{f}$ *is an isomorphism if and only if* f *is an epimomorphism and* $N = \ker f$.

Proof. First we show that the map $\overline{f}$ is well-defined. To see this, suppose $aN = bN$. Then

$$\begin{aligned} aN = bN &\Rightarrow b = be \in bN = aN \\ &\Rightarrow b = an, n \in N \\ &\Rightarrow f(b) = f(an) = f(a)f(n) = f(a)e = f(a) \text{ since } N < \ker f \\ &\Rightarrow \overline{f}(bN) = \overline{f}(aN)\,. \end{aligned}$$

If $b \in aN$, then $b = an, n \in N$, and $f(b) = f(a)f(n) = f(a)e = f(a)$ since $N < \ker f$. Therefore, f has the same effect on every element of the coset aN and the map $\overline{f}$ is a well-defined funtion. Since

$$\overline{f}(aNbN) = \overline{f}(abN) = f(ab) = f(a)f(b) = \overline{f}(aN)\overline{f}(bN),$$

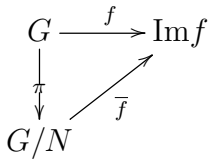
$\overline{f}$ is a group homomorphism. Clearly $\mathrm{Im}\overline{f} = \mathrm{Im} f$ and

$$\begin{aligned}
\ker\overline{f} &= \{an \in G/N \mid \overline{f}(aN) = e_H\} \\
&= \{aN \in G/N \mid f(a) = e_H\} \\
&= \{aN \in G/N \mid a \in \ker f\} \\
&= \{aN \mid a \in \ker f \cap G\} \\
&= \{aN \mid a \in \ker f\} \\
&= \ker f/N\,.
\end{aligned}$$

The map $\overline{f}$ is unique since it is completely determined by f. Finally it is clear that $\overline{f}$ is an epimorphism if and only if f is. By Theorem 1.3.5, $\overline{f}$ is a monomorphism if and only if $\ker\overline{f} = \ker f/N$ is a trivial subgroup of G/N which occurs if and only if $\ker f = N$. □

Corollary 1.6.11 (First Isomorphism Theorem(FIT))**.** *If $f : G \to H$ is a homomorphism of groups, then f induces an isomorphism $G/\ker f \cong \mathrm{Im} f$.*

Proof. $f : G \to \mathrm{Im} f$ is an epimorphism. Let $N = \ker f$. By Theorem 1.6.8, N is a normal subgroup of G. By Theorem 1.6.10, there exists a unique injective (since $N = \ker f$) map $\overline{f} : G/N \to \mathrm{Im} f$ such that the diagram



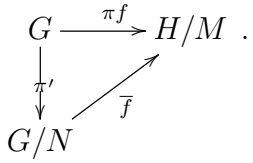
is commutative. Since f is an epimorphism so is $\overline{f}$. Thus $\overline{f}$ is an isomorphism. □

Corollary 1.6.12. *If $f : G \to H$ is a homomorphism of groups, $N \triangleleft G$, $M \triangleleft H$, and $f(N) < M$, then f induces a homomorphism $\overline{f} : G/N \to H/M$, given by $aN \mapsto f(a)M$. Moreover, $\overline{f}$ is an isomorphism if and only if $\mathrm{Im} f \vee M = H$ and $f^{-1}(M) \subseteq N$. In particular, if f is an epimorphism such that $f(N) = M$ and $\ker f \subseteq N$, then $\overline{f}$ is an isomorphism.*

Proof. Consider the composition map $G \xrightarrow{f} H \xrightarrow{\pi} H/M$. Since $f(N) < M$, we have $N \subseteq f^{-1}(M)$ and

$$\begin{aligned} \ker \pi f &= \{a \in G \mid \pi f(a) = M\} \\ &= \{a \in G \mid f(a)M = M\} \\ &= \{a \in G \mid f(a) \in M\} \\ &= \{a \in G \mid a \in f^{-1}(M)\} \\ &= G \cap f^{-1}(M) = f^{-1}(M)\,. \end{aligned}$$

Now consider the diagram



which is commutative by construction. By Theorem 1.6.10 (applied to πf), $\overline{f}$ given by $aN \mapsto \pi f(a) = f(a)M$, see the above diagram, is a homomorphism that is an isomorphism if and only if πf is an epimorphism and $N = \ker \pi f$. Thus it suffices to show that πf is an epimorphism and $N = \ker \pi f$ if and only if $\mathrm{Im} f \vee M = H$ and $f^{-1}(M) \subseteq N$. To see this,

$$\begin{aligned} \pi f \text{ is an epimorphism} &\Leftrightarrow \pi f(G) = H/M \\ &\Leftrightarrow f(G)M = H/M \\ &\Leftrightarrow f(G) = H \\ &\Leftrightarrow H = \mathrm{Im} f = \mathrm{Im} f \vee M\,. \end{aligned}$$

If $N = \ker \pi f = f^{-1}(M)$, then clearly $f^{-1}(M) \subseteq N$. Conversely, if $f^{-1}(M) \subseteq N$, then $N = \ker \pi f = f^{-1}(M)$ since $N \subseteq f^{-1}(M)$. In particular, if f is an epimorphism, then $H = \mathrm{Im} f = \mathrm{Im} f \vee M$. If $f(N) = M$ and $\ker f \subseteq N$, then $f^{-1}(M) \subseteq N$ since

$$\begin{aligned} x \in f^{-1}(M) &\Rightarrow f(x) \in M = f(N) \\ &\Rightarrow f(x) = f(n) \text{ for some } n \in N \\ &\Rightarrow f(xn^{-1}) = e_H \\ &\Rightarrow xn^{-1} \in \ker f \subseteq N \\ &\Rightarrow xn^{-1} = n_1 \text{ for some } n_1 \in N \\ &\Rightarrow x = n_1 n \in N \end{aligned}$$

Thus $\overline{f}$ is an isomorphism. □

Corollary 1.6.13 (Second Isomorphism Theorem(SIT)). *If K and N are subgroups of a group G, with N normal in G, then $K/(K \cap N) \cong NK/N$.*

Proof. Since $K, N < G$ and $N \triangleleft G$, we have $N \triangleleft N \vee K = NK = KN$ by Theorem 1.6.4 (ii-iii). Consider the composition map $f = \pi \circ \iota : K \xrightarrow{\iota} NK \xrightarrow{\pi} NK/N$. Clearly f is a group homomorphism with kernel $K \cap N$, whence the map $\overline{f} : K/(N \cap K) \to \mathrm{Im}f$ is an isommorphism by the first isomorphism theorem, see Corollary 1.6.11. Now it remains to show that $\mathrm{Im}f = NK/N$. Note that every element in NK/N is of the form nkN $(n \in N, k \in K)$. The normality of N implies that $nk = kn_1$ $(n_1 \in N)$, whence $nkN = kn_1N = kN = f(k)$. Therefore, f is an epimorphism and hence $\mathrm{Im}f = NK/N$. □

Example 1.6.14. Consider the group $(\mathbb{Z}, +)$ of integers and let $M = \langle 3 \rangle = 3\mathbb{Z}$ and $N = \langle 5 \rangle = 5\mathbb{Z}$. Since $+$ is commutative on $\mathbb{Z}$, M and N are normal subgroups of $\mathbb{Z}$. Moreover, we have $M \cap N = 15\mathbb{Z}$ and $M + N = \mathbb{Z}$. Thus by SIT

$$3\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z}\,.$$

Note that $3\mathbb{Z}/15\mathbb{Z} = \{0, 3, 6, 9, 12\}$ and $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$.

Corollary 1.6.15 (Third Isomorphism Theorem(TIT)). *If H and K are normal subgroups of a group G such that $K < H$, then H/K is a normal subgroup of G/K and $(G/K)/(H/K) \cong G/H$.*

Proof. The identity map $1_G : G \to G$ has $1_G(K) = K < H$ and therefore induces an epimorphism $\pi : G/K \to G/H$, with $\pi(aK) = aH$. Since $H = \pi(aK)$ if and only if $a \in H$, $\ker \pi = \{aK \mid a \in H\} = H/K$. Hence $H/K \triangleleft G/K$ by Theorem 1.6.8 and $G/H = \mathrm{Im}\,\pi \cong (G/K)/\ker \pi = (G/K)/(H/K)$ by FIT. □

1.7 Symmetric, Alternating and Dihedral Groups

Definition 1.7.1. Let X be a non-empty set. Any bijection of X onto itself is called a *permutation* on X. The set $S(x)$ of all permutations on X forms a group under the composition of mappings. Any subgroup og X is called a *group of permutation* on X.

Definition 1.7.2. For any positive integer, the set I_n is defined by $I_n = \{1, 2, \ldots, n\}$ and the group $(S(I_n), \circ)$ of permutations on I_n is denoted by S_n and is called the *symmetric group* of degree n.

Definition 1.7.3. Let $i_1, i_2, \ldots, i_r \, (r \leq n)$ be distinct elements of I_n. Then $(i_1 i_2 i_3 \cdots i_r)$ denotes the permutation that maps $i_1 \mapsto i_2, i_2 \mapsto i_3, \ldots, i_{r-1} \mapsto i_r$ and $i_r \mapsto i_1$, and maps every other element of I_n onto itself. This permutation, $(i_1 i_2 i_3 \cdots i_r)$, is called a *cycle* of length r or an *r-cycle*. A 2-cycle is called a *transposition*.

Remark 1.7.4.

a) A 1-cycle (k) is the identity permutation.

b) An r-cycle is an element of order r in S_n.

Proof. If $\sigma = (\sigma_1 \cdots \sigma_r)$ is an r-cycle in S_n, then $\sigma(\sigma_1) = \sigma_2, \sigma^2(\sigma_1) = \sigma_3, \ldots, \sigma^r(\sigma_1) = \sigma_1$. Similarly, $\sigma^r(\sigma_i) = \sigma_i$ for $i = 2, \ldots, r$. Since σ^r fixes all the other elements, it is the identity permutation. But none of the permutations $\sigma, \sigma^2, \ldots, \sigma^{r-1}$ equal the identity permutation because they all move the element σ_1. Hence the order of σ is r. □

c) Let τ be a cycle such that $\tau(i) \neq i$ for some $i \in I_n$. Then

$$\tau = \begin{pmatrix} i & \tau(i) & \tau(\tau(i)) & \cdots & \tau^d(i) \\ \tau(i) & \tau(\tau(i)) & \cdots & \tau^d(i) & i \end{pmatrix}$$

for some $d \geq 1$.

Proof. Assume that $\tau = (i_1 i_2 \cdots i_d)$ be a d-cycle permutation for some $d \geq 1$. Since $\tau(i) \neq i$ for some $i \in I_n$, then we get that $i = i_k$ for $1 \leq k \leq d$. Now

$$\begin{aligned} \tau(i) &= \tau(i_k) = i_{k+1} \\ \tau^2(i) &= \tau(i_{k+1}) = i_{k+2} \\ &\vdots \\ \tau^{d-k}(i) &= \tau(i_{d-1}) = i_d \\ \tau^{d-k+1}(i) &= \tau(i_d) = i_1 \\ &\vdots \\ \tau^{(d-k)+(k-1)}(i) &= \tau(i_{k-2}) = i_{k-1} \\ \tau^d(i) &= \tau(i_{k-1}) = i_k = i \,. \end{aligned}$$

□

d) The inverse of the cycle $(i_1 i_2 \cdots i_r)$ is the cycle

$$(i_r i_{r-1} \cdots i_2 i_1) = (i_1 i_r i_{r-1} \cdots i_2)\,.$$

e) The cyclic representation $(i_1 i_2 \cdots i_r)$ is not unique. That is, $(i_1 i_2 \cdots i_r) = (i_2 \cdots i_r i_1)$ For example,

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \text{ is a 4-cycle}$$
$$= (1432) = (4321) = (3214) = (2143)$$

f) If $\tau = (i_1 \ldots i_r)$ is an r-cycle in S_n, then τ is an r-cycle in S_m for all $m \geq n$. In fact, if m is the maximum of $i_1, i_2, \ldots, i_r$, then $\tau = (i_1 \ldots i_r)$ is an r-cycle in S_m.

g) The composition of two permutation may not commute, that is, if $\tau, \sigma \in S_n$, then it is not always true that $\tau\sigma = \sigma\tau$. For example, if σ is the 3-cycle (125) and τ is as in e), then

$$\sigma\tau = (125)(1432) = (1435) \neq (2543) = (1432)(125) = \tau\sigma\,.$$

Definition 1.7.5. The permutation $\sigma_1, \sigma_2, \ldots, \sigma_r$ of S_n are said to be *disjoint* provided that for each $1 \leq i \leq r$, and every $k \in I_n$,

$$\sigma_i(k) \neq k \Rightarrow \sigma_j(k) = k$$

for all $j \neq i$.

In other words, $\sigma_1, \sigma_2, \ldots, \sigma_r$ are disjoint if and only if no element of I_n is moved by more than one of $\sigma_1, \sigma_2, \ldots, \sigma_r$. In this case, the composition of two disjoint permutations commutes.

Permutations that are not cycles can be split up into two or more cycles as follows:

Definition 1.7.6. If σ is a permutation in S_n and $i \in \{1, 2, 3, \ldots, n\}$, the *orbit* of i under σ consists of the distinct elements $i, \sigma(i), \sigma^2(i), \ldots$.

Based on the above definition, we can split a permutation up into its different orbits, and each orbit will give rise to a cycle.

Example 1.7.7. Consider the permutation

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

Here $\sigma(1) = 3, \sigma^2(1) = 8, \sigma^3(1) = 4$, and $\sigma^4(1) = 1$; thus the orbit of 1 is $\{1, 3, 8, 4\}$. This is also the orbit of 3, 4, and 8. This orbit gives rise to the cycle (1 3 8 4). Since σ leaves 2 and 5 fixed, their orbits are $\{2\}$ and $\{5\}$. The orbit of 6 and 7 is $\{6, 7\}$, which gives rise to the 2-cycle $(2, 6)$.

Theorem 1.7.8. *Every nonidentity permutation in S_n is uniquely (up to the order of the factors) a product of disjoint cycles, each of which has length at least 2.*

Corollary 1.7.9. *The order of a permutation $\sigma \in S_n$ is the least common multiple of the order of its disjoint cycles.*

Proof. Let $\sigma = \sigma_1 \cdots \sigma_r$, with $\{\sigma_i\}$ disjoint cycles. Since disjoint cycles commute, $\sigma^m = \sigma_1^m \cdots \sigma_r^m$ for all $m \in \mathbb{Z}$ and $\sigma^m = (1)$ if and only if $\sigma_i^m = (1)$ for all i. Thus, by Theorem 1.4.4, $\sigma^m = (1)$ if and only if $|\sigma_i|$ divides m for all i. Since $|\sigma|$ is the least such m, the conclusion follows. □

Example 1.7.10. Find the order of the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 8 & 7 & 1 & 4 & 6 & 2 \end{pmatrix}.$$

We can write this permutation in terms of disjoint cycles as

$$\sigma = \begin{pmatrix} 1 & 3 & 8 & 2 & 5 \end{pmatrix} \circ \begin{pmatrix} 4 & 7 & 6 \end{pmatrix}.$$

By Corollary 1.7.9, the order of σ is $\operatorname{lcm}(5, 3) = 15$.

Corollary 1.7.11. *Every permutation in S_n can be written as a product of (not necessarily disjoint) transpositions.*

Proof. It suffices by Theorem 1.7.8 to show that every cycle is a product of transpositions. For $r = 1$, we have $(x_1) = (x_1x_2)(x_1x_2)$ and for $r > 1$, $(x_1x_2x_3 \cdots x_r) = (x_1x_r)(x_1x_{r-1}) \cdots (x_1x_3)(x_1x_2)$. □

1.7.1 Odd and Even Permutations

Definition 1.7.12. A permutation $\sigma \in S_n$ is said to be *even* (resp. *odd*) if σ can be written as a product of an even (resp. odd) number of transpositions.

The sign of a permutation τ, denoted $\operatorname{sgn} \tau$, is 1 or -1 according as τ is even or odd. The fact that $\operatorname{sgn} \tau$ is well-defined is an immediate consequence of

Theorem 1.7.13. *A permutation in $S_n (n \geq 2)$ cannot be both even and odd.*

Theorem and Definition 1.7.14. For each $n \geq 2$, let A_n be the set of all even permutations of S_n. Then A_n is a normal subgroup of S_n of index 2 and order $|S_n|/2 = n!/2$. Furthermore, A_n is the only subgroup of S_n of index 2. The group A_n is called the *alternating group on n letters* or the *alternating group of degree n.*

Proof. Let C be the multipicative subgroup $\{1, -1\}$ of the integers. Consider the map f defined as

$$\begin{aligned} f : S_n &\to C, \\ \sigma &\mapsto \operatorname{sgn} \sigma \,. \end{aligned}$$

Clearly, it is easy to see that the map f is an epimorphism of groups. The kernel of f is A_n and, hence, is a normal subgroup of S_n since the kernel is normal in S_n. Thus, by the first isomorphism theorem of groups, we have

$$S_n/A_n \cong C$$

which implies $[S_n : A_n] = 2$ and $|A_n| = S_n/2$. Show uniqueness! □

Definition 1.7.15. A group G is said to be *simple* if G has no proper normal subgroups.

The only simple abelian groups are the $\mathbb{Z}_p$ with p prime. In fact, there are a number of nonabelian simple groups, in particular, we have:

Lemma 1.7.16. *The alternating group A_n is simple if and only if $n \neq 4$.*

1.8 Categories: Products, Coproducts, and Free Objects

Categories will serve as a useful language and provide a general context for dealing with a number of different mathematical situations.

The intuitive idea underlying the definition of a category is that several of the mathematical objects already introduced (sets, groups, monoids) or to be introduced (rings, modules) together with the appropriate maps of these objects (functions for sets; homomorphisms for groups, etc.) have a number of formal properties in common.

Definition 1.8.1. A *category* is a class $\mathcal{C}$ of objects (denoted $A, B, C, \ldots$) together with

i) a class of disjoint sets, denoted $\hom(A, B)$, one for each pair of objects in $\mathcal{C}$; (an element f of $\hom(A, B)$ is called a *morphism* form A to B and is denoted $f : A \to B$);

ii) for each triple (A, B, C) of objects of $\mathcal{C}$ a function

$$\hom(B, C) \times \hom(A, B) \to \hom(A, C);$$

(for morphism $f : A \to B, g : B \to C$, this function is written $(g, f) \mapsto g \circ f$ and $g \circ f : A \to C$ is called the *composite* of f and g); all subject to the two axioms:

1. *Associativity:* If $f : A \to B, g : B \to C, h : C \to D$ are morphisms of $\mathcal{C}$, then $h \circ (g \circ f) = (h \circ g) \circ f$.
2. *Identity:* For each object B of $\mathcal{C}$ there exists a morphism $1_B : B \to B$ such that for any $f : A \to B, g : B \to C$,

$$1_B \circ f = f \text{ and } g \circ 1_B = g\,.$$

Definition 1.8.2. In a category a morphism $f : A \to B$ is called an *equivalence* if there is in $\mathcal{C}$ a morphism $g : B \to A$ such that $g \circ f = 1_A$ and $f \circ g = 1_B$. The composite of two equivalences, when defined, is an equivalence. If $f : A \to B$ is an equivalence, A and B are said to be *equivalent*.

Example 1.8.3.

a) Let $\mathcal{S}$ be the class of all sets. For $A, B \in \mathcal{S}$, $\hom(A, B)$ is the set of all functions $f : A \to B$. Then $\mathcal{S}$ is easily seen to be a category.