Contents

1 Groups **1**
1.1 Introduction 1
1.2 Semigroups, Monoids and Groups 1
1.3 Homomorphisms and Subgroups 6
1.4 Cyclic Groups 9

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.

Theorem 1.2.9. *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 $a_1b_1 \sim a_2b_2$ 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 $a_1b_1 \sim a_2b_2$ by hypothesis which also implies $\overline{a_1b_1} = \overline{a_2b_2}$ 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 1.2.10. If p is prime, then $(\mathbb{Z}_p \setminus \{p\}, \cdot)$ is a group of order $p-1$.

Definition 1.2.11. 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 1.2.12 (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 1.2.13 (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 1.2.14. 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 $a \in \mathrm{Ker}f$. 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 $ab^{-1} \in \mathrm{Ker}f = \{e_G\}$. 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 $\text{Ker}\alpha = 0$, then $\mathbb{Z} \cong G$ by Theorem 1.3.5. Otherwise $\text{Ker}\alpha$ is a nontrivial subgroup of $\mathbb{Z}$ and hence $\text{Ker}\alpha = \langle m \rangle$ where m is the least positive integer such that $a^m = e$. Now for all $r, s \in \mathbb{Z}$,

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

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 $\text{Ker}\alpha = \{0\}$ by Theorem 1.4.2. Thus $a^k = e \Rightarrow k \in \operatorname{Ker}\alpha = \{0\} \Rightarrow k = 0$. 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 $|H| < \infty$, 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

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

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

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

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,

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

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

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). □