1.3 Cyclic Groups

In this section we concentrate on the study of groups of a special kind, called *cyclic groups*. They will later be seen to be the building blocks out of which all finite Abelian groups can be constructed. We have already introduced (in Proposition 1.2.17) the notion of the cyclic subgroup $\langle a \rangle$ of a group G generated by an element a. We begin by reviewing some examples involving that notion.

1.3.1 EXAMPLE We have already observed that in $\mathbb{Z}_6$ the subgroup generated by 1 is the whole group, as is the subgroup generated by 5: $\mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle$. ◇

1.3.2 EXAMPLE Likewise, in $\mathbb{Z}$ the subgroup generated by 1 or by -1 is the whole group: $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. ◇

1.3.3 EXAMPLE Likewise, in $G = \{1, i, -1, -i\}$, the subgroup generated by i is the whole group, since $i^2 = -1$, $i^3 = -i$, $i^4 = 1$. ◇

These are examples of the notion of a cyclic group introduced in the next definition.

1.3.4 DEFINITION A group G is called **cyclic** if there exists an element $a \in G$ such that $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. Any such element is called a **generator** of G. ○

When the group operation is being written as addition, the condition $G = \{a^n \mid n \in \mathbb{Z}\}$ is written $G = \{na \mid n \in \mathbb{Z}\}$. When we calculate $\langle a \rangle$ for an element a of a group G, we calculate the successive powers of a, or when the group operation is written as addition, the successive multiples of a. If these give all the elements of G, then G is generated by a.

1.3.5 EXAMPLE For any $n > 1$, $\mathbb{Z}_n = \langle 1 \rangle = \langle n - 1 \rangle$. This is a cyclic group of order n. ◇

1.3.6 EXAMPLE $\mathbb{Z}_{10} = \langle 1 \rangle = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle$ or, in other words, 1, 3, 7, and 9 are all generators of $\mathbb{Z}_{10}$. We verify this for 7 by computing its successive multiples. (The case of 3 is similar and the cases of 1 and 9 were included already in the preceding example.) We have $2 \cdot 7 = 7 + 7 = 4$, since $14 \equiv 4 \bmod 10$. Likewise $3 \cdot 7 = 7 + 7 + 7 = 1$, since $21 \equiv 1 \bmod 10$. Similarly, $4 \cdot 7 = 8$, $5 \cdot 7 = 5$, $6 \cdot 7 = 2$, $8 \cdot 7 = 6$, $9 \cdot 7 = 3$, $10 \cdot 7 = 0$. ◇

1.3.7 EXAMPLE $U(10) = \{1, 3, 7, 9\} = \{3^0, 3^1, 3^2, 3^3\} = \langle 3 \rangle$. ◇

We have also encountered some examples of groups that are not cyclic.

1.3.8 EXAMPLE In S_3, $\langle \rho \rangle = \langle \rho^2 \rangle = \{\rho_0, \rho, \rho^2\}$, while $\langle \mu_i \rangle = \{\rho_0, \mu_i\}$ for $i = 1, 2, 3$. Hence none of the elements of S_3 generates the whole group, and S_3 is not cyclic. ◇

1.3.9 EXAMPLE $2\mathbb{Z} = \langle 2 \rangle$ and, in general, for any $n \geq 1$, $n\mathbb{Z} = \langle n \rangle$. These are all infinite cyclic groups. ◇

1.3.10 EXAMPLE $\mathbb{Z}_{10} \neq \{0, 2, 4\} = \langle 2 \rangle$. We verify this by computing successive multiples. We have $2 \cdot 2 = 2 + 2 = 4$, $3 \cdot 2 = 2 + 2 + 2 = 6$, $4 \cdot 2 = 8$, $5 \cdot 2 = 0$, $6 \cdot 2 = 2$, $7 \cdot 2 = 4$, $8 \cdot 2 = 6$, $9 \cdot 2 = 8$, $10 \cdot 2 = 0$, and the pattern repeats. ◇

The next theorem tells us that the kind of repetition seen in the preceding example happens generally.

1.3.11 THEOREM Let G be a group and $a \in G$. Then for all $i, j \in \mathbb{Z}$ we have

(1) If a has infinite order, then $a^i = a^j$ if and only if $i = j$.

(2) If a has finite order $|a| = n$, then $a^i = a^j$ if and only if n divides $i - j$.

Proof (1) Suppose a has infinite order. For one direction, if $i = j$, then clearly $a^i = a^j$. For the other direction, if $a^i = a^j$, then $a^{i-j} = a^i a^{-j} = e$. But since a has infinite order, $a^n = e$ if and only if $n = 0$, so we have $i - j = 0$ or $i = j$.

(2) Suppose a has finite order $|a| = n$. For one direction, if n divides $i - j$, so that $i = nk + j$ for some $k \in \mathbb{Z}$, then we have $a^i = a^{nk+j} = a^{nk}a^j = (a^n)^k a^j = e^k a^j = ea^j = a^j$. For the other direction, suppose $a^i = a^j$ or, equivalently, $a^{i-j} = e$. By the division algorithm we can write $i - j = qn + r$, where $0 \leq r < n$. Then $e = a^{i-j} = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r = e^q a^r = ea^r = a^r$. Since $0 \leq r < n$ and n is by definition the *least* positive integer such that $a^n = e$, we must have $r = 0$, so $i - j = qn$ and $i - j$ is divisible by n. □

We leave the proofs of the following three corollaries to the reader. (See Exercises 13 through 15.)

1.3.12 COROLLARY Let G be a group and $a \in G$ an element of finite order $|a| = n$. Then for any $k \in \mathbb{Z}$, $a^k = e$ if and only if n divides k. □

1.3.13 COROLLARY Let G be a group and $a \in G$ an element of finite order $|a| = n$. Then $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$. □

1.3.14 COROLLARY Let G be a group and $a \in G$ an element of finite order. Then $|\langle a \rangle| = |a|$. □

1.3.15 EXAMPLE Let G be a cyclic group of order 6, $G = \langle a \rangle = \{e, a, a^2, a^3, a^4, a^5\}$. Let us find $|a^4|$. We have $(a^4)^2 = a^8 = a^{6+2} = a^6a^2 = ea^2 = a^2 \neq e$, while $(a^4)^3 = a^{12} = a^{6+6} = a^{6 \cdot 2} = (a^6)^2 = e^2 = e$. Hence $|a^4| = 3$. ◇

The next theorem gives a formula enabling us to find the orders of elements of a cyclic group more easily.

1.3.16 THEOREM Let $G = \langle a \rangle$ be a cyclic group with generator a, of order $|G| = |a| = n$. Then for any element $a^s \in G$ we have $|a^s| = n / \gcd(n, s)$.

Proof By Corollary 1.3.12, $(a^s)^k = a^{sk} = e$ if and only if sk is a multiple of n. Since the order $|a^s|$ is by definition the least k such that $(a^s)^k = e$, it follows that the order $|a^s|$ is the least k such that the multiple sk of s is also a multiple of n or, equivalently, sk is the least positive integer that is a multiple of n as well as of s. This is to say that $sk = \text{lcm}(n, s)$ and $k = \text{lcm}(n, s)/s$. Since $\text{lcm}(a, b) = ab/\text{gcd}(a, b)$ by Proposition 0.3.29, part (3), we have $k = sn/s\text{gcd}(n, s) = n/\text{gcd}(n, s)$. □

1.3.17 EXAMPLE In a cyclic group $G = \langle a \rangle$ of order 210, the order of a^{80} is $|a^{80}| = 210/\text{gcd}(210, 80) = 210/10 = 21$. ◇

1.3.18 EXAMPLE In $\mathbb{Z}_{105}$, the order of 84 is $|84| = 105/\text{gcd}(105, 84) = 105/21 = 5$. ◇

The theorem can be used not only to simplify the calculations of orders of arbitrary elements of a cyclic group, as in the preceding examples, but also, as in the next example, to find all generators of the group.

1.3.19 EXAMPLE Consider $\mathbb{Z}_{12}$ and let us find all its generators, which is to say all elements $s \in \mathbb{Z}_{12}$ such that $|s| = 12$. By Theorem 1.3.16, $|s| = 12/\text{gcd}(12, s)$. So $|s| = 12$ if and only if $\text{gcd}(12, s) = 1$. Thus the generators of $\mathbb{Z}_{12}$ are the elements $s \in \mathbb{Z}_{12}$ such that $\text{gcd}(12, s) = 1$, namely, the elements $s = 1, 5, 7$, or 11. ◇

1.3.20 COROLLARY Let $G = \langle a \rangle$ be a cyclic group with generator a, of order $|G| = |a| = n$. Then for any element $a^s \in G$, we have

$$a^s \text{ is a generator of } G \text{ if and only if } \text{gcd}(n, s) = 1$$

Proof By definition, a^s is a generator of G if and only if $G = \langle a^s \rangle$, and hence if and only if $|\langle a^s \rangle| = n$. By Corollary 1.3.14, $|\langle a^s \rangle| = |a^s|$, and by Theorem 1.3.16, $|a^s| = n/\text{gcd}(n, s)$. So a^s is a generator of G if and only if $n/\text{gcd}(n, s) = n$ or, equivalently, $\text{gcd}(n, s) = 1$. □

1.3.21 COROLLARY Let G be a cyclic group of order n. Then the number of generators of G is $\phi(n)$, where ϕ is the Euler function.

Proof This is immediate from the preceding corollary, since by definition $\phi(n)$ is the number of integers s, $1 \leq s < n$, such that $\text{gcd}(n, s) = 1$. □

The next example illustrates a property of cyclic groups that makes them especially easy to understand.

1.3.22 EXAMPLE Let us find all subgroups of $\mathbb{Z}_{15}$. To begin with we have the trivial subgroup $\langle 0 \rangle$. Let H be any nontrivial subgroup. By Corollary 1.3.20, if H contains any of the elements 1, 2, 4, 7, 8, 11, 13, 14, then H will be the improper subgroup $\mathbb{Z}_{15} = \langle 1 \rangle = \langle 2 \rangle = \langle 4 \rangle = \langle 7 \rangle = \langle 8 \rangle = \langle 11 \rangle = \langle 13 \rangle = \langle 14 \rangle$. Now let H be a nontrivial proper subgroup. First suppose $3 \in H$. Then for any $y \in H$, using the

division algorithm we can write $y = q3 + r$ for some r with $0 \leq r < 3$. Since $3, y \in H$, we have $r = y - q3 \in H$. But since H is proper, $1, 2 \notin H$. So we must have $r = 0$, and y is a multiple of 3. Thus $H = \langle 3 \rangle = \{0, 3, 6, 9, 12\} = 3\mathbb{Z}_{15}$. Since $6 + 6 + 6 = 9 + 9 = 12 + 12 + 12 + 12 = 3$, any nontrivial proper subgroup containing any of 6, 9, or 12 will also contain 3 and be equal to $3\mathbb{Z}_{15} = \langle 3 \rangle = \langle 6 \rangle = \langle 9 \rangle = \langle 12 \rangle$. Now suppose H is a nontrivial proper subgroup and $5 \in H$. A similar argument shows that $H = \langle 5 \rangle = \{0, 5, 10\} = 5\mathbb{Z}_{15}$, and that any proper subgroup containing 10 will also be equal to $5\mathbb{Z}_{15} = \langle 5 \rangle = \langle 10 \rangle$. Since we have accounted for all possible elements, we have found all possible subgroups. ◇

1.3.23 THEOREM Every subgroup of a cyclic group is cyclic.

Proof Let $G = \langle a \rangle$ be a cyclic group and H a subgroup of G. If H is the trivial subgroup $\{e\}$, then $H = \langle e \rangle$ and is cyclic. Now assume that H is nontrivial, so there exists an element $b \in H$ with $b \neq e$. Since $b \in G = \langle a \rangle$, $b = a^s$ for some integer s, and since $b \neq e$, $s \neq 0$. Also, since $b \in H$, $a^{-s} = (a^s)^{-1} = b^{-1} \in H$. Since one or the other of s or $-s$ is positive, H contains some positive power of a. Now let m be the least positive integer such that $a^m \in H$. Consider any other element $y \in H$. Then $y = a^n$ for some integer n. Applying the division algorithm to m and n, we can write $n = qm + r$ for some integers q, r with $0 \leq r < m$. Then $y = a^n = a^{qm + r} = a^{qm}a^r = (a^m)^q a^r$, and $a^r = y(a^m)^{-q}$. Since $y, a^m \in H$, it follows that $a^r \in H$. But since $0 \leq r < m$ and m is the least positive integer with $a^m \in H$, we must have $r = 0$, and $y = (a^m)^q$. Thus every element of H is a power of a^m and $H = \langle a^m \rangle$ is cyclic. □

1.3.24 COROLLARY The subgroups of $\mathbb{Z}$ are $n\mathbb{Z} = \langle n \rangle$ for all $n \geq 0$.

Proof $\mathbb{Z} = \langle 1 \rangle$ is cyclic; hence every subgroup H of $\mathbb{Z}$ is also cyclic by Theorem 1.3.23, and hence is of the form $H = \langle m \rangle$ for some integer m. Since $\langle -m \rangle = \langle m \rangle$, and either $m \geq 0$ or $-m \geq 0$, $H = \langle n \rangle = n\mathbb{Z}$ for some $n \geq 0$. □

1.3.25 EXAMPLE Since $\mathbb{Z}_{12}$ is cyclic, all the subgroups of $\mathbb{Z}_{12}$ are cyclic, and if $H = \langle s \rangle$ is a subgroup, then $|H| = |s| = 12/\gcd(12, s)$ and is a divisor of 12. Let us consider a divisor of 12, say 4, and find all subgroups H with $|H| = 4$. We know that $|3| = 12/\gcd(12, 3) = 12/3 = 4$, and hence $H = \langle 3 \rangle = \{0, 3, 6, 9\}$ is one subgroup of order 4. It is in fact the only subgroup of order 4, since the only other element of order 4 in $\mathbb{Z}_{12}$ is 9, and $\langle 9 \rangle = \langle 3 \rangle$. ◇

1.3.26 THEOREM Let $G = \langle a \rangle$ be a cyclic group of order n. Then

(1) The order $|H|$ of any subgroup H of G is a divisor of $n = |G|$.

(2) For each positive integer d that divides n there exists a unique subgroup of order d, the subgroup $H = \langle a^{n/d} \rangle$.

Proof (1) Let H be a subgroup of $G = \langle a \rangle$. By Theorem 1.3.23, $H = \langle a^m \rangle$ for some integer $m \geq 0$, and by Theorem 1.3.16, $|H| = |a^m| = n/\gcd(n, m)$, which is a divisor of n.

(2) Since $e \in H$ for any subgroup H of G, the only subgroup of G of order 1 is the trivial subgroup $\{e\} = \langle e \rangle$. Let d be a divisor of n, $d > 1$. Then by Theorem 1.3.16, $|a^{n/d}| = n/\gcd(n, n/d) = d$. Hence $\langle a^{n/d} \rangle$ is a subgroup of G of order d. What remains to be shown is that this is the only subgroup of G of order d. So let H be a subgroup of G of order $|H| = d$. As in the proof of Theorem 1.3.23, $H = \langle a^s \rangle$, where s is the smallest positive integer such that $a^s \in H$. We know from Theorem 0.3.16 that there are integers u, v such that $\gcd(n, s) = un + vs$. Therefore, $a^{\gcd(n,s)} = a^{un + vs} = (a^n)^u(a^s)^v = e(a^s)^v \in H$. Since $1 \leq \gcd(n, s) \leq s$ and s was the least positive integer with $a^s \in H$, we must have $\gcd(n, s) = s$. Then by Theorem 1.3.16, $d = |H| = |a^s| = n/\gcd(n, s) = n/s$, so that $s = n/d$ and $H = \langle a^s \rangle = \langle a^{n/d} \rangle$ as desired. □

1.3.27 EXAMPLE Using Theorem 1.3.26, all the subgroups of $\mathbb{Z}_{12}$ and their orders are as follows:

$\langle 0 \rangle$ has order 1	$\langle 6 \rangle$ has order 2	$\langle 4 \rangle$ has order 3
$\langle 3 \rangle$ has order 4	$\langle 2 \rangle$ has order 6	$\langle 1 \rangle = \mathbb{Z}_{12}$ has order 12

We can display these in a diagram of the **subgroup lattice** of the group as in Figure 6. This is a diagram showing how the various subgroups of the group are related. Lines in the diagram represent inclusion. Thus the diagram indicates that $\langle 3 \rangle$ includes $\langle 6 \rangle$ and that $\langle 6 \rangle$ includes $\langle 0 \rangle$. It also indicates that the intersection of $\langle 3 \rangle$ and $\langle 2 \rangle$ is $\langle 6 \rangle$, and that the intersection of $\langle 6 \rangle$ and $\langle 4 \rangle$ is $\langle 0 \rangle$. ◇

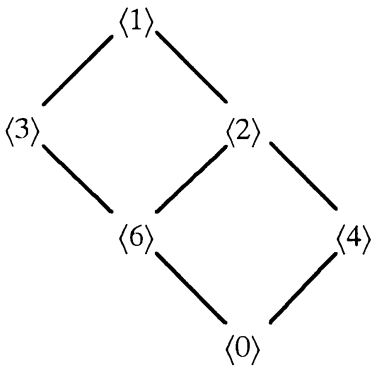

FIGURE 6

Exercises 1.3

1. Find the orders of the indicated elements in the indicated groups:

(a) $6 \in \mathbb{Z}_{10}$	(b) $6 \in \mathbb{Z}_{15}$	(c) $10 \in \mathbb{Z}_{42}$
(d) $77 \in \mathbb{Z}_{210}$	(e) $40 \in \mathbb{Z}_{210}$	(f) $70 \in \mathbb{Z}_{210}$

2. Let $G = \langle a \rangle$ be a cyclic group of order $|G| = 21$. Calculate the orders of a^2, a^6, a^8, a^9, a^{14}, a^{15}, a^{18}.