Chapter 4
Cyclic Groups

The simplest type of groups are group of integers modulo n and cyclic groups. Cyclic groups are groups in which every element is a power of some fixed element. In this chapter, we examine cyclic groups in detail and determine their important characteristics. We observe that a cyclic subgroup with generator a is the smallest subgroup containing the set $A = \{a\}$. Can we extend subgroups generated by sets with more than one element? We answer this question in this chapter too.

4.1 Group of Integers Modulo *n*

Let $a, b \in \mathbb{Z}$ and n be a positive integer. Already, we defined

$$a \equiv b (\text{mod } n) \ \Leftrightarrow \ n|a - b.$$

This relation is named as congruence modulo n. In Lemma 1.62, we proved that this relation is an equivalence relation. The equivalence class of $a \in \mathbb{Z}$ is the set

$$\overline{a} = \{b \in \mathbb{Z} \mid a \equiv b (\text{mod } n)\}.$$

The integers modulo n partition $\mathbb{Z}$ into n different equivalence classes. We denote the set of these equivalence classes by $\mathbb{Z}_n$. Thus,

$$\mathbb{Z}_n = \{\overline{0}, \ \overline{1}, \ldots, \overline{n-1}\}.$$

For instance, if $n = 5$, then

B. Davvaz, *A First Course in Group Theory*,
https://doi.org/10.1007/978-981-16-6365-9_4

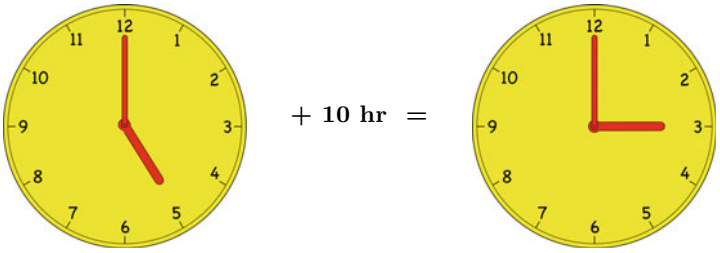

Fig. 4.1 5+10=3

$$\begin{aligned}
\overline{0} &= \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\},\\
\overline{1} &= \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\},\\
\overline{2} &= \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\},\\
\overline{3} &= \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\},\\
\overline{4} &= \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\},
\end{aligned}$$

and

$$\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}.$$

Theorem 4.1 *$(\mathbb{Z}_n, +)$ is an abelian group, where $+$ is the addition modulo n, i.e., $\overline{a} + \overline{b} = \overline{a+b}$, for all $\overline{a}, \overline{b} \in \mathbb{Z}_n$.*

Proof First we show that $+$ is well defined on $\mathbb{Z}_n$. If $\overline{a_1} = \overline{a_2}$ and $\overline{b_1} = \overline{b_2}$, then there exist integers q_1 and q_2 such that $a_1 - a_2 = q_1 n$ and $b_1 - b_2 = q_2 n$. So, we have

$$(a_1 + b_1) - (a_2 + b_2) = a_1 - a_2 + b_1 - b_2 = q_1 n + q_2 n = (q_1 + q_2)n.$$

This implies that $a_1 + b_1 \equiv a_2 + b_2 (\text{mod } n)$, or equivalently $\overline{a_1 + b_1} = \overline{a_2 + b_2}$. Clearly, addition on $\mathbb{Z}_n$ is associative and commutative. $\overline{0}$ is the additive identity for $\mathbb{Z}_n$ and each $\overline{a} \in \mathbb{Z}_n$ has an additive inverse $\overline{-a}$ in $\mathbb{Z}_n$. Note that $\overline{-a} = \overline{n-a}$. ■

Sometimes, when no confusion can arise, we use $0, 1, \ldots, n-1$ to indicate the equivalence classes $\overline{0}, \overline{1}, \ldots, \overline{n-1}$.

Example 4.2 For $n = 12$, we have $3 + 6 = 9$, $8 + 9 = 5$, $6 + 7 = 1$ and $5 + 10 = 3$. A familiar use of modular arithmetic is in the 12-hour clock (see Fig. 4.1, in which the day is divided into two 12-hour periods).

Example 4.3 The Cayley table for $(\mathbb{Z}_5, +)$ is as follows:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

We can also multiply elements of $\mathbb{Z}_n$. Given two elements $\overline{a}$ and $\overline{b}$ in $\mathbb{Z}_n$, we define

$$\overline{a} \cdot \overline{b} = \overline{ab}.$$

This is well defined and with respect to it, $\mathbb{Z}_n$ becomes a commutative monoid.

A multiplicative inverse for $\overline{a} \in \mathbb{Z}_n$ is an element $\overline{b} \in \mathbb{Z}_n$ such that $\overline{a} \cdot \overline{b} = \overline{1}$. An element $\overline{a} \in \mathbb{Z}_n$ is a *unit* if it has a multiplicative inverse in $\mathbb{Z}_n$. In other words, the integer a is a unit modulo n, meaning that $ab \equiv 1 (\mathrm{mod}\ n)$ for some integer b.

By the above operation we do not obtain a group. For instance, $\overline{0}$ does not have a multiplicative inverse.

Lemma 4.4 *$\overline{a}$ is a unit in $\mathbb{Z}_n$ if and only if $(a, n) = 1$.*

Proof If $\overline{a}$ is a unit, then $ab - 1 = qn$ for some integers b and q, and so $ab + qn = 1$. Now, by Theorem (1.51) we conclude that $(a, n) = 1$.

Conversely, if $(a, n) = 1$, then by Theorem (1.51) there exist $x, y \in \mathbb{Z}$ such that $1 = ax + by$. Thus, $\overline{x}$ is a multiplicative inverse of $\overline{a}$. ■

Let U_n denote the set of units of $\mathbb{Z}_n$.

Theorem 4.5 *For each integer $n \geq 1$, the set U_n forms an abelian group under multiplication modulo n, with identity element $\overline{1}$.*

Proof We first show that the product of two units $\overline{a}$ and $\overline{b}$ is also a unit. If $\overline{a}$ and $\overline{b}$ are units, then they have inverses $\overline{c}$ and $\overline{d}$, respectively, such that

$$\overline{a} \cdot \overline{c} = \overline{ac} = \overline{1} \text{ and } \overline{b} \cdot \overline{d} = \overline{bd} = \overline{1}.$$

Hence, we obtain that

$$\overline{ab} \cdot \overline{cd} = \overline{abcd} = \overline{acbd} = \overline{ac} \cdot \overline{bd} = \overline{1} \cdot \overline{1} = \overline{1}.$$

Consequently, $\overline{ab}$ has the inverse $\overline{cd}$, and is a unit. Moreover, for each $\overline{a}, \overline{b}, \overline{c} \in U_n$, we have

$$\begin{aligned}
&\overline{a} \cdot \overline{b} = \overline{ab} = \overline{ba} = \overline{b} \cdot \overline{a}, \\
&\overline{a} \cdot (\overline{b} \cdot \overline{c}) = \overline{a} \cdot \overline{bc} = \overline{a(bc)} = \overline{(ab)c} = \overline{ab} \cdot \overline{c} = (\overline{a} \cdot \overline{b}) \cdot \overline{c}.
\end{aligned}$$

Table 4.1 A short table of values $\varphi(n)$

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8

The identity element of U_n is $\overline{1}$, since $\overline{a} \cdot \overline{1} = \overline{a} = \overline{1} \cdot \overline{a}$, for all $\overline{a} \in U_n$. Finally, if $\overline{a} \in U_n$, then by the definition of U_n, there exists $\overline{c} \in \mathbb{Z}_n$ such that $\overline{a} \cdot \overline{c} = \overline{1} = \overline{c} \cdot \overline{a}$. This yields that $\overline{c} \in U_n$ and $\overline{c}$ is the inverse of $\overline{a}$. ■

Definition 4.6 Let n be a positive integer. The *Euler function* φ is defined to be the number of positive integers not exceeding n which are relatively prime to n.

Table 4.1 is a short table of values $\varphi(n)$:

Corollary 4.7 *For each integer* $n \geq 1$, $|U_n| = \varphi(n)$.

Proof It follows from Lemma 4.4 and Theorem 4.5. ■

Example 4.8 In $\mathbb{Z}_{14}$, the group of units is $U_{14} = \{1, 3, 5, 9, 11, 13\}$. The operation in U_{14} is multiplication modulo 14. The following is Cayley table for U_{14}:

$\cdot$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{9}$	$\overline{11}$	$\overline{13}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{9}$	$\overline{11}$	$\overline{13}$
$\overline{3}$	$\overline{3}$	$\overline{9}$	$\overline{1}$	$\overline{13}$	$\overline{5}$	$\overline{11}$
$\overline{5}$	$\overline{5}$	$\overline{1}$	$\overline{11}$	$\overline{3}$	$\overline{13}$	$\overline{9}$
$\overline{9}$	$\overline{9}$	$\overline{13}$	$\overline{3}$	$\overline{11}$	$\overline{1}$	$\overline{5}$
$\overline{11}$	$\overline{11}$	$\overline{5}$	$\overline{13}$	$\overline{1}$	$\overline{9}$	$\overline{3}$
$\overline{13}$	$\overline{13}$	$\overline{11}$	$\overline{9}$	$\overline{5}$	$\overline{3}$	$\overline{1}$

Example 4.9 If p is prime, then all positive integers smaller than p are relatively prime to p. Hence, $U_p = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$.

Theorem 4.10 *Let* $p > 1$ *be an integer. Then the following statements are equivalent.*

(1) p is prime;
(2) If $\overline{a} \cdot \overline{b} = \overline{0}$ *in* $\mathbb{Z}_p$, *then* $\overline{a} = \overline{0}$ *or* $\overline{b} = \overline{0}$.

Proof $(1 \Rightarrow 2)$ Since p is prime, it follows that $U_p = \mathbb{Z}_p - \{0\}$ is a group. Assume that $\overline{a} \cdot \overline{b} = \overline{0}$ in $\mathbb{Z}_p$. If $\overline{a} = \overline{0}$, then there is nothing to prove. If $\overline{a} \neq \overline{0}$, then $\overline{a} \in U_p$. So, there exists $\overline{x} \in U_p$ such that $\overline{x} \cdot \overline{a} = \overline{1}$. Therefore, we get

$$\overline{0} = \overline{x} \cdot \overline{0} = \overline{x} \cdot (\overline{a} \cdot \overline{b}) = (\overline{x} \cdot \overline{a}) \cdot \overline{b} = \overline{1} \cdot \overline{b} = \overline{b}.$$

($2 \Rightarrow 1$) Suppose that $p = ab$ for some integers a and b. We show $a = \pm 1$ or $\pm p$. Since $p = ab$, it follows that $\overline{ab} = \overline{p} = \overline{0}$. This implies that $\overline{a} \cdot \overline{b} = \overline{0}$ in $\mathbb{Z}_p$. Now, by (2) we conclude that $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$. If $\overline{a} = \overline{0}$, then $p|a$, or equivalently $a = kp$ for some integer k. Hence, we have $p = ab = kpb$. This implies that $1 = kb$. Since k and b are integers, it follows that the only possibilities are $b = \pm 1$, and so $a = \pm p$. If $\overline{b} = \overline{0}$, then a similar argument shows that $a = \pm 1$. Therefore, p is prime. ■

Exercises

1. Solve equation $x^2 + \overline{4}x + \overline{8} = \overline{0}$ in $\mathbb{Z}_{11}$.
2. Find the number of distinct solutions to the equation $x^2 + \overline{(-1)} = \overline{0}$ in $\mathbb{Z}_5$, $\mathbb{Z}_{13}$, and in $\mathbb{Z}_9$.
3. Find, if possible, a multiplicative inverse for $\overline{8}$ in each of $\mathbb{Z}_5$, $\mathbb{Z}_{21}$, and $\mathbb{Z}_{264}$.
4. Find a positive integer n and three elements $\overline{a}$, $\overline{b}$, and $\overline{b}$ in $\mathbb{Z}_n$ such that none of $\overline{a} \cdot \overline{b}$, $\overline{b} \cdot \overline{c}$, and $\overline{c} \cdot \overline{a}$ is equal to $\overline{0}$, yet $\overline{a} \cdot \overline{b} \cdot \overline{c} = \overline{0}$.
5. Given $\overline{a}$, $\overline{b} \in \mathbb{Z}_n$, we say that $\overline{b}$ is a *square root* of $\overline{a}$ if $\overline{b} \cdot \overline{b} = \overline{a}$.
   (a) Find all square roots of elements in $\mathbb{Z}_{17}$, if exist;
   (b) If p is any prime, show that a has at most two square roots modulo n;
   (c) Give an example that shows that it is possible for a number to have more than two square roots.

4.2 Cyclic Groups

This section contains a few observations about cyclic groups. The structure of cyclic groups is relatively simple. We examine cyclic groups in detail and determine many of their important characteristics.

If G is a group, $a \in G$ and $k \in \mathbb{Z}$, then we define

$$a^n = \begin{cases} \underbrace{aa \ldots a}_{k \text{ times}} & \text{if } k > 0 \\ e & \text{if } k = 0 \\ \underbrace{a^{-1}a^{-1} \ldots a^{-1}}_{-k \text{ times}} & \text{if } k < 0. \end{cases}$$

Lemma 4.11 *If G is a group and $a \in G$, then $H = \{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G.*

Proof It is straightforward. ■

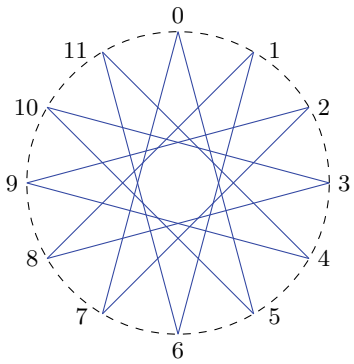

Fig. 4.2 An examples of string art to show that 5 is a generator of $\mathbb{Z}_{12}$

Definition 4.12 Let G be a group. A subgroup H of G is *cyclic* if $H = \{a^n \mid n \in \mathbb{Z}\}$, for some $a \in H$. In this case we say that H is the *cyclic subgroup generated by* a.

When this happens, we write $H = \langle a \rangle$.

Definition 4.13 A group G is called *cyclic* if there is an element $a \in G$ such that $G = \langle a \rangle$. Such an element a is called a *generator* of G.

Example 4.14 The set of integers under addition is an example of an infinite group which is cyclic and is generated by both 1 and -1.

Example 4.15 If $K_4 = \{e,\ a,\ b,\ c\}$ is the Klein's 4-group, then $H = \{e,\ a\}$ is a cyclic subgroup of K_4; however, K_4 is not a cyclic group.

Example 4.16 The set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ for $n \geq 1$ is a cyclic group under addition modulo n. Both 1 and -1 are generators.

Depending on which n we are given, $\mathbb{Z}_n$ may have many generators.

Example 4.17 $\mathbb{Z}_{12} = \langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle$. To verify for instance that $\mathbb{Z}_{12} = \langle 5 \rangle$ we can use a *string art*. Figure 4.2 is an example of string art that illustrates how 5 generates $\mathbb{Z}_{12}$. Twelve tacks are placed along a circle and numbered. A string is tied to tack 0 and then looped around every fifth tack. As a result, the numbers of the tacks that are reached are exactly the ordered numbers of 5 modulo 12. Note that if every seventh tack were used, the same artwork would be obtained. If every third tack were connected, as in Fig. 4.3, the resulting loop would only use four tacks, and so 3 does not generate $\mathbb{Z}_{12}$.

Example 4.18 An *nth root of unity* is a complex number z which satisfies the equation $z^n = 1$ for some positive integer n. Let $\omega_n = e^{2\pi i/n}$ be an nth root of unity. All the nth roots of unity form a group under multiplication. It is a cyclic group, generated by ω_n, which is called a *primitive root of unity*. The term "primitive" exactly refers to being a generator of the cyclic group, namely an nth root of unity is primitive when there is no positive integer k smaller than n such that $\omega_n^k = 1$. See Fig. 4.4 for $n = 5$.

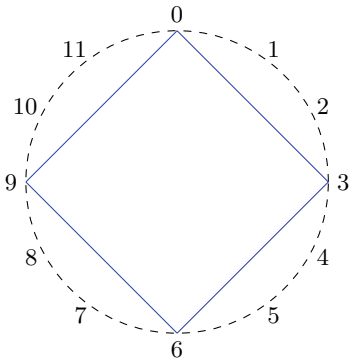

Fig. 4.3 An example of string art to show that 3 is not a generator of $\mathbb{Z}_{12}$

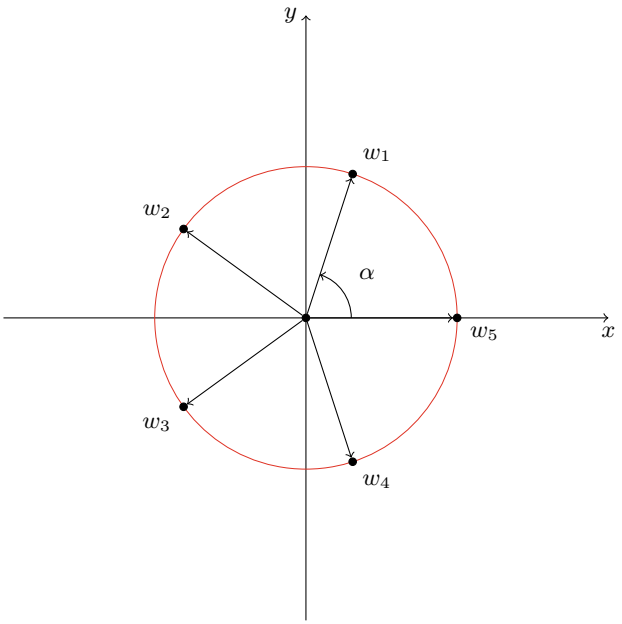

Fig. 4.4 5th roots of unity, where $\alpha = \dfrac{2\pi}{5}$

Definition 4.19 The *order of an element* a in a group G is the least positive integer n such that $a^n = e$. In additive notation this would be $na = 0$. If no such integer exist, then we say a has *infinite order*. The order of an element a is denoted by $o(a)$.

Note that the critical part of Definition 4.19 is that the order is the *least* positive integer with the given property. The terminology *order* is used both for groups and group elements, but it is usually clear from the context which one is considered.

So, to find the order of an element a we need only compute the series of products $a,\ a^2,\ a^3, \ldots$ until we first reach the identity. If the identity never appears in the series, then a has infinite order.

Definition 4.20 A *torsion group* is a group all of whose elements have finite order. On the other hand, a group is said to be *torsion-free* if all its non-identity elements have infinite order.

Lemma 4.21 *Let $a \neq e$ be an element of a group G. If n is the order of a and $a^k = e$ for some integer k, then n divides k.*

Proof By the Division algorithm, there exist integers q and r such that $k = qn + r$ and r is strictly smaller than n. So, we have

$$e = a^k = a^{nq+r} = a^{nq}a^r.$$

Since a has order n, it follows that $a^{nq} = (a^n)^q = e$. This implies that $a^r = e$, which contradicts our choice of n as the smallest positive integer for which a power of a is the identity, unless $r = 0$. In this case $k = nq$ and we conclude that n must divide k. ■

Theorem 4.22 *If $a \in G$ has order n, then*

$$o(a^k) = \frac{n}{(n, k)}.$$

Proof Suppose that $(n, k) = d$. Then, there exist integers u and v such that $k = ud$, $n = vd$ and $(u, v) = 1$. Now, we have

$$(a^k)^v = (a^{ud})^v = a^{uvd} = a^{un} = (a^n)^u = e.$$

Moreover, if $(a^k)^m = e$, then $n|km$. So, $vd|udm$, or equivalently $v|um$. Since $(u, v) = 1$, by Euclid's lemma we conclude that $v|m$. Therefore, we obtain $o(a^k) = n/d$. ■

We now turn to some results about cyclic groups.

Theorem 4.23 *Every cyclic group is abelian.*

Proof Suppose that G is a cyclic group. By definition, there exists $a \in G$ such that $G = \langle a \rangle$. We need to show that $xy = yx$, for all $x, y \in G$. Now, x and y are of the form x^m and y^n, for some integers m and n, respectively. Moreover, we have

$$xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = yx,$$

as desired. ■

Theorem 4.24 *Every subgroup of a cyclic group is also cyclic.*

Proof Let $G = \langle a \rangle$ be our cyclic group and suppose that H is a subgroup of G. We must show that H is cyclic. If it consists of the identity alone, then it is trivial subgroup and there is nothing to prove. So, we may assume that $H \neq \{e\}$. We consider the set

$$S = \{s \in \mathbb{N} \mid a^s \in H\}.$$

Since H is non-trivial, it follows that S is non-empty. But being a non-empty subset of positive integers, S must have the least positive integer, call it k. We next claim that $H = \langle a^k \rangle$. In order to prove this claim, it suffices to let h be an arbitrary element of H and show that $h \in \langle a^k \rangle$. Since $h \in G = \langle a \rangle$, it follows that $h = a^m$, for some integer m. We now invoke the Division algorithm to m and k to obtain integers q and r such that $m = kq + r$, where $0 \leq r < k$. Therefore, we have

$$h = a^m = a^{kq+r} = a^{kq}a^r.$$

This implies that

$$a^r = a^{-kq}a^m.$$

As a^k belongs to H, so does a^{-kq}. By closure property of a subgroup, we know that $a^{-kq}a^m = a^r$ belongs to H. As r is strictly smaller than k, it contradicts the choice of k as the smallest element of S, unless $r = 0$. This proves that $h = a^{qk} = (a^k)^q \in \langle a^k \rangle = H$. ■

Remark 4.25 Theorem 4.24 tells us that all subgroups of additive group $\mathbb{Z}$ are of the form $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$.

Theorem 4.26 *Let G be a finite cyclic group generated by a.*

(1) *The generator a has finite order;*
(2) *If $o(a) = n$, then the elements a^k with $k = 0, 1, \ldots, n-1$ are all distinct and*

$$G = \{e,\ a,\ a^2,\ \ldots, a^{n-1}\}.$$

Proof Since G is cyclic, it follows that

$$G = \langle a \rangle = \{\ldots,\ a^{-2},\ a^{-1},\ e,\ a,\ a^2, \ldots\}.$$

Since G is finite, it follows that for some integers k and m we have $a^m = a^k$. This implies that $a^{m-k} = e$ and so a has finite order.

If $o(a) = n$, then we claim that $G = \{e,\ a,\ a^2,\ \ldots, a^{n-1}\}$. We see that for $0 \leq m < k \leq n-1$, the elements a^m and a^k are distinct as otherwise $a^{m-k} = e$ with $|m-k| < n$. Consequently, $\{e,\ a,\ a^2,\ \ldots, a^{n-1}\}$ is a subgroup of G containing n elements. Now, if x is an arbitrary element of G, then $x = a^j$, for some integer j. If $j > 0$, then applying the Division algorithm, we obtain $a^j = a^r$, where $0 \leq r < n-1$. If $j < 0$ and $s = -j$, then we can make $a^s = a^r$, for some $r < n$ and $a^j = a^{-s} = (a^s)^{-1} = (a^r)^{-1} = a^{n-r}$. This yields that $G = \{e,\ a,\ a^2,\ \ldots, a^{n-1}\}$.

Therefore, we conclude that the cyclic group generated by an element of order n has precisely n elements. ■

Corollary 4.27 *Let G be a group and a be an element of G. Then,*

$$o(a) = |\langle a \rangle|.$$

Corollary 4.28 *Let G be a finite group of order n. Then, G is cyclic if and only if there exists an element of G of order n.*

Corollary 4.29 *If G is an infinite cyclic group, then G has an infinite number of subgroups.*

Proof If $G = \langle a \rangle$, then $\langle a^n \rangle \neq \langle a^m \rangle$, for each integer $n \neq m$. ■

Theorem 4.30 *Let G be a cyclic group of order n generated by a and let k be a positive integer. If $d = (n, k)$, then x^k and x^d generate the same cyclic subgroup of G.*

Proof If $d = (n, k)$, we show that a^k and a^d are both powers of each other. Since $d|k$, it follows that $a^k = (x^d)^{k/d}$. On the other hand, since $d = (k, n)$, it follows that $d = kr + ns$, for some $r, s \in \mathbb{Z}$. This implies that $a^d = a^{kr+ns} = a^{kr}a^{ns} = a^{kr} = (a^k)^r$. This yields that a^k and a^d generate the same subgroup of G. ■

Theorem 4.31 *Let G be a cyclic group of order n. Then, for each m dividing n, G has a unique subgroup of order m, namely $\langle a^{n/m} \rangle$.*

Proof If $k = n/m$, then $(a^k)^m = (a^{n/m})^m = a^n = e$ and no smaller positive integer power of a^k could be e. So, $\langle a^k \rangle$ is a subgroup of order m. Next, we show that $\langle a^k \rangle$ is the only subgroup of order m. In order to do this, let H be an arbitrary subgroup of G of order m. By the proof of Theorem 4.24, we have $H = \langle a^d \rangle$, where d is the smallest positive integer such that a^d is in H. We apply the Division algorithm to obtain integers q and r such that $n = dq + r$ and $0 \leq r < d$. Then, we have $e = a^n = a^{dq+r} = (a^d)^q a^r$. This implies that $a^r = (a^d)^{-q} \in H$. Consequently, $r = 0$ and so $n = dq$. Moreover, we have

$$m = |H| = |\langle a^d \rangle| = \frac{n}{d}.$$

Therefore, we obtain $d = n/m = k$, i.e., $H = \langle a^d \rangle = \langle a^k \rangle$. This completes the proof. ■

Theorem 4.32 (Generators of a Finite Cyclic Group) *Let G be a cyclic group of order n generated by a. Then, $G = \langle a^k \rangle$ if and only if k and n are relatively prime.*

Proof Suppose that k and n are relatively prime. Then, we may write $1 = kx + ny$, for some integers x and y. Then, we have

$$a = a^{kx+ny} = a^{kx}a^{ny} = a^{kx} = (a^k)^x.$$

This implies that a belongs to $\langle a^k \rangle$, and so all powers of a belong to $\langle a^k \rangle$. Thus, we conclude that $G = \langle a^k \rangle$ and a^k is a generator of G.

Conversely, suppose that k and n are not relatively prime. Then, there exists an integer $d > 1$ such that $d|n$ and $d|k$. Hence, there exist integers m and r such that $n = md$ and $k = dr$. So, we get

$$(a^k)^m = a^{drm} = a^{rn} = (a^n)^r = e.$$

Since $d > 1$, it follows that $m < n$. This shows that a^k is not a generator of G. ■

Corollary 4.33 *Let G be a cyclic group of order n generated by a. Then, G has $\phi(n)$ generators.*

Corollary 4.34 *Let k be a positive integer. Then, k is a generator of $\mathbb{Z}_n$ if and only if k and n are relatively prime.*

Theorem 4.35 *Let G be a cyclic group of order n generated by a. If d is a positive divisor of n, then the number of elements of order d is $\phi(d)$.*

Proof By Theorem 4.31, there exists exactly one subgroup of order d, say $\langle b \rangle$. Then, every element of order d generates $\langle b \rangle$. On the other hand, by Theorem 4.32, an element b^k generates $\langle b \rangle$ if and only if $(k, d) = 1$. The number of such elements is $\varphi(d)$. ■

Theorem 4.36 *Every infinite cyclic group has exactly two generators.*

Proof Suppose that a is a generator of the infinite cyclic group G. Then, we have $G = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\}$. Now, if $a^k \in G$ is another generator of G, then $G = \{\ldots, a^{-2k}, a^{-k}, e, a^k, a^{2k}, \ldots\}$. Since $a^{k+1} \in G$, it follows that there exists an integer m such that $a^{k+1} = a^{km}$. This implies that $a^{k(1-m)+1} = e$. Since G is infinite, it follows that $k(m-1) + 1 = 0$, or equivalently $k(m-1) = 1$. This yields that $k = \pm 1$. Consequently, if a is a generator of G, then another generator of G is only a^{-1}. ■

For any finite group G, let $\theta_G(d)$ be the number of elements of G of order d. Then, it is clear that

$$|G| = \sum_{d=1}^{|G|} \theta_G(d).$$

Theorem 4.37 *In a finite group (not necessary cyclic), $\theta_G(d)$ is divisible by $\varphi(d)$.*

Proof Let G be a finite group. If G has no element of order d, then $\varphi(d)|0 = \theta_G(d)$ and we are done. So, suppose that there is $a \in G$ such that $o(a) = d$. By Theorem 4.35, $\langle a \rangle$ has $\varphi(d)$ elements of order d. Now, if all elements of order d belong to $\langle a \rangle$, we are done. Hence, suppose that $x \in G$ such that $o(x) = d$ and $x \in \langle a \rangle$.

Then, $\langle x \rangle$ has $\varphi(d)$ elements of order d too. Next, if $\langle a \rangle$ and $\langle x \rangle$ have no elements of order d in common, we have found $2\varphi(d)$ elements of order d. Note that if there is $y \in \langle a \rangle \cap \langle x \rangle$ with $o(y) = d$, then we obtain $\langle a \rangle = \langle x \rangle = \langle y \rangle$, and this is a contradiction. Continuing, we conclude that the number of elements of order d is a multiple of $\varphi(d)$. ■

Exercises

1. Draw the Hasse diagram for a cyclic group of order 30.
2. Show that the elements of finite order in an abelian group G form a subgroup of G.
3. Let U_{24} be the group of invertible elements in $\mathbb{Z}_{24}$. Find all cyclic subgroups of U_{24}.
4. Find an example of a non-cyclic group, all of whose proper subgroups are cyclic.
5. Find a collection of distinct subgroups $\langle a_1 \rangle, \langle a_2 \rangle, \ldots, \langle a_n \rangle$ with the property that $\langle a_1 \rangle \leq \langle a_2 \rangle \leq \ldots \leq \langle a_n \rangle$ with n as large as possible.
6. Let G be a group and $a, b \in G$. Prove that
   (a) $o(a) = o(a^{-1})$;
   (b) $o(ab) = o(ba)$;
   (c) $o(a) = o(g^{-1}ag)$, for all $g \in G$;
   (d) If $ab = ba$, and $o(a)$ and $o(b)$ are relatively prime, then $o(ab) = o(a)o(b)$.
7. If a cyclic group has an element of infinite order, how many elements of finite order does it have?
8. Give an example of a group that has exactly 6 subgroups (including the trivial subgroup and the group itself). Generalize to exactly n subgroups for any positive integer n.
9. If G is an abelian group and contains cyclic subgroups of orders 4 and 5, what other sizes of cyclic subgroups must G contain? Generalize.
10. If G is an abelian group and contains a pair of cyclic subgroups of order 2, show that G must contain a subgroup of order 4. Must this subgroup be cyclic?
11. Let G be an abelian group. Show that the elements of finite order in G form a subgroup. This subgroup is called the *torsion subgroup* of G.
12. Find the torsion subgroup of the multiplicative group $\mathbb{R}^*$ of non-zero real numbers.
13. Find the torsion subgroup T of the multiplicative group $\mathbb{C}^*$ of non-zero complex numbers.
14. Let G be an abelian group of order mn such that m and n are relatively prime. If there exists $a, b \in G$ such that $o(a) = m$ and $o(b) = n$, prove that G is cyclic.
15. Show that both U_{25} and U_{27} are cyclic groups.
16. Prove that U_{2^n} $(n \geq 3)$ is not cyclic.
17. Let a and b be elements of a group. If $o(a) = m$, $o(b) = n$, and m and n are relatively prime, show that $\langle a \rangle \cap \langle b \rangle = \{e\}$.

18. Suppose that $o(x) = n$. Find a necessary and sufficient condition on r and s such that $\langle x^r \rangle \leq \langle x^s \rangle$.
19. Suppose that $o(x) = n$. Show that $\langle x^r \rangle = \langle x^s \rangle$ if and only if $(n, r) = (n, s)$.
20. Suppose that a is a group element such that $o(a^{28}) = 10$ and $o(a^{22}) = 20$. Determine $o(a)$.
21. Determine the Hasse diagram for subgroups of $\mathbb{Z}_{p^2q}$, where p and q are distinct.
22. Give an example of a group and elements $a, b \in G$ such that $o(a)$ and $o(b)$ are finite but $o(ab)$ is not of finite order.

4.3 Generating Sets

We are interested in answering the following questions: What is the smallest subgroup of a group G containing elements $x_1, \ldots, x_n \in G$? How can we describe an arbitrary element in this subgroup? Or, more generally, what is the smallest subgroup of a group G containing a subset A of G and how can we describe an arbitrary element in this subgroup?

Definition 4.38 Let G be a group and A be a subset of G. Let $\{H_i \mid i \in I\}$ be the family of all subgroups of G which contain A. Then

$$\bigcap_{i \in I} H_i$$

is called the *subgroup of G generated by the set A* and denoted by $\langle A \rangle$.

Indeed, $\langle A \rangle$ is the smallest subgroup of G that contains A. The elements of A are the generators of the subgroup $\langle A \rangle$, which may also be generated by other subsets. If $A = \{x_1, \ldots, x_n\}$, then we write $\langle x_1, \ldots, x_n \rangle$ instead of $\langle A \rangle$. If $G = \langle x_1, \ldots, x_n \rangle$, then G is said to be *finitely generated*.

Remark 4.39 If $A = \{a\}$, then $G = \langle a \rangle$ is a cyclic group.

Theorem 4.40 *If G is a group and A is a non-empty subset of G, then*

$$\langle A \rangle = \{x_1^{\alpha_1} \ldots x_n^{\alpha_n} \mid x_i \in A,\ \alpha_i \in \mathbb{Z},\ 1 \leq i \leq n,\ n \in \mathbb{N}\}.$$

Proof Let

$$H = \{x_1^{\alpha_1} \ldots x_n^{\alpha_n} \mid x_i \in A,\ \alpha_i \in \mathbb{Z},\ 1 \leq i \leq n,\ n \in \mathbb{N}\}.$$

Clearly, H is a non-empty subset of G. Suppose that x and y are two arbitrary elements of H. Then, there exist $x_1, \ldots, x_n, y_1, \ldots, y_m \in A$ and $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m \in \mathbb{Z}$ such that

$$x = x_1^{\alpha_1} \ldots x_n^{\alpha_n} \text{ and } y = y_1^{\beta_1} \ldots y_m^{\beta_m}.$$

Hence, we obtain

$$xy^{-1} = x_1^{\alpha_1} \dots x_n^{\alpha_n} y_m^{-\beta_m} \dots y_1^{-\beta_1} \in H.$$

Thus, H is a subgroup of G. Moreover, $A \subseteq H$. Consequently, by the definition of $\langle A \rangle$, we conclude that $\langle A \rangle \subseteq H$.

On the other hand, since $\langle A \rangle$ is a subgroup of G, it follows that all elements of the form $x_1^{\alpha_1} \dots x_n^{\alpha_n}$ (for $x_i \in A$ and $\alpha_i \in \mathbb{Z}$) belong to $\langle A \rangle$. This yields that $H \subseteq \langle A \rangle$. Therefore, we deduce that $\langle A \rangle = H$. ■

Remark 4.41 If G is an additive group and A is a non-empty subset of G, then

$$\langle A \rangle = \{\alpha_1 x_1 + \dots \alpha_n x_n \mid x_i \in A,\ \alpha_i \in \mathbb{Z},\ 1 \leq i \leq n,\ n \in \mathbb{N}\}.$$

Example 4.42 Every finite group is finitely generated since $G = \langle G \rangle$.

Example 4.43 The additive group $\mathbb{Q}$ is not finitely generated: a finite set of rational numbers has a common denominator, say m, and the subgroup of $\mathbb{Q}$ generated by these rational numbers (their integral multiples and sums thereof) will only give rise to rational numbers with denominators dividing m. Not all rationales have such denominators (try $\frac{1}{m+1}$), so $\mathbb{Q}$ does not have a finite set of generators as an additive group.

Example 4.44 A finitely generated group is at most countable, so an uncountable group is not finitely generated. For example, the group of real numbers under addition is not finitely generated.

If G is a group and $\{H_i \mid i \in I\}$ is a family of subgroups of G, then $\bigcup_{i \in I} H_i$ is not a subgroup of G in general. The subgroup $\langle \bigcup_{i \in I} H_i \rangle$ generated by the set $\bigcup_{i \in I} H_i$ is called the *subgroup generated by groups* $\{H_i \mid i \in I\}$. If H and K are subgroups of G, then the subgroup $\langle H \cup K \rangle$ generated by H and K is called the *join* of H and K and is denote by $H \vee K$.

Theorem 4.45 *If G is a group, A is a subgroup of $Z(G)$, the center of G, and $z \in G$, then $\langle A \cup \{z\} \rangle$, the subgroup generated by A and z, is abelian.*

Proof Let $H = \langle A \cup \{z\} \rangle$ and y be an arbitrary element of H. First, we show that $y = az^k$, for some $a \in A$ and integer k. By Theorem 4.40, we can write $y = a_1 a_2 \dots a_n$, where for each $1 \leq i \leq n$, $a_i \in A$, $a_i = z$ or $a_i = z^{-1}$. Since A is a subgroup of $Z(G)$, it follows that $a_1, a_2, \dots, a_n$ commute. We set all a_is that belong to A on the left side and hence other elements will be z or z^{-1}. If a is the product of a_is that are in A, then $y = az^k$ for some integer k.

Now, suppose that x and y are two arbitrary elements of H. Then, we have

$$x = a_1 z^{k_1} \text{ and } y = a_2 z^{k_2},$$

for some $a_1, a_2 \in A$ and integers k_1, k_2. Thus, we obtain

$$\begin{aligned} xy &= (a_1 z^{k_1}) a_2 z^{k_2} \\ &= a_2 (a_1 z^{k_1}) z^{k_2} \\ &= a_2 a_1 z^{k_2} z^{k_1} \\ &= a_2 z^{k_2} a_1 z^{k_1} \\ &= yx. \end{aligned}$$

This yields that H is an abelian subgroup of H. ■

Exercises

1. In $(\mathbb{Z}, +)$, determine the subgroup generated by
   (a) $\{4,\ 6\}$;
   (b) $\{4,\ 5\}$.
2. Let G be a group and X be a non-empty subset of G. For every $a \in G$, prove that $\langle a^{-1} X a \rangle = a^{-1} \langle X \rangle a$.
3. Prove that group generated by $G \setminus H$ equals G, where H is a proper subgroup of G.
4. Let G be an abelian group and $A = \{a_1, \ldots, a_n\}$ be a finite subset of G. If the order of each element of A is finite, prove that $\langle A \rangle$ is a finite subgroup of G.
5. Suppose that G is a group containing subgroups H and K. Show that $H \cup K = H \vee K$ if and only if $H \cap K \in \{H,\ K\}$.
6. Show that there is a group G containing subgroups H, K, L such that $H \cup K \cup L = H \vee K \vee L$ but $H \cap K \cap L \notin \{H,\ K,\ L\}$.

4.4 Worked-Out Problems

Problem 4.46 Let G be an abelian group and $x, y \in G$ be of finite orders.

(1) Show that $o(xy) | [o(x), o(y)]$, where $[o(x), o(y)]$ stands for least common multiple;
(2) Give an example to illustrate that $o(xy) \neq [o(x), o(y)]$, in general.

Solution (1) Assume that x and y are two elements of orders m and n, respectively. Let $[m, n] = r$. Then, we have $r = mm' = nn'$, and hence

$$x^r y^r = (x^m)^{m'} (y^n)^{n'} = e.$$

Now, suppose that $o(xy) = k$, then k is the smallest positive integer k such that $(xy)^k = e$. Since G is abelian, it follows that

$$(xy)^r = x^r y^r = e \text{ and } (xy)^k = x^k y^k = e.$$

This shows that $(xy)^k = (xy)^r = e$. Since $o(xy) = k$, we conclude that $k|r$. This completes the proof.

(2) For this part, let x be a non-identity element of G and let $y = x^{-1}$. Then, it is clear that $1 = o(e) = o(xx^{-1}) = o(xy) \neq [o(x), o(y)]$. ■

Problem 4.47 Prove that a group is finite if and only if it has only finitely many subgroups.

Solution Suppose that G is a finite group of order n. Since the number of subsets of G is 2^n, it follows that the number of subgroups of G is less than 2^n.

Conversely, suppose that the number of subgroups of G is finite. Let $a \in G$ be an arbitrary element. We claim that $\langle a \rangle$ is finite. If $\langle a \rangle$ is an infinite group, then the order of a is infinite. Now, for each positive integer k, let $H_k = \langle a^k \rangle$. We prove H_ks are distinct. Indeed, if $H_i = H_j$, for some positive integers m and n, then $a^i \in \langle a^j \rangle$ and $a^j \in \langle a^i \rangle$. So, there exist integers r and s such that $a^i = a^{jr}$ and $a^j = a^{is}$. This yields that $a^{i-jr} = e$ and $a^{j-is} = e$. Since the order of a is infinite, it follows that $i - jr = 0$ and $j - is = 0$, or $i|j$ and $j|i$. Hence, $i = j$. Consequently, H_ks are distinct. This means that G has many infinitely subgroups, and it is a contradiction. Therefore, $\langle a \rangle$ is finite, for every $a \in G$. Since

$$G = \bigcup_{a \in G} \langle a \rangle$$

and the number of subgroups of G is finite, we conclude that

$$G = \langle a_1 \rangle \cup \langle a_2 \rangle \cup \ldots \cup \langle a_n \rangle.$$

Since the finite union of finite sets is finite, it follows that G is finite. ■

4.5 Supplementary Exercises

1. Let $G = \{a_1, a_2, \ldots, a_n\}$ be a finite abelian group of order n and $x = a_1 a_2 \ldots a_n$ be the product of all the elements in G. Show that $x^2 = e$.
2. Suppose that the elements x, y in the group G satisfy the relation $xyx^{-1} = y^2$, where y is a non-identity element.
   (a) Show that $x^5 y x^{-5} = y^{32}$;
   (b) If $o(x) = 5$, compute $o(y)$.
3. Let G be the collection of all rational numbers x which satisfy $0 \leq x < 1$. Show that the binary operation

$$x \oplus y = \begin{cases} x + y & \text{if } 0 \leq x + y < 1 \\ x + y - 1 & \text{if } x + y \geq 1. \end{cases}$$

makes G into an infinite abelian group all of whose elements have finite order.

4. Let G be a group and $x \in G$ such that $o(x) = mn$, where m and n are positive integers and relatively prime. Show that one can write $x = ab$, where $o(a) = m$, $o(b) = n$ and $ab = ba$. Moreover, prove the uniqueness of such a representation.
5. Give an example of an infinite group that has exactly two elements of order 4.
6. For every integer n greater than 2, prove that the group U_{n^2-1} is not cyclic.
7. Let G be an abelian and suppose that G has elements of orders m and n, respectively. Prove that G has an element whose order is the least common multiple of m and n.
8. Let G be a finite group. Prove that the following conditions are equivalent:

   (a) G is cyclic and $|G| = p^n$, where p is prime and n is a non-negative integer;
   (b) If A and B are subgroups of G, then $A \leq B$ or $B \leq A$.

9. Prove that the additive group of all rational numbers is a torsion-free group and, further, that it can be represented as a union of an ascending chain of cyclic subgroups.
10. Suppose that G is a finitely generated group and that $G = \langle Y \rangle$, where Y is not necessarily a finite set. Prove that there is a finite subset X of Y such that $G = \langle X \rangle$.
11. Prove that a group G is finitely generated if and only if any increasing sequence $H_1 \leq H_2 \leq \ldots$ of subgroups of G stabilizes, i.e., $H_i = H_j$ for $i, j \geq k$ starting from some k.