6

Abelian groups

This chapter introduces the notion of an abelian group. This is an abstraction that models many different algebraic structures, and yet despite the level of generality, a number of very useful results can be easily obtained.

6.1 Definitions, basic properties, and examples

Definition 6.1. *An **abelian group** is a set G together with a binary operation $\star$ on G such that:*

(i) for all $a, b, c \in G$, $a \star (b \star c) = (a \star b) \star c$ (i.e., $\star$ is associative);

*(ii) there exists $e \in G$ (called the **identity element**) such that for all $a \in G$, $a \star e = a = e \star a$;*

*(iii) for all $a \in G$ there exists $a' \in G$ (called the **inverse of** a) such that $a \star a' = e = a' \star a$;*

(iv) for all $a, b \in G$, $a \star b = b \star a$ (i.e., $\star$ is commutative).

While there is a more general notion of a **group**, which may be defined simply by dropping property (iv) in Definition 6.1, we shall not need this notion in this text. The restriction to abelian groups helps to simplify the discussion significantly. Because we will only be dealing with abelian groups, we may occasionally simply say "group" instead of "abelian group."

Before looking at examples, let us state some very basic properties of abelian groups that follow directly from the definition:

Theorem 6.2. *Let G be an abelian group with binary operation $\star$. Then we have:*

(i) G contains only one identity element;

(ii) every element of G has only one inverse.

Proof. Suppose e, e' are both identities. Then we have

$$e = e \star e' = e',$$

where we have used part (ii) of Definition 6.1, once with e' as the identity, and once with e as the identity. That proves part (i) of the theorem.

To prove part (ii) of the theorem, let $a \in G$, and suppose that a has two inverses, a' and a''. Then using parts (i)–(iii) of Definition 6.1, we have

$$\begin{aligned} a' &= a' \star e \ \text{(by part (ii))} \\ &= a' \star (a \star a'') \ \text{(by part (iii) with inverse } a'' \text{ of } a) \\ &= (a' \star a) \star a'' \ \text{(by part (i))} \\ &= e \star a'' \ \text{(by part (iii) with inverse } a' \text{ of } a) \\ &= a'' \ \text{(by part (ii))}. \ \square \end{aligned}$$

These uniqueness properties justify use of the definite article in Definition 6.1 in conjunction with the terms "identity element" and "inverse." Note that we never used part (iv) of the definition in the proof of the above theorem.

Abelian groups are lurking everywhere, as the following examples illustrate.

Example 6.1. The set of integers $\mathbb{Z}$ under addition forms an abelian group, with 0 being the identity, and $-a$ being the inverse of $a \in \mathbb{Z}$. $\square$

Example 6.2. For each integer n, the set $n\mathbb{Z} = \{nz : z \in \mathbb{Z}\}$ under addition forms an abelian group, again, with 0 being the identity, and $n(-z)$ being the inverse of nz. $\square$

Example 6.3. The set of non-negative integers under addition does not form an abelian group, since additive inverses do not exist for any positive integers. $\square$

Example 6.4. The set of integers under multiplication does not form an abelian group, since inverses do not exist for any integers other than ± 1. $\square$

Example 6.5. The set of integers $\{\pm 1\}$ under multiplication forms an abelian group, with 1 being the identity, and -1 its own inverse. $\square$

Example 6.6. The set of rational numbers $\mathbb{Q} = \{a/b : a, b \in \mathbb{Z},\ b \neq 0\}$ under addition forms an abelian group, with 0 being the identity, and $(-a)/b$ being the inverse of a/b. $\square$

Example 6.7. The set of non-zero rational numbers $\mathbb{Q}^*$ under multiplication forms an abelian group, with 1 being the identity, and b/a being the inverse of a/b. $\square$

Example 6.8. The set $\mathbb{Z}_n$ under addition forms an abelian group, where $[0]_n$ is the identity, and where $[-a]_n$ is the inverse of $[a]_n$. $\square$

Example 6.9. The set $\mathbb{Z}_n^*$ of residue classes $[a]_n$ with $\gcd(a, n) = 1$ under multiplication forms an abelian group, where $[1]_n$ is the identity, and if b is a multiplicative inverse of a modulo n, then $[b]_n$ is the inverse of $[a]_n$. □

Example 6.10. For every positive integer n, the set of n-bit strings under the "exclusive or" operation forms an abelian group, where the "all zero" bit string is the identity, and every bit string is its own inverse. □

Example 6.11. The set $\mathcal{F}^*$ of all arithmetic functions f, such that $f(1) \neq 0$, and with the Dirichlet product as the binary operation (see §2.9) forms an abelian group. The special function I is the identity, and inverses are guaranteed by Exercise 2.54. □

Example 6.12. The set of all finite bit strings under concatenation does not form an abelian group. Although concatenation is associative and the empty string acts as an identity element, inverses do not exist (except for the empty string), nor is concatenation commutative. □

Example 6.13. The set of 2×2 integer matrices with determinant ± 1, together with the binary operation of matrix multiplication, is an example of a *non-abelian* group; that is, it satisfies properties (i)–(iii) of Definition 6.1, but not property (iv). □

Example 6.14. The set of all permutations on a given set of size $n \geq 3$, together with the binary operation of function composition, is another example of a non-abelian group (for $n = 1, 2$, it is an abelian group). □

Consider an abelian group G with binary operation $\star$. Since the group operation is associative, for all $a_1, \ldots, a_k \in G$, we may write $a_1 \star \cdots \star a_k$ without parentheses, and there can be no ambiguity as to the value of such an expression: any explicit parenthesization of this expression yields the same value. Furthermore, since the group operation is commutative, reordering the a_i's does not change this value.

Note that in specifying a group, one must specify both the underlying set G as well as the binary operation; however, in practice, the binary operation is often implicit from context, and by abuse of notation, one often refers to G itself as the group. For example, when talking about the abelian groups $\mathbb{Z}$ and $\mathbb{Z}_n$, it is understood that the group operation is addition, while when talking about the abelian group $\mathbb{Z}_n^*$, it is understood that the group operation is multiplication.

Typically, instead of using a special symbol like "$\star$" for the group operation, one uses the usual addition ("$+$") or multiplication ("$\cdot$") operations.

Additive notation. If an abelian group G is written additively, using "$+$" as the group operation, then the identity element is denoted by 0_G (or just 0 if G is

clear from context), and is also called the **zero element**. The inverse of an element $a \in G$ is denoted by $-a$. For $a, b \in G$, $a - b$ denotes $a + (-b)$.

Multiplicative notation. If an abelian group G is written multiplicatively, using "$\cdot$" as the group operation, then the identity element is denoted by 1_G (or just 1 if G is clear from context). The inverse of an element $a \in G$ is denoted by a^{-1}. As usual, one may write ab in place of $a \cdot b$. Also, one may write a/b for ab^{-1}.

For any particular, concrete abelian group, the most natural choice of notation is clear (e.g., addition for $\mathbb{Z}$ and $\mathbb{Z}_n$, multiplication for $\mathbb{Z}_n^*$); however, for a "generic" group, the choice is largely a matter of taste. By convention, **whenever we consider a "generic" abelian group, we shall use *additive* notation for the group operation**, unless otherwise specified.

The next theorem states a few simple but useful properties of abelian groups (stated using our default, additive notation).

Theorem 6.3. *Let G be an abelian group. Then for all $a, b, c \in G$, we have:*

(i) if $a + b = a + c$, then $b = c$;

(ii) the equation $a + x = b$ has a unique solution $x \in G$;

(iii) $-(a + b) = (-a) + (-b)$;

(iv) $-(-a) = a$.

Proof. These statements all follow easily from Definition 6.1 and Theorem 6.2. For (i), just add $-a$ to both sides of the equation $a + b = a + c$. For (ii), the solution is $x = b - a$. For (iii), we have

$$(a + b) + ((-a) + (-b)) = (a + (-a)) + (b + (-b)) = 0_G + 0_G = 0_G,$$

which shows that $(-a) + (-b)$ is indeed the inverse of $a + b$. For (iv), we have $(-a) + a = 0_G$, which means that a is the inverse of $-a$. □

Part (i) of the above theorem is the **cancellation law** for abelian groups.

If $a_1, \ldots, a_k$ are elements of an abelian group G, we naturally write $\sum_{i=1}^k a_i$ for their sum $a_1 + \cdots + a_k$. By convention, the sum is 0_G when $k = 0$. Part (iii) of Theorem 6.3 obviously generalizes, so that $-\sum_{i=1}^k a_i = \sum_{i=1}^k (-a_i)$. In the special case where all the a_i's have the same value a, we define $k \cdot a := \sum_{i=1}^k a$, whose inverse is $k \cdot (-a)$, which we may write as $(-k) \cdot a$. Thus, the notation $k \cdot a$, or more simply, ka, is defined for all integers k. Observe that by definition, $1a = a$ and $(-1)a = -a$.

Theorem 6.4. *Let G be an abelian group. Then for all $a, b \in G$ and $k, \ell \in \mathbb{Z}$, we have:*

(i) $k(\ell a) = (k\ell)a = \ell(ka)$;

(ii) $(k+\ell)a = ka + \ell a$;

(iii) $k(a+b) = ka + kb$.

Proof. The proof of this is easy, but tedious. We leave the details as an exercise to the reader. □

Multiplicative notation: It is perhaps helpful to translate the above discussion from additive to multiplicative notation. If a group G is written using multiplicative notation, then Theorem 6.3 says that (i) $ab = ac$ implies $b = c$, (ii) $ax = b$ has a unique solution, (iii) $(ab)^{-1} = a^{-1}b^{-1}$, and (iv) $(a^{-1})^{-1} = a$. If $a_1, \ldots, a_k \in G$, we write their product $a_1 \cdots a_k$ as $\prod_{i=1}^{k} a_i$, which is 1_G when $k = 0$. We have $(\prod_{i=1}^{k} a_i)^{-1} = \prod_{i=1}^{k} a_i^{-1}$. We also define $a^k := \prod_{i=1}^{k} a$, and we have $(a^k)^{-1} = (a^{-1})^k$, which we may write as a^{-k}. Theorem 6.4 says that (i) $(a^\ell)^k = a^{k\ell} = (a^k)^\ell$, (ii) $a^{k+\ell} = a^k a^\ell$, and (iii) $(ab)^k = a^k b^k$.

An abelian group G may be **trivial**, meaning that it consists of just the zero element 0_G, with $0_G + 0_G = 0_G$. An abelian group G may be infinite or finite: if the group is finite, we define its **order** to be the number of elements in the underlying set G; otherwise, we say that the group has **infinite order**.

Example 6.15. The order of the additive group $\mathbb{Z}_n$ is n. If $n = 1$, then $\mathbb{Z}_n$ is the trivial group. □

Example 6.16. The order of the multiplicative group $\mathbb{Z}_n^*$ is $\varphi(n)$, where φ is Euler's phi function, defined in §2.6. □

Example 6.17. The additive group $\mathbb{Z}$ has infinite order. □

We close this section with two simple constructions for combining groups to build new groups.

Example 6.18. If $G_1, \ldots, G_k$ are abelian groups, we can form the **direct product** $H := G_1 \times \cdots \times G_k$, which consists of all k-tuples $(a_1, \ldots, a_k)$ with $a_1 \in G_1$, $\ldots$, $a_k \in G_k$. We can view H in a natural way as an abelian group if we define the group operation component-wise:

$$(a_1, \ldots, a_k) + (b_1, \ldots, b_k) := (a_1 + b_1, \ldots, a_k + b_k).$$

Of course, the groups $G_1, \ldots, G_k$ may be different, and the group operation applied in the ith component corresponds to the group operation associated with G_i. We leave it to the reader to verify that H is in fact an abelian group, where $0_H = (0_{G_1}, \ldots, 0_{G_k})$ and $-(a_1, \ldots, a_k) = (-a_1, \ldots, -a_k)$. As a special case, if $G = G_1 = \cdots = G_k$, then the k-wise direct product of G is denoted $G^{\times k}$. □

Example 6.19. Let G be an abelian group. An element $(a_1, \ldots, a_k)$ of $G^{\times k}$ may be identified with the function $f : \{1, \ldots, k\} \to G$ given by $f(i) = a_i$ for $i = 1, \ldots, k$. We can generalize this, replacing $\{1, \ldots, k\}$ by an arbitrary set I. We define $\mathrm{Map}(I, G)$ to be the set of all functions $f : I \to G$, which we naturally view as a group by defining the group operation point-wise: for $f, g \in \mathrm{Map}(I, G)$, we define

$$(f + g)(i) := f(i) + g(i) \text{ for all } i \in I.$$

Again, we leave it to the reader to verify that $\mathrm{Map}(I, G)$ is an abelian group, where the identity element is the function that maps each $i \in I$ to 0_G, and for $f \in \mathrm{Map}(I, G)$, we have $(-f)(i) = -(f(i))$ for all $i \in I$. □

EXERCISE 6.1. For a finite abelian group, one can completely specify the group by writing down the group operation table. For instance, Example 2.7 presented an addition table for $\mathbb{Z}_6$.

(a) Write down group operation tables for the following finite abelian groups: $\mathbb{Z}_5$, $\mathbb{Z}_5^*$, and $\mathbb{Z}_3 \times \mathbb{Z}_4^*$.

(b) Show that the group operation table for every finite abelian group is a **Latin square**; that is, each element of the group appears exactly once in each row and column.

(c) Below is an addition table for an abelian group that consists of the elements $\{a, b, c, d\}$; however, some entries are missing. Fill in the missing entries.

$+$	a	b	c	d
a	a			
b	b	a		
c			a	
d				

EXERCISE 6.2. Let $G := \{x \in \mathbb{R} : x > 1\}$, and define $a \star b := ab - a - b + 2$ for all $a, b \in \mathbb{R}$. Show that:

(a) G is closed under $\star$;

(b) the set G under the operation $\star$ forms an abelian group.

EXERCISE 6.3. Let G be an abelian group, and let g be an arbitrary, fixed element of G. Assume that the group operation of G is written additively. We define a new binary operation $\odot$ on G, as follows: for $a, b \in G$, let $a \odot b := a + b + g$. Show that the set G under $\odot$ forms an abelian group.

EXERCISE 6.4. Let G be a finite abelian group of even order. Show that there exists $a \in G$ with $a \neq 0_G$ and $2a = 0_G$.

EXERCISE 6.5. Let $\star$ be a binary operation on a non-empty, *finite* set G. Assume that $\star$ is associative, commutative, and satisfies the cancellation law: $a \star b = a \star c$ implies $b = c$. Show that G under $\star$ forms an abelian group.

EXERCISE 6.6. Show that the result of the previous exercise need not hold if G is infinite.

6.2 Subgroups

We next introduce the notion of a subgroup.

Definition 6.5. *Let G be an abelian group, and let H be a non-empty subset of G such that*

(i) $a + b \in H$ for all $a, b \in H$, and

(ii) $-a \in H$ for all $a \in H$.

Then H is called a ***subgroup of*** *G.*

In words: H is a subgroup of G if it is closed under the group operation and taking inverses.

Multiplicative notation: if the abelian group G in the above definition is written using multiplicative notation, then H is a subgroup if $ab \in H$ and $a^{-1} \in H$ for all $a, b \in H$.

Theorem 6.6. *If G is an abelian group, and H is a subgroup of G, then H contains 0_G; moreover, the binary operation of G, when restricted to H, yields a binary operation that makes H into an abelian group whose identity is 0_G.*

Proof. First, to see that $0_G \in H$, just pick any $a \in H$, and using both properties of the definition of a subgroup, we see that $0_G = a + (-a) \in H$.

Next, note that by property (i) of Definition 6.5, H is closed under addition, which means that the restriction of the binary operation "+" on G to H induces a well-defined binary operation on H. So now it suffices to show that H, together with this operation, satisfies the defining properties of an abelian group. Associativity and commutativity follow directly from the corresponding properties for G. Since 0_G acts as the identity on G, it does so on H as well. Finally, property (ii) of Definition 6.5 guarantees that every element $a \in H$ has an inverse in H, namely, $-a$. □

Clearly, for an abelian group G, the subsets G and $\{0_G\}$ are subgroups, though not very interesting ones. Other, more interesting subgroups may sometimes be found by using the following two theorems.

Theorem 6.7. *Let G be an abelian group, and let m be an integer. Then*

$$mG := \{ma : a \in G\}$$

is a subgroup of G.

Proof. The set mG is non-empty, since $0_G = m0_G \in mG$. For $ma, mb \in mG$, we have $ma + mb = m(a + b) \in mG$, and $-(ma) = m(-a) \in mG$. □

Theorem 6.8. *Let G be an abelian group, and let m be an integer. Then*

$$G\{m\} := \{a \in G : ma = 0_G\}$$

is a subgroup of G.

Proof. The set $G\{m\}$ is non-empty, since $m0_G = 0_G$, and so $G\{m\}$ contains 0_G. If $ma = 0_G$ and $mb = 0_G$, then $m(a + b) = ma + mb = 0_G + 0_G = 0_G$ and $m(-a) = -(ma) = -0_G = 0_G$. □

Multiplicative notation: if the abelian group G in the above two theorems is written using multiplicative notation, then we write the subgroup of the first theorem as $G^m := \{a^m : a \in G\}$. The subgroup in the second theorem is denoted in the same way: $G\{m\} := \{a \in G : a^m = 1_G\}$.

Example 6.20. We already proved that $(\mathbb{Z}_n^*)^m$ is a subgroup of $\mathbb{Z}_n^*$ in Theorem 2.16. Also, the proof of Theorem 2.17 clearly works for an arbitrary abelian group G: for each $a \in G$, and all $\ell, m \in \mathbb{Z}$ with $\gcd(\ell, m) = 1$, if $\ell a \in mG$, then $a \in mG$. □

Example 6.21. Let p be an odd prime. Then by Theorem 2.20, $(\mathbb{Z}_p^*)^2$ is a subgroup of $\mathbb{Z}_p^*$ of order $(p-1)/2$, and as we saw in Theorem 2.18, $\mathbb{Z}_p^*\{2\} = \{[\pm 1]\}$. □

Example 6.22. For every integer m, the set $m\mathbb{Z}$ is the subgroup of the additive group $\mathbb{Z}$ consisting of all multiples of m. This is the same as the *ideal of $\mathbb{Z}$ generated by m*, which we already studied in some detail in §1.2. Two such subgroups $m\mathbb{Z}$ and $m'\mathbb{Z}$ are equal if and only if $m = \pm m'$. The subgroup $\mathbb{Z}\{m\}$ is equal to $\mathbb{Z}$ if $m = 0$, and is equal to $\{0\}$ otherwise. □

Example 6.23. Let n be a positive integer, let $m \in \mathbb{Z}$, and consider the subgroup $m\mathbb{Z}_n$ of the additive group $\mathbb{Z}_n$. Now, for every residue class $[z] \in \mathbb{Z}_n$, we have $m[z] = [mz]$. Therefore, $[b] \in m\mathbb{Z}_n$ if and only if there exists $z \in \mathbb{Z}$ such that $mz \equiv b \pmod{n}$. By part (i) of Theorem 2.5, such a z exists if and only if $d \mid b$, where $d := \gcd(m, n)$. Thus, $m\mathbb{Z}_n$ consists precisely of the n/d distinct residue classes

$$[i \cdot d] \quad (i = 0, \ldots, n/d - 1),$$

and in particular, $m\mathbb{Z}_n = d\mathbb{Z}_n$.

Now consider the subgroup $\mathbb{Z}_n\{m\}$ of $\mathbb{Z}_n$. The residue class $[z]$ is in $\mathbb{Z}_n\{m\}$ if and only if $mz \equiv 0 \pmod{n}$. By part (ii) of Theorem 2.5, this happens if and only if $z \equiv 0 \pmod{n/d}$, where $d := \gcd(m, n)$ as above. Thus, $\mathbb{Z}_n\{m\}$ consists precisely of the d residue classes

$$[i \cdot n/d] \quad (i = 0, \ldots, d-1),$$

and in particular, $\mathbb{Z}_n\{m\} = \mathbb{Z}_n\{d\} = (n/d)\mathbb{Z}_n$. □

Example 6.24. For $n = 15$, consider again the table in Example 2.2. For $m = 1, 2, 3, 4, 5, 6$, the elements appearing in the mth row of that table form the subgroup $m\mathbb{Z}_n$ of $\mathbb{Z}_n$, and also the subgroup $\mathbb{Z}_n\{n/d\}$, where $d := \gcd(m, n)$. □

Because the abelian groups $\mathbb{Z}$ and $\mathbb{Z}_n$ are of such importance, it is a good idea to completely characterize all subgroups of these abelian groups. As the following two theorems show, the subgroups in Examples 6.22 and 6.23 are the *only* ones.

Theorem 6.9. *If G is a subgroup of $\mathbb{Z}$, then there exists a unique non-negative integer m such that $G = m\mathbb{Z}$. Moreover, for two non-negative integers m_1 and m_2, we have $m_1\mathbb{Z} \subseteq m_2\mathbb{Z}$ if and only if $m_2 \mid m_1$.*

Proof. Actually, we have already proven this. One only needs to observe that a subset G of $\mathbb{Z}$ is a subgroup if and only if it is an ideal of $\mathbb{Z}$, as defined in §1.2 (see Exercise 1.8). The first statement of the theorem then follows from Theorem 1.6. The second statement follows easily from the definitions, as was observed in §1.2. □

Theorem 6.10. *If G is a subgroup of $\mathbb{Z}_n$, then there exists a unique positive integer d dividing n such that $G = d\mathbb{Z}_n$. Also, for all positive divisors d_1, d_2 of n, we have $d_1\mathbb{Z}_n \subseteq d_2\mathbb{Z}_n$ if and only if $d_2 \mid d_1$.*

Proof. Note that the second statement implies the uniqueness part of the first statement, so it suffices to prove just the existence part of the first statement and the second statement.

Let G be an arbitrary subgroup of $\mathbb{Z}_n$, and let $H := \{z \in \mathbb{Z} : [z] \in G\}$. We claim that H is a subgroup of $\mathbb{Z}$. To see this, observe that if $a, b \in H$, then $[a]$ and $[b]$ belong to G, and hence so do $[a + b] = [a] + [b]$ and $[-a] = -[a]$, and thus $a + b$ and $-a$ belong to H. That proves the claim, and Theorem 6.9 implies that $H = d\mathbb{Z}$ for some non-negative integer d. It follows that

$$G = \{[y] : y \in H\} = \{[dz] : z \in \mathbb{Z}\} = d\mathbb{Z}_n.$$

Evidently, $n \in H = d\mathbb{Z}$, and hence $d \mid n$. That proves the existence part of the first statement of the theorem.

To prove the second statement of the theorem, observe that if d_1 and d_2 are arbitrary integers, then

$$\begin{aligned} d_1\mathbb{Z}_n \subseteq d_2\mathbb{Z}_n &\iff d_2 z \equiv d_1 \pmod{n} \text{ for some } z \in \mathbb{Z} \\ &\iff \gcd(d_2, n) \mid d_1 \text{ (by part (i) of Theorem 2.5).} \end{aligned}$$

In particular, if d_2 is a positive divisor of n, then $\gcd(d_2, n) = d_2$, which proves the second statement. □

Of course, not all abelian groups have such a simple subgroup structure.

Example 6.25. Consider the group $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. For every non-zero $\alpha \in G$, $\alpha + \alpha = 0_G$. From this, it is clear that the set $H = \{0_G, \alpha\}$ is a subgroup of G. However, for every integer m, $mG = G$ if m is odd, and $mG = \{0_G\}$ if m is even. Thus, the subgroup H is not of the form mG for any m. □

Example 6.26. Consider the group $\mathbb{Z}_{15}^*$. We can enumerate its elements as

$$[\pm 1],\ [\pm 2],\ [\pm 4],\ [\pm 7].$$

Therefore, the elements of $(\mathbb{Z}_{15}^*)^2$ are

$$[1]^2 = [1],\ [2]^2 = [4],\ [4]^2 = [16] = [1],\ [7]^2 = [49] = [4];$$

thus, $(\mathbb{Z}_{15}^*)^2$ has order 2, consisting as it does of the two distinct elements [1] and [4].

Going further, one sees that $(\mathbb{Z}_{15}^*)^4 = \{[1]\}$. Thus, $\alpha^4 = [1]$ for all $\alpha \in \mathbb{Z}_{15}^*$.

By direct calculation, one can determine that $(\mathbb{Z}_{15}^*)^3 = \mathbb{Z}_{15}^*$; that is, cubing simply permutes $\mathbb{Z}_{15}^*$.

For any given integer m, write $m = 4q + r$, where $0 \le r < 4$. Then for every $\alpha \in \mathbb{Z}_{15}^*$, we have $\alpha^m = \alpha^{4q+r} = \alpha^{4q}\alpha^r = \alpha^r$. Thus, $(\mathbb{Z}_{15}^*)^m$ is either $\mathbb{Z}_{15}^*$, $(\mathbb{Z}_{15}^*)^2$, or $\{[1]\}$.

However, there are certainly other subgroups of $\mathbb{Z}_{15}^*$—for example, the subgroup $\{[\pm 1]\}$. □

Example 6.27. Consider the group $\mathbb{Z}_5^* = \{[\pm 1], [\pm 2]\}$. The elements of $(\mathbb{Z}_5^*)^2$ are

$$[1]^2 = [1],\ [2]^2 = [4] = [-1];$$

thus, $(\mathbb{Z}_5^*)^2 = \{[\pm 1]\}$ and has order 2.

There are in fact no other subgroups of $\mathbb{Z}_5^*$ besides $\mathbb{Z}_5^*$, $\{[\pm 1]\}$, and $\{[1]\}$. Indeed, if H is a subgroup containing [2], then we must have $H = \mathbb{Z}_5^*$: $[2] \in H$ implies $[2]^2 = [4] = [-1] \in H$, which implies $[-2] \in H$ as well. The same holds if H is a subgroup containing $[-2]$. □

Example 6.28. Consider again the abelian group $\mathcal{F}^*$ of arithmetic functions f, such that $f(1) \neq 0$, and with the Dirichlet product as the binary operation, as discussed in Example 6.11. Exercises 2.48 and 2.55 imply that the subset of all multiplicative functions is a subgroup. □

We close this section with two theorems that provide useful ways to build new subgroups out of old ones.

Theorem 6.11. *If H_1 and H_2 are subgroups of an abelian group G, then so is*

$$H_1 + H_2 := \{a_1 + a_2 : a_1 \in H_1, a_2 \in H_2\}.$$

Proof. It is evident that $H_1 + H_2$ is non-empty, as it contains $0_G + 0_G = 0_G$. Consider two elements in $H_1 + H_2$, which we can write as $a_1 + a_2$ and $b_1 + b_2$, where $a_1, b_1 \in H_1$ and $a_2, b_2 \in H_2$. Then by the closure properties of subgroups, $a_1+b_1 \in H_1$ and $a_2+b_2 \in H_2$, and hence $(a_1+a_2)+(b_1+b_2) = (a_1+b_1)+(a_2+b_2) \in H_1 + H_2$. Similarly, $-(a_1 + a_2) = (-a_1) + (-a_2) \in H_1 + H_2$. □

Multiplicative notation: if the abelian group G in the above theorem is written multiplicatively, then the subgroup defined in the theorem is written $H_1H_2 := \{a_1a_2 : a_1 \in H_1,\ a_2 \in H_2\}$.

Theorem 6.12. *If H_1 and H_2 are subgroups of an abelian group G, then so is $H_1 \cap H_2$.*

Proof. It is evident that $H_1 \cap H_2$ is non-empty, as both H_1 and H_2 contain 0_G, and hence so does their intersection. If $a \in H_1 \cap H_2$ and $b \in H_1 \cap H_2$, then since $a, b \in H_1$, we have $a + b \in H_1$, and since $a, b \in H_2$, we have $a + b \in H_2$; therefore, $a + b \in H_1 \cap H_2$. Similarly, $-a \in H_1$ and $-a \in H_2$, and therefore, $-a \in H_1 \cap H_2$. □

Let G be an abelian group and H_1, H_2, H_3 subgroups of G. The reader may verify that $H_1 + H_2 = H_2 + H_1$ and $(H_1 + H_2) + H_3 = H_1 + (H_2 + H_3)$. It follows that if $H_1, \ldots, H_k$ are subgroups of G, then we can write $H_1 + \cdots + H_k$ without any parentheses, and there can be no ambiguity; moreover, the order of the H_i's does not matter. The same holds with "+" replaced by "∩."

A warning: If H is a subgroup of an abelian group G, then in general, we have $H + H \neq 2H$. For example, $\mathbb{Z} + \mathbb{Z} = \mathbb{Z}$, while $2\mathbb{Z} \neq \mathbb{Z}$.

EXERCISE 6.7. Let G be an abelian group.

(a) Suppose that H is a non-empty subset of G. Show that H is a subgroup of G if and only if $a - b \in H$ for all $a, b \in H$.

(b) Suppose that H is a non-empty, *finite* subset of G such that $a + b \in H$ for all $a, b \in H$. Show that H is a subgroup of G.

EXERCISE 6.8. Let G be an abelian group.

(a) Show that if H is a subgroup of G, $h \in H$, and $g \in G \setminus H$, then $h + g \in G \setminus H$.

(b) Suppose that H is a non-empty subset of G such that for all $h, g \in G$: (i) $h \in H$ implies $-h \in H$, and (ii) $h \in H$ and $g \in G \setminus H$ implies $h+g \in G \setminus H$. Show that H is a subgroup of G.

EXERCISE 6.9. Show that if H is a subgroup of an abelian group G, then a set $K \subseteq H$ is a subgroup of G if and only if K is a subgroup of H.

EXERCISE 6.10. Let G be an abelian group with subgroups H_1 and H_2. Show that every subgroup H of G that contains $H_1 \cup H_2$ must contain all of $H_1 + H_2$, and that $H_1 \subseteq H_2$ if and only if $H_1 + H_2 = H_2$.

EXERCISE 6.11. Let H_1 be a subgroup of an abelian group G_1 and H_2 a subgroup of an abelian group G_2. Show that $H_1 \times H_2$ is a subgroup of $G_1 \times G_2$.

EXERCISE 6.12. Show that if G_1 and G_2 are abelian groups, and m is an integer, then $m(G_1 \times G_2) = mG_1 \times mG_2$.

EXERCISE 6.13. Let G_1 and G_2 be abelian groups, and let H be a subgroup of $G_1 \times G_2$. Define

$$H_1 := \{a_1 \in G_1 : (a_1, a_2) \in H \text{ for some } a_2 \in G_2\}.$$

Show that H_1 is a subgroup of G_1.

EXERCISE 6.14. Let I be a set and G be an abelian group, and consider the group $\mathrm{Map}(I, G)$ of functions $f : I \to G$. Let $\mathrm{Map}^{\#}(I, G)$ be the set of functions $f \in \mathrm{Map}(I, G)$ such that $f(i) \neq 0_G$ for at most finitely many $i \in I$. Show that $\mathrm{Map}^{\#}(I, G)$ is a subgroup of $\mathrm{Map}(I, G)$.

6.3 Cosets and quotient groups

We now generalize the notion of a congruence relation.

Let G be an abelian group, and let H be a subgroup of G. For $a, b \in G$, we write $a \equiv b \pmod{H}$ if $a - b \in H$. In other words, $a \equiv b \pmod{H}$ if and only if $a = b + h$ for some $h \in H$.

Analogous to Theorem 2.2, if we view the subgroup H as fixed, then the following theorem says that the binary relation "$\cdot \equiv \cdot \pmod{H}$" is an equivalence relation on the set G:

Theorem 6.13. *Let G be an abelian group and H a subgroup of G. For all $a, b, c \in G$, we have:*

(i) $a \equiv a \pmod{H}$;

(ii) $a \equiv b \pmod{H}$ *implies* $b \equiv a \pmod{H}$;

(iii) $a \equiv b \pmod{H}$ *and* $b \equiv c \pmod{H}$ *implies* $a \equiv c \pmod{H}$.

Proof. For (i), observe that H contains $0_G = a - a$. For (ii), observe that if H contains $a - b$, then it also contains $-(a - b) = b - a$. For (iii), observe that if H contains $a - b$ and $b - c$, then it also contains $(a - b) + (b - c) = a - c$. □

Since the binary relation "$\cdot \equiv \cdot \pmod{H}$" is an equivalence relation, it partitions G into equivalence classes (see Theorem 2.1). For $a \in G$, we denote the equivalence class containing a by $[a]_H$. By definition, we have

$$x \in [a]_H \iff x \equiv a \pmod{H} \iff x = a + h \text{ for some } h \in H,$$

and hence

$$[a]_H = a + H := \{a + h : h \in H\}.$$

It is also clear that $[0_G]_H = H$.

Historically, these equivalence classes are called **cosets of H in G**, and we shall adopt this terminology here as well. Any member of a coset is called a **representative** of the coset.

Multiplicative notation: if G is written multiplicatively, then $a \equiv b \pmod{H}$ means $ab^{-1} \in H$, and $[a]_H = aH := \{ah : h \in H\}$.

Example 6.29. Let $G := \mathbb{Z}$ and $H := n\mathbb{Z}$ for some positive integer n. Then $a \equiv b \pmod{H}$ if and only if $a \equiv b \pmod{n}$. The coset $[a]_H$ is exactly the same thing as the residue class $[a]_n \in \mathbb{Z}_n$. □

Example 6.30. Let $G := \mathbb{Z}_6$, which consists of the residue classes $[0], [1], [2], [3], [4], [5]$. Let H be the subgroup $3G = \{[0], [3]\}$ of G. The coset of H containing the residue class $[1]$ is $[1] + H = \{[1], [4]\}$, and the coset of H containing the residue class $[2]$ is $[2] + H = \{[2], [5]\}$. The cosets $\{[0], [3]\}$, $\{[1], [4]\}$, and $\{[2], [5]\}$ are the only cosets of H in G, and they clearly partition the set $\mathbb{Z}_6$. Note that each coset of H in G contains two elements, each of which is itself a coset of $6\mathbb{Z}$ in $\mathbb{Z}$ (i.e., a residue classes modulo 6). □

In the previous example, we saw that each coset contained the same number of elements. As the next theorem shows, this was no accident.

Theorem 6.14. *Let G be an abelian group and H a subgroup of G. For all $a, b \in G$, the function*

$$\begin{aligned} f: \quad & G \to G \\ & x \mapsto b - a + x \end{aligned}$$

is a bijection, which, when restricted to the coset $[a]_H$, yields a bijection from $[a]_H$ to the coset $[b]_H$. In particular, every two cosets of H in G have the same cardinality.

Proof. First, we claim that f is a bijection. Indeed, if $f(x) = f(x')$, then $b - a + x = b - a + x'$, and subtracting b and adding a to both sides of this equation yields $x = x'$. That proves that f is injective. To prove that f is surjective, observe that for any given $x' \in G$, we have $f(a - b + x') = x'$.

Second, we claim that for all $x \in G$, we have $x \in [a]_H$ if and only if $f(x) \in [b]_H$. On the one hand, suppose that $x \in [a]_H$, which means that $x = a+h$ for some $h \in H$. Subtracting a and adding b to both sides of this equation yields $b - a + x = b + h$, which means $f(x) \in [b]_H$. Conversely, suppose that $f(x) \in [b]_H$, which means that $b - a + x = b + h$ for some $h \in H$. Subtracting b and adding a to both sides of this equation yields $x = a + h$, which means that $x \in [a]_H$.

The theorem is now immediate from these two claims. □

An incredibly useful consequence of the above theorem is:

Theorem 6.15 (Lagrange's theorem). *If G is a finite abelian group, and H is a subgroup of G, then the order of H divides the order of G.*

Proof. This is an immediate consequence of the previous theorem, and the fact that the cosets of H in G partition G. □

Analogous to Theorem 2.3, we have:

Theorem 6.16. *Suppose G is an abelian group and H is a subgroup of G. For all $a, a', b, b' \in G$, if $a \equiv a' \pmod{H}$ and $b \equiv b' \pmod{H}$, then we have $a + b \equiv a' + b' \pmod{H}$.*

Proof. Now, $a \equiv a' \pmod{H}$ and $b \equiv b' \pmod{H}$ means that $a = a' + x$ and $b = b'+y$ for some $x, y \in H$. Therefore, $a+b = (a'+x)+(b'+y) = (a'+b')+(x+y)$, and since $x + y \in H$, this means that $a + b \equiv a' + b' \pmod{H}$. □

Let G be an abelian group and H a subgroup. Let G/H denote the set of all cosets of H in G. Theorem 6.16 allows us to define a binary operation on G/H in the following natural way: for $a, b \in G$, define

$$[a]_H + [b]_H := [a + b]_H.$$

That this definition is unambiguous follows immediately from Theorem 6.16: if $[a]_H = [a']_H$ and $[b]_H = [b']_H$, then $[a+b]_H = [a'+b']_H$.

We can easily verify that this operation makes G/H into an abelian group. We need to check that the four properties of Definition 6.1 are satisfied:

(i) Associativity:

$$\begin{aligned}[a]_H + ([b]_H + [c]_H) &= [a]_H + [b+c]_H = [a+(b+c)]_H \\ &= [(a+b)+c]_H = [a+b]_H + [c]_H \\ &= ([a]_H + [b]_H) + [c]_H.\end{aligned}$$

Here, we have used the definition of addition of cosets, and the corresponding associativity property for G.

(ii) Identity element: the coset $[0_G]_H = H$ acts as the identity element, since

$$[a]_H + [0_G]_H = [a+0_G]_H = [a]_H = [0_G+a]_H = [0_G]_H + [a]_H.$$

(iii) Inverses: the inverse of the coset $[a]_H$ is $[-a]_H$, since

$$[a]_H + [-a]_H = [a+(-a)]_H = [0_G]_H = [(-a)+a]_H = [-a]_H + [a]_H.$$

(iv) Commutativity:

$$[a]_H + [b]_H = [a+b]_H = [b+a]_H = [b]_H + [a]_H.$$

The group G/H is called the **quotient group of G modulo H**. The order of the group G/H is sometimes denoted $[G : H]$ and is called the **index of H in G**. Note that if $H = G$, then the quotient group G/H is the trivial group, and so $[G : H] = 1$.

Multiplicative notation: if G is written multiplicatively, then the definition of the group operation of G/H is expressed $[a]_H \cdot [b]_H := [a \cdot b]_H$; the identity element of G/H is $[1_G]_H = H$, and the inverse of $[a]_H$ is $[a^{-1}]_H$.

Theorem 6.17. *Suppose G is a finite abelian group and H is a subgroup of G. Then $[G : H] = |G|/|H|$. Moreover, if K is a subgroup of H, then*

$$[G : K] = [G : H][H : K].$$

Proof. The fact that $[G : H] = |G|/|H|$ follows directly from Theorem 6.14. The fact that $[G : K] = [G : H][H : K]$ follows from a simple calculation:

$$[G : H] = \frac{|G|}{|H|} = \frac{|G|/|K|}{|H|/|K|} = \frac{[G : K]}{[H : K]}. \quad \square$$

Example 6.31. For each $n \geq 1$, the group $\mathbb{Z}_n$ is precisely the quotient group $\mathbb{Z}/n\mathbb{Z}$. $\square$

Example 6.32. Continuing with Example 6.30, let $G := \mathbb{Z}_6$ and $H := 3G = \{[0], [3]\}$. The quotient group G/H has order 3, and consists of the cosets

$$\alpha := \{[0], [3]\}, \quad \beta := \{[1], [4]\}, \quad \gamma := \{[2], [5]\}.$$

If we write out an addition table for G, grouping together elements in cosets of H in G, then we also get an addition table for the quotient group G/H:

$+$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$	$[5]$
$[0]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$	$[5]$
$[3]$	$[3]$	$[0]$	$[4]$	$[1]$	$[5]$	$[2]$
$[1]$	$[1]$	$[4]$	$[2]$	$[5]$	$[3]$	$[0]$
$[4]$	$[4]$	$[1]$	$[5]$	$[2]$	$[0]$	$[3]$
$[2]$	$[2]$	$[5]$	$[3]$	$[0]$	$[4]$	$[1]$
$[5]$	$[5]$	$[2]$	$[0]$	$[3]$	$[1]$	$[4]$

This table illustrates quite graphically the point of Theorem 6.16: for every two cosets, if we take any element from the first and add it to any element of the second, we always end up in the same coset.

We can also write down just the addition table for G/H:

$+$	α	β	γ
α	α	β	γ
β	β	γ	α
γ	γ	α	β

Note that by replacing α with $[0]_3$, β with $[1]_3$, and γ with $[2]_3$, the addition table for G/H becomes the addition table for $\mathbb{Z}_3$. In this sense, we can view G/H as essentially just a "renaming" of $\mathbb{Z}_3$. □

Example 6.33. Let us return to Example 6.26. The multiplicative group $\mathbb{Z}_{15}^*$, as we saw, is of order 8. The subgroup $(\mathbb{Z}_{15}^*)^2$ of $\mathbb{Z}_{15}^*$ has order 2. Therefore, the quotient group $\mathbb{Z}_{15}^*/(\mathbb{Z}_{15}^*)^2$ has order 4. Indeed, the cosets are

$$\alpha_{00} := (\mathbb{Z}_{15}^*)^2 = \{[1], [4]\}, \qquad \alpha_{01} := [-1](\mathbb{Z}_{15}^*)^2 = \{[-1], [-4]\},$$
$$\alpha_{10} := [2](\mathbb{Z}_{15}^*)^2 = \{[2], [-7]\}, \quad \alpha_{11} := [-2](\mathbb{Z}_{15}^*)^2 = \{[-2], [7]\}.$$

We can write down the multiplication table for the quotient group:

$\cdot$	α_{00}	α_{01}	α_{10}	α_{11}
α_{00}	α_{00}	α_{01}	α_{10}	α_{11}
α_{01}	α_{01}	α_{00}	α_{11}	α_{10}
α_{10}	α_{10}	α_{11}	α_{00}	α_{01}
α_{11}	α_{11}	α_{10}	α_{01}	α_{00}

Note that this group is essentially just a "renaming" of the additive group $\mathbb{Z}_2 \times \mathbb{Z}_2$. □

Example 6.34. As we saw in Example 6.27, $(\mathbb{Z}_5^*)^2 = \{[\pm 1]\}$. Therefore, the quotient group $\mathbb{Z}_5^*/(\mathbb{Z}_5^*)^2$ has order 2. The cosets of $(\mathbb{Z}_5^*)^2$ in $\mathbb{Z}_5^*$ are $\alpha_0 := \{[\pm 1]\}$ and $\alpha_1 := \{[\pm 2]\}$, and the multiplication table looks like this:

$\cdot$	α_0	α_1
α_0	α_0	α_1
α_1	α_1	α_0

We see that the quotient group is essentially just a "renaming" of $\mathbb{Z}_2$. □

EXERCISE 6.15. Write down the cosets of $(\mathbb{Z}_{35}^*)^2$ in $\mathbb{Z}_{35}^*$, along with the multiplication table for the quotient group $\mathbb{Z}_{35}^*/(\mathbb{Z}_{35}^*)^2$.

EXERCISE 6.16. Let n be an odd, positive integer whose factorization into primes is $n = p_1^{e_1} \cdots p_r^{e_r}$. Show that $[\mathbb{Z}_n^* : (\mathbb{Z}_n^*)^2] = 2^r$.

EXERCISE 6.17. Let n be a positive integer, and let m be any integer. Show that $[\mathbb{Z}_n : m\mathbb{Z}_n] = n/\gcd(m, n)$.

EXERCISE 6.18. Let G be an abelian group and H a subgroup with $[G : H] = 2$. Show that if $a, b \in G \setminus H$, then $a + b \in H$.

EXERCISE 6.19. Let H be a subgroup of an abelian group G, and let $a, b \in G$ with $a \equiv b \pmod{H}$. Show that $ka \equiv kb \pmod{H}$ for all $k \in \mathbb{Z}$.

EXERCISE 6.20. Let G be an abelian group, and let $\sim$ be an equivalence relation on G. Further, suppose that for all $a, a', b \in G$, if $a \sim a'$, then $a + b \sim a' + b$. Let $H := \{a \in G : a \sim 0_G\}$. Show that H is a subgroup of G, and that for all $a, b \in G$, we have $a \sim b$ if and only if $a \equiv b \pmod{H}$.

EXERCISE 6.21. Let H be a subgroup of an abelian group G, and let $a, b \in G$. Show that $[a + b]_H = \{x + y : x \in [a]_H, y \in [b]_H\}$.

6.4 Group homomorphisms and isomorphisms

In this section, we study maps that relate the structure of one group to another. Such maps are often very useful, as they may allow us to transfer hard-won knowledge about one group to another, perhaps more mysterious, group.

Definition 6.18. *A **group homomorphism** is a function ρ from an abelian group G to an abelian group G' such that $\rho(a + b) = \rho(a) + \rho(b)$ for all $a, b \in G$.*

Note that in the equality $\rho(a + b) = \rho(a) + \rho(b)$ in the above definition, the addition on the left-hand side is taking place in the group G while the addition on the right-hand side is taking place in the group G'.

Two sets play a critical role in the study of a group homomorphism $\rho : G \to G'$. The first set is the **image** of ρ, that is, the set $\rho(G) = \{\rho(a) : a \in G\}$. The second set is the **kernel** of ρ, defined as the set of all elements of G that are mapped to $0_{G'}$ by ρ, that is, the set $\rho^{-1}(\{0_{G'}\}) = \{a \in G : \rho(a) = 0_{G'}\}$. We introduce the following notation for these sets: $\operatorname{Im}\rho$ denotes the image of ρ, and $\operatorname{Ker}\rho$ denotes the kernel of ρ.

Example 6.35. If H is a subgroup of an abelian group G, then the inclusion map $i : H \to G$ is obviously a group homomorphism. □

Example 6.36. Suppose H is a subgroup of an abelian group G. We define the map

$$\begin{aligned} \rho : \quad & G \to G/H \\ & a \mapsto [a]_H. \end{aligned}$$

It is not hard to see that this is a group homomorphism. Indeed, this follows almost immediately from the way we defined addition in the quotient group G/H:

$$\rho(a + b) = [a + b]_H = [a]_H + [b]_H = \rho(a) + \rho(b).$$

It is clear that ρ is surjective. It is also not hard to see that $\operatorname{Ker}\rho = H$; indeed, H is the identity element in G/H, and $[a]_H = H$ if and only if $a \in H$. The map ρ is called the **natural map** from G to G/H. □

Example 6.37. For a given positive integer n, the natural map from $\mathbb{Z}$ to $\mathbb{Z}_n$ sends $a \in \mathbb{Z}$ to the residue class $[a]_n$. This map is a surjective group homomorphism with kernel $n\mathbb{Z}$. □

Example 6.38. Suppose G is an abelian group and m is an integer. The map

$$\begin{aligned} \rho : \quad & G \to G \\ & a \mapsto ma \end{aligned}$$

is a group homomorphism, since

$$\rho(a + b) = m(a + b) = ma + mb = \rho(a) + \rho(b).$$

The image of this homomorphism is the subgroup mG and the kernel is the subgroup $G\{m\}$. We call this map the **m-multiplication map on G**. If G is written multiplicatively, then this map, which sends $a \in G$ to $a^m \in G$, is called the **m-power map on G**, and its image is G^m. □

Example 6.39. Let p be an odd prime. Consider the 2-power, or squaring, map on $\mathbb{Z}_p^*$. Then as we saw in Example 6.21, the image $(\mathbb{Z}_p^*)^2$ of this map is a subgroup of $\mathbb{Z}_p^*$ of order $(p - 1)/2$, and its kernel is $\mathbb{Z}_p^*\{2\} = \{[\pm 1]\}$. □

Example 6.40. Consider the m-multiplication map on $\mathbb{Z}$. As we saw in Example 6.22, its image $m\mathbb{Z}$ is equal to $\mathbb{Z}$ if and only if $m = \pm 1$, while its kernel $\mathbb{Z}\{m\}$ is equal to $\mathbb{Z}$ if $m = 0$, and is equal to $\{0\}$ otherwise. □

Example 6.41. Consider the m-multiplication map on $\mathbb{Z}_n$. As we saw in Example 6.23, if $d := \gcd(m, n)$, the image $m\mathbb{Z}_n$ of this map is a subgroup of $\mathbb{Z}_n$ of order n/d, while its kernel $\mathbb{Z}_n\{m\}$ is a subgroup of order d. □

Example 6.42. Suppose G is an abelian group and a is an element of G. It is easy to see that the map

$$\begin{aligned} \rho : \quad & \mathbb{Z} \to G \\ & z \mapsto za \end{aligned}$$

is a group homomorphism, since

$$\rho(z + z') = (z + z')a = za + z'a = \rho(z) + \rho(z').$$ □

Example 6.43. As a special case of the previous example, let n be a positive integer and let α be an element of $\mathbb{Z}_n^*$. Let $\rho : \mathbb{Z} \to \mathbb{Z}_n^*$ be the group homomorphism that sends $z \in \mathbb{Z}$ to $\alpha^z \in \mathbb{Z}_n^*$. That ρ is a group homomorphism means that $\alpha^{z+z'} = \alpha^z \alpha^{z'}$ for all $z, z' \in \mathbb{Z}$ (note that the group operation is addition in $\mathbb{Z}$ and multiplication in $\mathbb{Z}_n^*$). If the multiplicative order of α is equal to k, then as discussed in §2.7, the image of ρ consists of the k distinct group elements $\alpha^0, \alpha^1, \ldots, \alpha^{k-1}$. The kernel of ρ consists of those integers z such that $\alpha^z = 1$. Again by the discussion in §2.7, the kernel of ρ is equal to the subgroup $k\mathbb{Z}$. □

Example 6.44. Generalizing Example 6.42, the reader may verify that if $a_1, \ldots, a_k$ are fixed elements of an abelian group G, then the map

$$\begin{aligned} \rho : \quad & \mathbb{Z}^{\times k} \to G \\ & (z_1, \ldots, z_k) \mapsto z_1 a_1 + \cdots + z_k a_k \end{aligned}$$

is a group homomorphism. □

Example 6.45. Suppose that $H_1, \ldots, H_k$ are subgroups of an abelian group G. The reader may easily verify that the map

$$\begin{aligned} \rho : \quad & H_1 \times \cdots \times H_k \to G \\ & (a_1, \ldots, a_k) \mapsto a_1 + \cdots + a_k \end{aligned}$$

is a group homomorphism whose image is the subgroup $H_1 + \cdots + H_k$. □

The following theorem summarizes some of the most important properties of group homomorphisms.

Theorem 6.19. *Let ρ be a group homomorphism from G to G'. Then:*

(i) $\rho(0_G) = 0_{G'}$;

(ii) $\rho(-a) = -\rho(a)$ *for all* $a \in G$;

(iii) $\rho(na) = n\rho(a)$ *for all* $n \in \mathbb{Z}$ *and* $a \in G$;

(iv) if H is a subgroup of G, then $\rho(H)$ is a subgroup of G'; in particular (setting $H := G$), $\operatorname{Im}\rho$ is a subgroup of G';

(v) if H' is a subgroup of G', then $\rho^{-1}(H')$ is a subgroup of G; in particular (setting $H' := \{0_{G'}\}$), $\operatorname{Ker}\rho$ is a subgroup of G;

(vi) for all $a, b \in G$, $\rho(a) = \rho(b)$ if and only if $a \equiv b \pmod{\operatorname{Ker}\rho}$;

(vii) ρ is injective if and only if $\operatorname{Ker}\rho = \{0_G\}$.

Proof. These are all straightforward calculations.

(i) We have

$$0_{G'} + \rho(0_G) = \rho(0_G) = \rho(0_G + 0_G) = \rho(0_G) + \rho(0_G).$$

Now cancel $\rho(0_G)$ from both sides.

(ii) We have

$$0_{G'} = \rho(0_G) = \rho(a + (-a)) = \rho(a) + \rho(-a),$$

and hence $\rho(-a)$ is the inverse of $\rho(a)$.

(iii) For $n = 0$, this follows from part (i). For $n > 0$, this follows from the definitions by induction on n. For $n < 0$, this follows from the positive case and part (ii).

(iv) For all $a, b \in H$, we have $a + b \in H$ and $-a \in H$; hence, $\rho(H)$ contains $\rho(a + b) = \rho(a) + \rho(b)$ and $\rho(-a) = -\rho(a)$.

(v) $\rho^{-1}(H')$ is non-empty, since $\rho(0_G) = 0'_G \in H'$. If $\rho(a) \in H'$ and $\rho(b) \in H'$, then $\rho(a + b) = \rho(a) + \rho(b) \in H'$, and $\rho(-a) = -\rho(a) \in H'$.

(vi) We have

$$\begin{aligned}\rho(a) = \rho(b) &\iff \rho(a) - \rho(b) = 0_{G'} \iff \rho(a - b) = 0_{G'} \\ &\iff a - b \in \operatorname{Ker}\rho \iff a \equiv b \pmod{\operatorname{Ker}\rho}.\end{aligned}$$

(vii) If ρ is injective, then in particular, $\rho^{-1}(\{0_{G'}\})$ cannot contain any other element besides 0_G. If ρ is not injective, then there exist two distinct elements $a, b \in G$ with $\rho(a) = \rho(b)$, and by part (vi), $\operatorname{Ker}\rho$ contains the element $a - b$, which is non-zero. □

Part (vii) of the above theorem is particularly useful: to check that a group homomorphism is injective, it suffices to determine if $\operatorname{Ker}\rho = \{0_G\}$. Thus, the

injectivity and surjectivity of a given group homomorphism $\rho : G \to G'$ may be characterized in terms of its kernel and image:

- ρ is injective if and only if its kernel is trivial (i.e. $\operatorname{Ker}\rho = \{0_G\}$);
- ρ is surjective if and only if $\operatorname{Im}\rho = G'$.

We next present two very easy theorems that allow us to compose group homomorphisms in simple ways.

Theorem 6.20. *If $\rho : G \to G'$ and $\rho' : G' \to G''$ are group homomorphisms, then so is their composition $\rho' \circ \rho : G \to G''$.*

Proof. For all $a, b \in G$, we have

$$\rho'(\rho(a+b)) = \rho'(\rho(a) + \rho(b)) = \rho'(\rho(a)) + \rho'(\rho(b)). \quad \square$$

Theorem 6.21. *Let $\rho_i : G \to G'_i$, for $i = 1, \ldots, k$, be group homomorphisms. Then the map*

$$\begin{aligned} \rho : \quad & G \to G'_1 \times \cdots \times G'_k \\ & a \mapsto (\rho_1(a), \ldots, \rho_k(a)) \end{aligned}$$

is a group homomorphism.

Proof. For all $a, b \in G$, we have

$$\begin{aligned} \rho(a+b) &= (\rho_1(a+b), \ldots, \rho_k(a+b)) = (\rho_1(a) + \rho_1(b), \ldots, \rho_k(a) + \rho_k(b)) \\ &= \rho(a) + \rho(b). \quad \square \end{aligned}$$

Consider a group homomorphism $\rho : G \to G'$. If ρ is bijective, then ρ is called a **group isomorphism** of G with G'. If such a group isomorphism ρ exists, we say that G **is isomorphic to** G', and write $G \cong G'$. Moreover, if $G = G'$, then ρ is called a **group automorphism** on G.

Theorem 6.22. *If ρ is a group isomorphism of G with G', then the inverse function ρ^{-1} is a group isomorphism of G' with G.*

Proof. For all $a', b' \in G'$, we have

$$\rho(\rho^{-1}(a') + \rho^{-1}(b')) = \rho(\rho^{-1}(a')) + \rho(\rho^{-1}(b')) = a' + b',$$

and hence $\rho^{-1}(a') + \rho^{-1}(b') = \rho^{-1}(a' + b')$. $\square$

Because of this theorem, if G is isomorphic to G', we may simply say that "G and G' are isomorphic."

We stress that a group isomorphism $\rho : G \to G'$ is essentially just a "renaming" of the group elements. This can be visualized as follows. Imagine the addition table for G written out with rows and columns labeled by elements of G, with the

entry in row a and column b being $a + b$. Now suppose we use the function ρ to consistently rename all the elements of G appearing in this table: the label on row a is replaced by $\rho(a)$, the label on column b by $\rho(b)$, and the entry in row a and column b by $\rho(a + b)$. Because ρ is bijective, every element of G' appears exactly once as a label on a row and as a label on a column; moreover, because $\rho(a + b) = \rho(a) + \rho(b)$, what we end up with is an addition table for G'. It follows that all structural properties of the group are preserved, even though the two groups might look quite different syntactically.

Example 6.46. As was shown in Example 6.32, the quotient group G/H discussed in that example is isomorphic to $\mathbb{Z}_3$. As was shown in Example 6.33, the quotient group $\mathbb{Z}_{15}^*/(\mathbb{Z}_{15}^*)^2$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. As was shown in Example 6.34, the quotient group $\mathbb{Z}_5^*/(\mathbb{Z}_5^*)^2$ is isomorphic to $\mathbb{Z}_2$. □

Example 6.47. If $\gcd(m, n) = 1$, then the m-multiplication map on $\mathbb{Z}_n$ is a group automorphism. □

The next theorem tells us that corresponding to any group homomorphism, there is a natural group isomomorphism. As group isomorphisms are much nicer than group homomorphisms, this is often very useful.

Theorem 6.23 (First isomorphism theorem). *Let $\rho : G \to G'$ be a group homomorphism with kernel K and image H'. Then we have a group isomorphism*

$$G/K \cong H'.$$

Specifically, the map

$$\begin{aligned} \bar{\rho} : \quad G/K &\to G' \\ [a]_K &\mapsto \rho(a) \end{aligned}$$

is an injective group homomorphism whose image is H'.

Proof. Using part (vi) of Theorem 6.19, we see that for all $a, b \in G$, we have

$$[a]_K = [b]_K \iff a \equiv b \pmod{K} \iff \rho(a) = \rho(b).$$

This immediately implies that the definition of $\bar{\rho}$ is unambiguous ($[a]_K = [b]_K$ implies $\rho(a) = \rho(b)$), and that $\bar{\rho}$ is injective ($\rho(a) = \rho(b)$ implies $[a]_K = [b]_K$). It is clear that $\bar{\rho}$ maps onto H', since every element of H' is of the form $\rho(a)$ for some $a \in G$, and the map $\bar{\rho}$ sends $[a]_K$ to $\rho(a)$. Finally, to see that $\bar{\rho}$ is a group homomorphism, note that

$$\bar{\rho}([a]_K + [b]_K) = \bar{\rho}([a + b]_K) = \rho(a + b) = \rho(a) + \rho(b) = \bar{\rho}([a]_K) + \bar{\rho}([b]_K). \quad \square$$

We can generalize the previous theorem, as follows:

Theorem 6.24. *Let $\rho : G \to G'$ be a group homomorphism. Then for every subgroup H of G with $H \subseteq \operatorname{Ker}\rho$, we may define a group homomorphism*

$$\begin{aligned} \bar{\rho} : \quad & G/H \to G' \\ & [a]_H \mapsto \rho(a). \end{aligned}$$

Moreover, $\operatorname{Im}\bar{\rho} = \operatorname{Im}\rho$, and $\bar{\rho}$ is injective if and only if $H = \operatorname{Ker}\rho$.

Proof. Using the assumption that $H \subseteq \operatorname{Ker}\rho$, we see that $\bar{\rho}$ is unambiguously defined, since for all $a, b \in G$, we have

$$[a]_H = [b]_H \implies a \equiv b \pmod{H} \implies a \equiv b \pmod{\operatorname{Ker}\rho} \implies \rho(a) = \rho(b).$$

That $\bar{\rho}$ is a group homomorphism, with $\operatorname{Im}\bar{\rho} = \operatorname{Im}\rho$, follows as in the proof of Theorem 6.23. If $H = \operatorname{Ker}\rho$, then by Theorem 6.23, $\bar{\rho}$ is injective, and if $H \subsetneq \operatorname{Ker}\rho$, then $\bar{\rho}$ is not injective, since if we choose $a \in \operatorname{Ker}\rho \setminus H$, we see that $\bar{\rho}([a]_H) = 0_{G'}$, and hence $\operatorname{Ker}\bar{\rho}$ is non-trivial. □

The next theorem gives us another important construction of a group isomorphism.

Theorem 6.25 (Internal direct product). *Let G be an abelian group with subgroups H_1, H_2, where $H_1 \cap H_2 = \{0_G\}$. Then we have a group isomorphism*

$$H_1 \times H_2 \cong H_1 + H_2$$

given by the map

$$\begin{aligned} \rho : \quad & H_1 \times H_2 \to H_1 + H_2 \\ & (a_1, a_2) \mapsto a_1 + a_2. \end{aligned}$$

Proof. We already saw that ρ is a surjective group homomorphism in Example 6.45. To see that ρ is injective, it suffices to show that $\operatorname{Ker}\rho$ is trivial; that is, it suffices to show that for all $a_1 \in H_1$ and $a_2 \in H_2$, if $a_1 + a_2 = 0_G$, then $a_1 = a_2 = 0_G$. But $a_1 + a_2 = 0_G$ implies $a_1 = -a_2 \in H_2$, and hence $a_1 \in H_1 \cap H_2 = \{0_G\}$, and so $a_1 = 0_G$. Similarly, one shows that $a_2 = 0_G$, and that finishes the proof. □

If H_1, H_2 are as in the above theorem, then $H_1 + H_2$ is sometimes called the **internal direct product** of H_1 and H_2.

Example 6.48. We can use the general theory developed so far to get a quick-and-dirty proof of the Chinese remainder theorem (Theorem 2.6). Let $\{n_i\}_{i=1}^k$ be a pairwise relatively prime family of positive integers, and let $n := \prod_{i=1}^k n_i$. Consider the map

$$\begin{aligned} \rho : \quad & \mathbb{Z} \to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \\ & a \mapsto ([a]_{n_1}, \ldots, [a]_{n_k}). \end{aligned}$$

It is easy to see that this map is a group homomorphism; indeed, it is the map constructed in Theorem 6.21 applied with the natural maps $\rho_i : \mathbb{Z} \to \mathbb{Z}_{n_i}$, for $i = 1, \ldots, k$. Evidently, $a \in \operatorname{Ker} \rho$ if and only if $n_i \mid a$ for $i = 1, \ldots, k$, and since $\{n_i\}_{i=1}^k$ is pairwise relatively prime, it follows that $a \in \operatorname{Ker} \rho$ if and only if $n \mid a$; that is, $\operatorname{Ker} \rho = n\mathbb{Z}$. Theorem 6.23 then gives us an injective group homomorphism

$$\begin{aligned} \bar{\rho} : \quad \mathbb{Z}_n &\to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \\ [a]_n &\mapsto ([a]_{n_1}, \ldots, [a]_{n_k}). \end{aligned}$$

But since the sets $\mathbb{Z}_n$ and $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ have the same size, injectivity implies surjectivity. From this, Theorem 2.6 is immediate.

The map $\bar{\rho}$ is a group isomorphism

$$\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}.$$

In fact, the map $\bar{\rho}$ is the same as the map θ in Theorem 2.8, and so we also immediately obtain parts (i), (ii), (iii.a), and (iii.b) of that theorem.

Observe that parts (iii.c) and (iii.d) of Theorem 2.8 imply that restricting the map θ to $\mathbb{Z}_n^*$ yields an isomorphism of *multiplicative* groups

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*.$$

This fact does *not* follow from the general theory developed so far; however, in the next chapter, we will see how this fact fits into the broader algebraic picture.

One advantage of our original proof of Theorem 2.6 is that it gives us an explicit formula for the inverse map θ^{-1}, which is useful in computations. □

Example 6.49. Let n_1, n_2 be positive integers with $n_1 \mid n_2$. Consider the natural map $\rho : \mathbb{Z} \to \mathbb{Z}_{n_1}$. This is a surjective group homomorphism with $\operatorname{Ker} \rho = n_1\mathbb{Z}$. Since $H := n_2\mathbb{Z} \subseteq n_1\mathbb{Z}$, we may apply Theorem 6.24 with the subgroup H, obtaining the surjective group homomorphism

$$\begin{aligned} \bar{\rho} : \quad \mathbb{Z}_{n_2} &\to \mathbb{Z}_{n_1} \\ [a]_{n_2} &\mapsto [a]_{n_1}. \quad \square \end{aligned}$$

Example 6.50. Let us revisit Example 6.23. Let n be a positive integer, and let m be any integer. Let $\rho_1 : \mathbb{Z} \to \mathbb{Z}_n$ be the natural map, and let $\rho_2 : \mathbb{Z}_n \to \mathbb{Z}_n$ be the m-multiplication map. The composed map $\rho := \rho_2 \circ \rho_1$ from $\mathbb{Z}$ to $\mathbb{Z}_n$ is also a group homomorphism. For each $z \in \mathbb{Z}$, we have $\rho(z) = m[z]_n = [mz]_n$. The kernel of ρ consists of those integers z such that $mz \equiv 0 \pmod{n}$, and so part (ii) of Theorem 2.5 implies that $\operatorname{Ker} \rho = (n/d)\mathbb{Z}$, where $d := \gcd(m, n)$. The image of ρ is $m\mathbb{Z}_n$. Theorem 6.23 therefore implies that the map

$$\begin{aligned} \bar{\rho} : \quad \mathbb{Z}_{n/d} &\to m\mathbb{Z}_n \\ [z]_{n/d} &\mapsto m[z]_n \end{aligned}$$

is a group isomorphism. □

Example 6.51. Consider the group $\mathbb{Z}_p^*$ where p is an odd prime, and let $\rho : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ be the squaring map. By definition, $\operatorname{Im}\rho = (\mathbb{Z}_p^*)^2$, and we proved in Theorem 2.18 that $\operatorname{Ker}\rho = \{[\pm 1]\}$. Theorem 2.19 says that for all $\gamma, \beta \in \mathbb{Z}_p^*$, $\gamma^2 = \beta^2$ if and only if $\gamma = \pm\beta$. This fact can also be seen to be a special case of part (vi) of Theorem 6.19. Theorem 6.23 says that $\mathbb{Z}_p^*/\operatorname{Ker}\rho \cong \operatorname{Im}\rho$, and since $|\mathbb{Z}_p^*/\operatorname{Ker}\rho| = |\mathbb{Z}_p^*|/|\operatorname{Ker}\rho| = (p-1)/2$, we see that Theorem 2.20, which says that $|(\mathbb{Z}_p^*)^2| = (p-1)/2$, follows from this.

Let $H := (\mathbb{Z}_p^*)^2$, and consider the quotient group $\mathbb{Z}_p^*/H$. Since $|H| = (p-1)/2$, we know that $|\mathbb{Z}_p^*/H| = |\mathbb{Z}_p^*|/|H| = 2$, and hence $\mathbb{Z}_p^*/H$ consists of the two cosets H and $\overline{H} := \mathbb{Z}_p^* \setminus H$.

Let α be an arbitrary, fixed element of $\overline{H}$, and consider the map

$$\begin{aligned} \tau : \quad \mathbb{Z} &\to \mathbb{Z}_p^*/H \\ z &\mapsto [\alpha^z]_H. \end{aligned}$$

It is easy to see that τ is a group homomorphism; indeed, it is the composition of the homomorphism discussed in Example 6.43 and the natural map from $\mathbb{Z}_p^*$ to $\mathbb{Z}_p^*/H$. Moreover, it is easy to see (for example, as a special case of Theorem 2.17) that

$$\alpha^z \in H \iff z \text{ is even.}$$

From this, it follows that $\operatorname{Ker}\tau = 2\mathbb{Z}$; also, since $\mathbb{Z}_p^*/H$ consists of just the two cosets H and $\overline{H}$, it follows that τ is surjective. Therefore, Theorem 6.23 says that the map

$$\begin{aligned} \bar{\tau} : \quad \mathbb{Z}_2 &\to \mathbb{Z}_p^*/H \\ [z]_2 &\mapsto [\alpha^z]_H \end{aligned}$$

is a group isomorphism, under which $[0]_2$ corresponds to H, and $[1]_2$ corresponds to $\overline{H}$.

This isomorphism gives another way to derive Theorem 2.23, which says that in $\mathbb{Z}_p^*$, the product of two non-squares is a square; indeed, the statement "non-zero plus non-zero equals zero in $\mathbb{Z}_2$" translates via the isomorphism $\bar{\tau}$ to the statement "non-square times non-square equals square in $\mathbb{Z}_p^*$." □

Example 6.52. Let $\mathbb{Q}^*$ be the multiplicative group of non-zero rational numbers. Let H_1 be the subgroup $\{\pm 1\}$, and let H_2 be the subgroup of positive rationals. It is easy to see that $\mathbb{Q}^* = H_1 \cdot H_2$ and that $H_1 \cap H_2 = \{1\}$. Thus, $\mathbb{Q}^*$ is the internal direct product of H_1 and H_2, and Theorem 6.25 gives us a group isomorphism $\mathbb{Q}^* \cong H_1 \times H_2$. □

Let G and G' be abelian groups. Recall from Example 6.19 that $\mathrm{Map}(G, G')$ is the group of all functions $\sigma : G \to G'$, where the group operation is defined point-wise using the group operation of G':

$$(\sigma + \tau)(a) = \sigma(a) + \tau(a) \text{ and } (-\sigma)(a) = -\sigma(a)$$

for all $\sigma, \tau \in \mathrm{Map}(G, G')$ and all $a \in G$. The following theorem isolates an important subgroup of this group.

Theorem 6.26. *Let G and G' be abelian groups, and consider the group of functions* $\mathrm{Map}(G, G')$. *Then*

$$\mathrm{Hom}(G, G') := \{\sigma \in \mathrm{Map}(G, G') : \sigma \textit{ is a group homomorphism}\}$$

is a subgroup of $\mathrm{Map}(G, G')$.

Proof. First, observe that $\mathrm{Hom}(G, G')$ is non-empty, as it contains the map that sends everything in G to $0_{G'}$ (this is the identity element of $\mathrm{Map}(G, G')$).

Next, we have to show that if σ and τ are homomorphisms from G to G', then so are $\sigma + \tau$ and $-\sigma$. But $\sigma + \tau = \rho_2 \circ \rho_1$, where $\rho_1 : G \to G' \times G'$ is the map constructed in Theorem 6.21, applied with σ and τ, and $\rho_2 : G' \times G' \to G'$ is as in Example 6.45. Also, $-\sigma = \rho_{-1} \circ \sigma$, where ρ_{-1} is the (-1)-multiplication map. □

EXERCISE 6.22. Verify that the "is isomorphic to" relation on abelian groups is an equivalence relation; that is, for all abelian groups G_1, G_2, G_3, we have:

(a) $G_1 \cong G_1$;

(b) $G_1 \cong G_2$ implies $G_2 \cong G_1$;

(c) $G_1 \cong G_2$ and $G_2 \cong G_3$ implies $G_1 \cong G_3$.

EXERCISE 6.23. Let $\rho_i : G_i \to G_i'$, for $i = 1, \ldots, k$, be group homomorphisms. Show that the map

$$\begin{aligned} \rho : \quad & G_1 \times \cdots \times G_k \to G_1' \times \cdots \times G_k' \\ & (a_1, \ldots, a_k) \mapsto (\rho_1(a_1), \ldots, \rho_k(a_k)) \end{aligned}$$

is a group homomorphism. Also show that if each ρ_i is an isomorphism, then so is ρ.

EXERCISE 6.24. Let $\rho : G \to G'$ be a group homomorphism. Let H, K be subgroups of G and let m be a positive integer. Show that $\rho(H + K) = \rho(H) + \rho(K)$ and $\rho(mH) = m\rho(H)$.

EXERCISE 6.25. Let $\rho : G \to G'$ be a group homomorphism. Let H be a subgroup of G, and let $\tau : H \to G'$ be the restriction of ρ to H. Show that τ is a group homomorphism and that $\mathrm{Ker}\,\tau = \mathrm{Ker}\,\rho \cap H$.

EXERCISE 6.26. Suppose $G_1, \ldots, G_k$ are abelian groups. Show that for each $i = 1, \ldots, k$, the projection map $\pi_i : G_1 \times \cdots \times G_k \to G_i$ that sends $(a_1, \ldots, a_k)$ to a_i is a surjective group homomorphism.

EXERCISE 6.27. Show that if $G = G_1 \times G_2$ for abelian groups G_1 and G_2, and H_1 is a subgroup of G_1 and H_2 is a subgroup of G_2, then we have a group isomorphism $G/(H_1 \times H_2) \cong G_1/H_1 \times G_2/H_2$.

EXERCISE 6.28. Let G be an abelian group with subgroups H and K.

(a) Show that we have a group isomorphism $(H + K)/K \cong H/(H \cap K)$.

(b) Show that if H and K are finite, then $|H + K| = |H||K|/|H \cap K|$.

EXERCISE 6.29. Let G be an abelian group with subgroups H, K, and A, where $K \subseteq H$. Show that $(H \cap A)/(K \cap A)$ is isomorphic to a subgroup of H/K.

EXERCISE 6.30. Let $\rho : G \to G'$ be a group homomorphism with kernel K. Let H be a subgroup of G. Show that we have a group isomorphism $G/(H + K) \cong \rho(G)/\rho(H)$.

EXERCISE 6.31. Let $\rho : G \to G'$ be a surjective group homomorphism. Let $\mathcal{S}$ be the set of all subgroups of G that contain $\operatorname{Ker} \rho$, and let $\mathcal{S}'$ be the set of all subgroups of G'. Show that the sets $\mathcal{S}$ and $\mathcal{S}'$ are in one-to-one correspondence, via the map that sends $H \in \mathcal{S}$ to $\rho(H) \in \mathcal{S}'$. Also show that this correspondence preserves inclusions; that is, for all $H_1, H_2 \in \mathcal{S}$, we have $H_1 \subseteq H_2 \iff \rho(H_1) \subseteq \rho(H_2)$.

EXERCISE 6.32. Use the previous exercise, together with Theorem 6.9, to get a short proof of Theorem 6.10.

EXERCISE 6.33. Show that the homomorphism of Example 6.44 arises by direct application of Example 6.42, combined with Theorems 6.20 and 6.21.

EXERCISE 6.34. Suppose that G, G_1, and G_2 are abelian groups, and that $\rho : G_1 \times G_2 \to G$ is a group isomorphism. Let $H_1 := \rho(G_1 \times \{0_{G_2}\})$ and $H_2 := \rho(\{0_{G_1}\} \times G_2)$. Show that G is the internal direct product of H_1 and H_2.

EXERCISE 6.35. Let $\mathbb{Z}^+$ denote the set of positive integers, and let $\mathbb{Q}^*$ be the multiplicative group of non-zero rational numbers. Consider the abelian groups $\operatorname{Map}^{\#}(\mathbb{Z}^+, \mathbb{Z})$ and $\operatorname{Map}^{\#}(\mathbb{Z}^+, \mathbb{Z}_2)$, as defined in Exercise 6.14. Show that we have group isomorphisms

(a) $\mathbb{Q}^* \cong \mathbb{Z}_2 \times \operatorname{Map}^{\#}(\mathbb{Z}^+, \mathbb{Z})$, and

(b) $\mathbb{Q}^*/(\mathbb{Q}^*)^2 \cong \operatorname{Map}^{\#}(\mathbb{Z}^+, \mathbb{Z}_2)$.

EXERCISE 6.36. Let n be an odd, positive integer whose factorization into primes is $n = p_1^{e_1} \cdots p_r^{e_r}$. Show that:

(a) we have a group isomorphism $\mathbb{Z}_n^*/(\mathbb{Z}_n^*)^2 \cong \mathbb{Z}_2^{\times r}$;

(b) if $p_i \equiv 3 \pmod 4$ for each $i = 1, \ldots, r$, then the squaring map on $(\mathbb{Z}_n^*)^2$ is a group automorphism.

EXERCISE 6.37. Which of the following pairs of groups are isomorphic? Why or why not? (a) $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$, (b) $\mathbb{Z}_{12}^*$ and $\mathbb{Z}_8^*$, (c) $\mathbb{Z}_5^*$ and $\mathbb{Z}_4$, (d) $\mathbb{Z}_2 \times \mathbb{Z}$ and $\mathbb{Z}$, (e) $\mathbb{Q}$ and $\mathbb{Z}$, (f) $\mathbb{Z} \times \mathbb{Z}$ and $\mathbb{Z}$.

6.5 Cyclic groups

Let G be an abelian group. For $a \in G$, define $\langle a \rangle := \{za : z \in \mathbb{Z}\}$. It is easy to see that $\langle a \rangle$ is a subgroup of G; indeed, it is the image of the group homomorphism discussed in Example 6.42. Moreover, $\langle a \rangle$ is the smallest subgroup of G containing a; that is, $\langle a \rangle$ contains a, and every subgroup of G that contains a must contain everything in $\langle a \rangle$. Indeed, if a subgroup contains a, it must contain $a + a = 2a$, $a + a + a = 3a$, and so on; it must also contain $0_G = 0a$, $-a = (-1)a$, $(-a) + (-a) = (-2)a$, and so on. The subgroup $\langle a \rangle$ is called **the subgroup (of G) generated by** a. Also, one defines the **order** of a to be the order of the subgroup $\langle a \rangle$.

More generally, for $a_1, \ldots, a_k \in G$, we define

$$\langle a_1, \ldots, a_k \rangle := \{z_1 a_1 + \cdots + z_k a_k : z_1, \ldots, z_k \in \mathbb{Z}\}.$$

It is easy to see that $\langle a_1, \ldots, a_k \rangle$ is a subgroup of G; indeed, it is the image of the group homomorphism discussed in Example 6.44. Moreover, this subgroup is the smallest subgroup of G that contains $a_1, \ldots, a_k$; that is, $\langle a_1, \ldots, a_k \rangle$ contains the elements $a_1, \ldots, a_k$, and every subgroup of G that contains these elements must contain everything in $\langle a_1, \ldots, a_k \rangle$. The subgroup $\langle a_1, \ldots, a_k \rangle$ is called the **subgroup (of G) generated by** $a_1, \ldots, a_k$.

An abelian group G is called **cyclic** if $G = \langle a \rangle$ for some $a \in G$, in which case, a is called a **generator for** G. An abelian group G is called **finitely generated** if $G = \langle a_1, \ldots, a_k \rangle$ for some $a_1, \ldots, a_k \in G$.

Multiplicative notation: if G is written multiplicatively, then $\langle a \rangle := \{a^z : z \in \mathbb{Z}\}$, and $\langle a_1, \ldots, a_k \rangle := \{a_1^{z_1} \cdots a_k^{z_k} : z_1, \ldots, z_k \in \mathbb{Z}\}$; also, for emphasis and clarity, we use the term **multiplicative order of** a.

Example 6.53. Consider the additive group $\mathbb{Z}$. This is a cyclic group, with 1 being a generator:

$$\langle 1 \rangle = \{z \cdot 1 : z \in \mathbb{Z}\} = \{z : z \in \mathbb{Z}\} = \mathbb{Z}.$$

For every $m \in \mathbb{Z}$, we have

$$\langle m \rangle = \{zm : z \in \mathbb{Z}\} = \{mz : z \in \mathbb{Z}\} = m\mathbb{Z}.$$

It follows that the only elements of $\mathbb{Z}$ that generate $\mathbb{Z}$ are 1 and -1: every other element generates a subgroup that is strictly contained in $\mathbb{Z}$. □

Example 6.54. For $n > 0$, consider the additive group $\mathbb{Z}_n$. This is a cyclic group, with $[1]$ being a generator:

$$\langle [1] \rangle = \{z[1] : z \in \mathbb{Z}\} = \{[z] : z \in \mathbb{Z}\} = \mathbb{Z}_n.$$

For every $m \in \mathbb{Z}$, we have

$$\langle [m] \rangle = \{z[m] : z \in \mathbb{Z}\} = \{[zm] : z \in \mathbb{Z}\} = \{m[z] : z \in \mathbb{Z}\} = m\mathbb{Z}_n.$$

By Example 6.23, the subgroup $m\mathbb{Z}_n$ has order $n/\gcd(m, n)$. Thus, $[m]$ has order $n/\gcd(m, n)$; in particular, $[m]$ generates $\mathbb{Z}_n$ if and only if m is relatively prime to n, and hence, the number of generators of $\mathbb{Z}_n$ is $\varphi(n)$. □

Implicit in Examples 6.53 and 6.54 is the following general fact:

Theorem 6.27. *Let G be a cyclic group generated by a. Then for every $m \in \mathbb{Z}$, we have*

$$\langle ma \rangle = mG.$$

Proof. We have

$$\langle ma \rangle = \{z(ma) : z \in \mathbb{Z}\} = \{m(za) : z \in \mathbb{Z}\} = m\langle a \rangle = mG. \quad \square$$

The following two examples present some groups that are *not* cyclic.

Example 6.55. Consider the additive group $G := \mathbb{Z} \times \mathbb{Z}$. Set

$$\alpha_1 := (1, 0) \in G \text{ and } \alpha_2 := (0, 1) \in G.$$

It is not hard to see that $G = \langle \alpha_1, \alpha_2 \rangle$, since for all $z_1, z_2 \in \mathbb{Z}$, we have

$$z_1\alpha_1 + z_2\alpha_2 = (z_1, 0) + (0, z_2) = (z_1, z_2).$$

However, G is not cyclic. To see this, let $\beta = (b_1, b_2)$ be an arbitrary element of G. We claim that one of α_1 or α_2 does not belong to $\langle \beta \rangle$. Suppose to the contrary that both α_1 and α_2 belong to $\langle \beta \rangle$. This would imply that there exist integers z and z' such that

$$\begin{aligned} zb_1 &= 1, & zb_2 &= 0, \\ z'b_1 &= 0, & z'b_2 &= 1. \end{aligned}$$

Multiplying the upper left equality by the lower right, and the upper right by the lower left, we obtain

$$1 = zz'b_1b_2 = 0,$$

which is impossible. □

Example 6.56. Consider the additive group $G := \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$. Set

$$\alpha_1 := ([1]_{n_1}, [0]_{n_2}) \in G \text{ and } \alpha_2 := ([0]_{n_1}, [1]_{n_2}) \in G.$$

It is not hard to see that $G = \langle \alpha_1, \alpha_2 \rangle$, since for all $z_1, z_2 \in \mathbb{Z}$, we have

$$z_1\alpha_1 + z_2\alpha_2 = ([z_1]_{n_1}, [0]_{n_2}) + ([0]_{n_1}, [z_2]_{n_2}) = ([z_1]_{n_1}, [z_2]_{n_2}).$$

However, G may or may not be cyclic: it depends on $d := \gcd(n_1, n_2)$.

If $d = 1$, then G is cyclic, with $\alpha := ([1]_{n_1}, [1]_{n_2})$ being a generator. One can see this easily using the Chinese remainder theorem: for all $z_1, z_2 \in \mathbb{Z}$, there exists $z \in \mathbb{Z}$ such that

$$z \equiv z_1 \pmod{n_1} \text{ and } z \equiv z_2 \pmod{n_2},$$

which implies

$$z\alpha = ([z]_{n_1}, [z]_{n_2}) = ([z_1]_{n_1}, [z_2]_{n_2}).$$

If $d > 1$, then G is not cyclic. To see this, let $\beta = ([b_1]_{n_1}, [b_2]_{n_2})$ be an arbitrary element of G. We claim that one of α_1 or α_2 does not belong to $\langle \beta \rangle$. Suppose to the contrary that both α_1 and α_2 belong to $\langle \beta \rangle$. This would imply that there exist integers z and z' such that

$$zb_1 \equiv 1 \pmod{n_1}, \qquad zb_2 \equiv 0 \pmod{n_2},$$
$$z'b_1 \equiv 0 \pmod{n_1}, \qquad z'b_2 \equiv 1 \pmod{n_2}.$$

All of these congruences hold modulo d as well, and multiplying the upper left congruence by the lower right, and the upper right by the lower left, we obtain

$$1 \equiv zz'b_1b_2 \equiv 0 \pmod{d},$$

which is impossible. □

It should be clear that since a group isomorphism preserves all structural properties of groups, it preserves the property of being cyclic. We state this, along with related facts, as a theorem.

Theorem 6.28. *Let $\rho : G \to G'$ be a group isomorphism.*

(i) For all $a \in G$, we have $\rho(\langle a \rangle) = \langle \rho(a) \rangle$.

(ii) For all $a \in G$, a and $\rho(a)$ have the same order.

(iii) G is cyclic if and only if G' is cyclic.

Proof. For all $a \in G$, we have

$$\rho(\langle a \rangle) = \{\rho(za) : z \in \mathbb{Z}\} = \{z\rho(a) : z \in \mathbb{Z}\} = \langle \rho(a) \rangle.$$

That proves (i).

(ii) follows from (i) and the fact that ρ is injective.

(iii) follows from (i), as follows. If G is cyclic, then $G = \langle a \rangle$, and since ρ is surjective, we have $G' = \rho(G) = \langle \rho(a) \rangle$. The converse follows by applying the same argument to the inverse isomorphism $\rho^{-1} : G' \to G$. □

Example 6.57. Consider again the additive group $G := \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, discussed in Example 6.56. If $\gcd(n_1, n_2) = 1$, then one can also see that G is cyclic as follows: by the discussion in Example 6.48, we know that G is isomorphic to $\mathbb{Z}_{n_1 n_2}$, and since $\mathbb{Z}_{n_1 n_2}$ is cyclic, so is G. □

Example 6.58. Consider again the subgroup $m\mathbb{Z}_n$ of $\mathbb{Z}_n$, discussed in Example 6.54. One can also see that this is cyclic of order n/d, where $d := \gcd(m, n)$, as follows: in Example 6.50, we constructed an isomorphism between $\mathbb{Z}_{n/d}$ and $m\mathbb{Z}_n$, and this implies $m\mathbb{Z}_n$ is cyclic of order n/d. □

Classification of cyclic groups. Examples 6.53 and 6.54 are extremely important examples of cyclic groups. Indeed, as we shall now demonstrate, every cyclic group is isomorphic either to $\mathbb{Z}$ or to $\mathbb{Z}_n$ for some $n > 0$.

Suppose that G is a cyclic group with generator a. Consider the map $\rho : \mathbb{Z} \to G$ that sends $z \in \mathbb{Z}$ to $za \in G$. As discussed in Example 6.42, this map is a group homomorphism, and since a is a generator for G, it must be surjective. There are two cases to consider.

Case 1: $\operatorname{Ker} \rho = \{0\}$. In this case, ρ is an isomorphism of $\mathbb{Z}$ with G.

Case 2: $\operatorname{Ker} \rho \neq \{0\}$. In this case, since $\operatorname{Ker} \rho$ is a subgroup of $\mathbb{Z}$ different from $\{0\}$, by Theorem 6.9, it must be of the form $n\mathbb{Z}$ for some $n > 0$. Hence, by Theorem 6.23, the map $\bar{\rho} : \mathbb{Z}_n \to G$ that sends $[z]_n$ to za is an isomorphism of $\mathbb{Z}_n$ with G.

Based on this isomorphism, we immediately obtain:

Theorem 6.29. *Let G be an abelian group and let $a \in G$. If there exists a positive integer m such that $ma = 0_G$, then the least such positive integer n is the order of a; in this case, we have:*

- *for every integer z, $za = 0_G$ if and only if n divides z, and more generally, for all integers z_1, z_2, we have $z_1 a = z_2 a$ if and only if $z_1 \equiv z_2 \pmod{n}$;*

- *the subgroup $\langle a \rangle$ consists of the n distinct elements*

$$0 \cdot a, 1 \cdot a, \ldots, (n-1) \cdot a.$$

Otherwise, a has infinite order, and every element of $\langle a \rangle$ can be expressed as za for some unique integer z.

In the case where the group is finite, we can say more:

Theorem 6.30. *Let G be a finite abelian group and let $a \in G$. Then $|G|a = 0_G$ and the order of a divides $|G|$.*

Proof. Since $\langle a \rangle$ is a subgroup of G, by Lagrange's theorem (Theorem 6.15), the order of a divides $|G|$. It then follows by Theorem 6.29 that $|G|a = 0_G$. □

Example 6.59. Let $a, n \in \mathbb{Z}$ with $n > 0$ and $\gcd(a, n) = 1$, and let $\alpha := [a] \in \mathbb{Z}_n^*$. Theorem 6.29 implies that the definition given in this section of the multiplicative order of α is consistent with that given in §2.7. Moreover, Euler's theorem (Theorem 2.13) can be seen as just a special case of Theorem 6.30. Also, note that α is a generator for $\mathbb{Z}_n^*$ if and only if a is a primitive root modulo p. □

Example 6.60. As we saw in Example 6.26, all elements of $\mathbb{Z}_{15}^*$ have multiplicative order dividing 4, and since $\mathbb{Z}_{15}^*$ has order 8, we conclude that $\mathbb{Z}_{15}^*$ is not cyclic. □

Example 6.61. The group $\mathbb{Z}_5^*$ is cyclic, with [2] being a generator:

$$[2]^2 = [4] = [-1], \quad [2]^3 = [-2], \quad [2]^4 = [1]. \quad \square$$

Example 6.62. Based on the calculations in Example 2.9, we may conclude that $\mathbb{Z}_7^*$ is cyclic, with both [3] and [5] being generators. □

Example 6.63. Consider again the additive group $G := \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, discussed in Example 6.56. If $d := \gcd(n_1, n_2) > 1$, then one can also see that G is not cyclic as follows: for every $\beta \in G$, we have $(n_1 n_2/d)\beta = 0_G$, and hence by Theorem 6.29, the order of β divides $n_1 n_2/d$. □

The following two theorems completely characterize the subgroup structure of cyclic groups. Actually, we have already proven most of the results in these two theorems, but nevertheless, they deserve special emphasis.

Theorem 6.31. *Let G be a cyclic group of infinite order.*

(i) G is isomorphic to $\mathbb{Z}$.

(ii) There is a one-to-one correspondence between the non-negative integers and the subgroups of G, where each such integer m corresponds to the cyclic group mG.

(iii) *For every two non-negative integers m, m', we have $mG \subseteq m'G$ if and only if $m' \mid m$.*

Proof. That $G \cong \mathbb{Z}$ was established in our classification of cyclic groups, and so it suffices to prove the other statements of the theorem for $G = \mathbb{Z}$. As we saw in Example 6.53, for every integer m, the subgroup $m\mathbb{Z}$ is cyclic, as it is generated by m. This fact, together with Theorem 6.9, establishes all the other statements. □

Theorem 6.32. *Let G be a cyclic group of finite order n.*

(i) *G is isomorphic to $\mathbb{Z}_n$.*

(ii) *There is a one-to-one correspondence between the positive divisors of n and the subgroups of G, where each such divisor d corresponds to the subgroup dG; moreover, dG is a cyclic group of order n/d.*

(iii) *For each positive divisor d of n, we have $dG = G\{n/d\}$; that is, the kernel of the (n/d)-multiplication map is equal to the image of the d-multiplication map; in particular, $G\{n/d\}$ has order n/d.*

(iv) *For every two positive divisors d, d' of n, we have $dG \subseteq d'G$ if and only if $d' \mid d$.*

(v) *For every positive divisor d of n, the number of elements of order d in G is $\varphi(d)$.*

(vi) *For every integer m, we have $mG = dG$ and $G\{m\} = G\{d\}$, where $d := \gcd(m, n)$.*

Proof. That $G \cong \mathbb{Z}_n$ was established in our classification of cyclic groups, and so it suffices to prove the other statements of the theorem for $G = \mathbb{Z}_n$.

The one-to-one correspondence in part (ii) was established in Theorem 6.10. By the discussion in Example 6.54, it is clear that $d\mathbb{Z}_n$ is generated by $[d]$ and has order n/d.

Part (iii) was established in Example 6.23.

Part (iv) was established in Theorem 6.10.

For part (v), the elements of order d in $\mathbb{Z}_n$ are all contained in $\mathbb{Z}_n\{d\}$, and so the number of such elements is equal to the number of generators of $\mathbb{Z}_n\{d\}$. The group $\mathbb{Z}_n\{d\}$ is cyclic of order d, and so is isomorphic to $\mathbb{Z}_d$, and as we saw in Example 6.54, this group has $\varphi(d)$ generators.

Part (vi) was established in Example 6.23. □

Since cyclic groups are in some sense the simplest kind of abelian group, it is nice to establish some sufficient conditions under which a group must be cyclic. The following three theorems provide such conditions.

Theorem 6.33. *If G is an abelian group of prime order, then G is cyclic.*

Proof. Let $|G| = p$, which, by hypothesis, is prime. Let $a \in G$ with $a \neq 0_G$, and let k be the order of a. As the order of an element divides the order of the group, we have $k \mid p$, and so $k = 1$ or $k = p$. Since $a \neq 0_G$, we must have $k \neq 1$, and so $k = p$, which implies that a generates G. □

Theorem 6.34. *If G_1 and G_2 are finite cyclic groups of relatively prime order, then $G_1 \times G_2$ is also cyclic. In particular, if G_1 is generated by a_1 and G_2 is generated by a_2, then $G_1 \times G_2$ is generated by (a_1, a_2).*

Proof. We give a direct proof, based on Theorem 6.29. Let $n_1 := |G_1|$ and $n_2 := |G_2|$, where $\gcd(n_1, n_2) = 1$. Also, let $a_1 \in G_1$ have order n_1 and $a_2 \in G_2$ have order n_2. We want to show that (a_1, a_2) has order $n_1 n_2$. Applying Theorem 6.29 to (a_1, a_2), we see that the order of (a_1, a_2) is the smallest positive integer k such that $k(a_1, a_2) = (0_{G_1}, 0_{G_2})$. Now, for every integer k, we have $k(a_1, a_2) = (ka_1, ka_2)$, and

$$\begin{aligned}(ka_1, ka_2) = (0_{G_1}, 0_{G_2}) &\iff n_1 \mid k \text{ and } n_2 \mid k \\ &\quad \text{(applying Theorem 6.29 to } a_1 \text{ and } a_2\text{)} \\ &\iff n_1 n_2 \mid k \ \text{(since } \gcd(n_1, n_2) = 1\text{).}\end{aligned}$$

□

Theorem 6.35. *Let G be a cyclic group. Then for every subgroup H of G, both H and G/H are cyclic.*

Proof. The fact that H is cyclic follows from part (ii) of Theorem 6.31 in the case where G is infinite, and part (ii) of Theorem 6.32 in the case where G is finite. If G is generated by a, then it is easy to see that G/H is generated by $[a]_H$. □

The next three theorems are often useful in calculating the order of a group element. The first generalizes Theorem 2.15.

Theorem 6.36. *Let G be an abelian group, let $a \in G$ be of finite order n, and let m be an arbitrary integer. Then the order of ma is $n/\gcd(m, n)$.*

Proof. Let $H := \langle a \rangle$, and $d := \gcd(m, n)$. By Theorem 6.27, we have $\langle ma \rangle = mH$, and by Theorem 6.32, we have $mH = dH$, which has order n/d.

That proves the theorem. Alternatively, we can give a direct proof, based on Theorem 6.29. Applying Theorem 6.29 to ma, we see that the order of ma is the smallest positive integer k such that $k(ma) = 0_G$. Now, for every integer k, we have $k(ma) = (km)a$, and

$$\begin{aligned}(km)a = 0_G &\iff km \equiv 0 \pmod{n} \ \text{(applying Theorem 6.29 to } a\text{)} \\ &\iff k \equiv 0 \pmod{n/\gcd(m, n)} \ \text{(by part (ii) of Theorem 2.5).}\end{aligned}$$

□

Theorem 6.37. *Suppose that a is an element of an abelian group, and for some prime p and integer $e \geq 1$, we have $p^e a = 0_G$ and $p^{e-1} a \neq 0_G$. Then a has order p^e.*

Proof. If m is the order of a, then since $p^e a = 0_G$, we have $m \mid p^e$. So $m = p^f$ for some $f = 0, \ldots, e$. If $f < e$, then $p^{e-1} a = 0_G$, contradicting the assumption that $p^{e-1} a \neq 0_G$. □

Theorem 6.38. *Suppose G is an abelian group with $a_1, a_2 \in G$ such that a_1 is of finite order n_1, a_2 is of finite order n_2, and $\gcd(n_1, n_2) = 1$. Then the order of $a_1 + a_2$ is $n_1 n_2$.*

Proof. Let $H_1 := \langle a_1 \rangle$ and $H_2 := \langle a_2 \rangle$ so that $|H_1| = n_1$ and $|H_2| = n_2$.

First, we claim that $H_1 \cap H_2 = \{0_G\}$. To see this, observe that $H_1 \cap H_2$ is a subgroup of H_1, and so $|H_1 \cap H_2|$ divides n_1; similarly, $|H_1 \cap H_2|$ divides n_2. Since $\gcd(n_1, n_2) = 1$, we must have $|H_1 \cap H_2| = 1$, and that proves the claim.

Using the claim, we can apply Theorem 6.25, obtaining a group isomorphism between $H_1 + H_2$ and $H_1 \times H_2$. Under this isomorphism, the group element $a_1 + a_2 \in H_1 + H_2$ corresponds to $(a_1, a_2) \in H_1 \times H_2$, which by Theorem 6.34 (again using the fact that $\gcd(n_1, n_2) = 1$) has order $n_1 n_2$. □

For an abelian group G, we say that an integer k **kills** G if $kG = \{0_G\}$. Consider the set $\mathcal{K}_G$ of integers that kill G. Evidently, $\mathcal{K}_G$ is a subgroup of $\mathbb{Z}$, and hence of the form $m\mathbb{Z}$ for a uniquely determined non-negative integer m. This integer m is called the **exponent** of G. If $m \neq 0$, then we see that m is the least positive integer that kills G.

The following two theorems state some simple properties of the exponent of a group.

Theorem 6.39. *Let G be an abelian group of exponent m.*

(i) For every integer k, k kills G if and only if $m \mid k$.

(ii) If G has finite order, then m divides $|G|$.

(iii) If $m \neq 0$, then for every $a \in G$, the order of a is finite and divides m.

(iv) If G is cyclic, then the exponent of G is 0 if G is infinite, and is $|G|$ if G is finite.

Proof. Exercise. □

Theorem 6.40. *If G_1 and G_2 are abelian groups of exponents m_1 and m_2, then the exponent of $G_1 \times G_2$ is $\operatorname{lcm}(m_1, m_2)$.*

Proof. Exercise. □

Example 6.64. The additive group $\mathbb{Z}$ has exponent 0. □

Example 6.65. The additive group $\mathbb{Z}_n$ has exponent n. □

Example 6.66. The additive group $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ has exponent $\operatorname{lcm}(n_1, n_2)$. □

Example 6.67. The multiplicative group $\mathbb{Z}_{15}^*$ has exponent 4 (see Example 6.26). □

The next two theorems develop some crucial properties about the structure of finite abelian groups.

Theorem 6.41. *If an abelian group G has non-zero exponent m, then G contains an element of order m. In particular, a finite abelian group is cyclic if and only if its order equals its exponent.*

Proof. The second statement follows immediately from the first. For the first statement, let $m = \prod_{i=1}^{r} p_i^{e_i}$ be the prime factorization of m.

First, we claim that for each $i = 1, \ldots, r$, there exists $a_i \in G$ such that $(m/p_i)a_i \neq 0_G$. Suppose the claim were false: then for some i, $(m/p_i)a = 0_G$ for all $a \in G$; however, this contradicts the minimality property in the definition of the exponent m. That proves the claim.

Let $a_1, \ldots, a_r$ be as in the above claim. Then by Theorem 6.37, $(m/p_i^{e_i})a_i$ has order $p_i^{e_i}$ for each $i = 1, \ldots, r$. Finally, by Theorem 6.38, the group element

$$(m/p_1^{e_1})a_1 + \cdots + (m/p_r^{e_r})a_r$$

has order m. □

Theorem 6.42. *Let G be a finite abelian group of order n. If p is a prime dividing n, then G contains an element of order p.*

Proof. We can prove this by induction on n.

If $n = 1$, then the theorem is vacuously true.

Now assume $n > 1$ and that the theorem holds for all groups of order strictly less than n. Let a be any non-zero element of G, and let m be the order of a. Since a is non-zero, we must have $m > 1$. If $p \mid m$, then $(m/p)a$ is an element of order p, and we are done. So assume that $p \nmid m$ and consider the quotient group G/H, where H is the subgroup of G generated by a. Since H has order m, G/H has order n/m, which is strictly less than n, and since $p \nmid m$, we must have $p \mid (n/m)$. So we can apply the induction hypothesis to the group G/H and the prime p, which says that there is an element $b \in G$ such that the coset $[b]_H \in G/H$ has order p. If ℓ is the order of b, then $\ell b = 0_G$, and so $\ell b \equiv 0_G \pmod{H}$, which implies that the order of $[b]_H$ divides ℓ. Thus, $p \mid \ell$, and so $(\ell/p)b$ is an element of G of order p. □

As a corollary, we have:

Theorem 6.43. *Let G be a finite abelian group. Then the primes dividing the exponent of G are the same as the primes dividing its order.*

Proof. Since the exponent divides the order, every prime dividing the exponent must divide the order. Conversely, if a prime p divides the order, then since there is an element of order p in the group, the exponent must be divisible by p. □

EXERCISE 6.38. Find $\alpha_1, \alpha_2 \in \mathbb{Z}_{15}^*$ such that $\mathbb{Z}_{15}^* = \langle \alpha_1, \alpha_2 \rangle$.

EXERCISE 6.39. Show that $\mathbb{Q}^*$ is not finitely generated.

EXERCISE 6.40. Let G be an abelian group, $a \in G$, and $m \in \mathbb{Z}$, such that $m > 0$ and $ma = 0_G$. Let $m = p_1^{e_1} \cdots p_r^{e_r}$ be the prime factorization of m. For $i = 1, \ldots, r$, let f_i be the largest non-negative integer such that $f_i \leq e_i$ and $m/p_i^{f_i} \cdot a = 0_G$. Show that the order of a is equal to $p_1^{e_1 - f_1} \cdots p_r^{e_r - f_r}$.

EXERCISE 6.41. Let G be an abelian group of order n, and let m be an integer. Show that $mG = G$ if and only if $\gcd(m, n) = 1$.

EXERCISE 6.42. Let H be a subgroup of an abelian group G. Show that:

(a) if H and G/H are both finitely generated, then so is G;

(b) if G is finite, $\gcd(|H|, |G/H|) = 1$, and H and G/H are both cyclic, then G is cyclic.

EXERCISE 6.43. Let G be an abelian group of exponent $m_1 m_2$, where m_1 and m_2 are relatively prime. Show that G is the internal direct product of $m_1 G$ and $m_2 G$.

EXERCISE 6.44. Show how Theorem 2.40 easily follows from Theorem 6.32.

EXERCISE 6.45. As additive groups, $\mathbb{Z}$ is clearly a subgroup of $\mathbb{Q}$. Consider the quotient group $G := \mathbb{Q}/\mathbb{Z}$, and show that:

(a) all elements of G have finite order;

(b) G has exponent 0;

(c) for all positive integers m, we have $mG = G$ and $G\{m\} \cong \mathbb{Z}_m$;

(d) all finite subgroups of G are cyclic.

EXERCISE 6.46. Suppose that G is an abelian group that satisfies the following properties:

(i) for all $m \in \mathbb{Z}$, $G\{m\}$ is either equal to G or is of finite order;

(ii) for some $m \in \mathbb{Z}$, $\{0_G\} \subsetneq G\{m\} \subsetneq G$.

Show that $G\{m\}$ is finite for all non-zero $m \in \mathbb{Z}$.

6.6 The structure of finite abelian groups (∗)

We next state a theorem that classifies all finite abelian groups up to isomorphism.

Theorem 6.44 (Fundamental theorem of finite abelian groups). *A finite abelian group (with more than one element) is isomorphic to a direct product of cyclic groups*

$$\mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_r^{e_r}},$$

where the p_i's are primes (not necessarily distinct) and the e_i's are positive integers. This direct product of cyclic groups is unique up to the order of the factors.

An alternative statement of this theorem is the following:

Theorem 6.45. *A finite abelian group (with more than one element) is isomorphic to a direct product of cyclic groups*

$$\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t},$$

where each $m_i > 1$, and where for $i = 1, \ldots, t-1$, we have $m_i \mid m_{i+1}$. Moreover, the integers $m_1, \ldots, m_t$ are uniquely determined, and m_t is the exponent of the group.

The statements of these theorems are much more important than their proofs, which are a bit technical. Even if the reader does not study the proofs, he is urged to understand what the theorems actually say.

In an exercise below, you are asked to show that these two theorems are equivalent. We now prove Theorem 6.45, which we break into two lemmas, the first of which proves the existence part of the theorem, and the second of which proves the uniqueness part.

Lemma 6.46. *A finite abelian group (with more than one element) is isomorphic to a direct product of cyclic groups*

$$\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t},$$

where each $m_i > 1$, and where for $i = 1, \ldots, t-1$, we have $m_i \mid m_{i+1}$; moreover, m_t is the exponent of the group.

Proof. Let G be a finite abelian group with more than one element, and let m be the exponent of G. By Theorem 6.41, there exists an element $a \in G$ of order m. Let $A = \langle a \rangle$. Then $A \cong \mathbb{Z}_m$. Now, if $A = G$, the lemma is proved. So assume that $A \subsetneq G$.

We will show that there exists a subgroup B of G such that $G = A + B$ and $A \cap B = \{0_G\}$. From this, Theorem 6.25 gives us an isomorphism of G with

$A \times B$. Moreover, the exponent of B is clearly a divisor of m, and so the lemma will follow by induction (on the order of the group).

So it suffices to show the existence of a subgroup B as above. We prove this by contradiction. Suppose that there is no such subgroup, and among all subgroups B such that $A \cap B = \{0_G\}$, assume that B is maximal, meaning that there is no subgroup B' of G such that $B \subsetneq B'$ and $A \cap B' = \{0_G\}$. By assumption $C := A + B \subsetneq G$.

Let d be any element of G that lies outside of C. Consider the quotient group G/C, and let r be the order of $[d]_C \in G/C$. Note that $r > 1$ and $r \mid m$. We shall define a group element d' with slightly nicer properties than d, as follows. Since $rd \in C$, we have $rd = sa + b$ for some $s \in \mathbb{Z}$ and $b \in B$. We claim that $r \mid s$. To see this, note that $0_G = md = (m/r)rd = (m/r)sa + (m/r)b$, and since $A \cap B = \{0_G\}$, we have $(m/r)sa = 0_G$, which can only happen if $r \mid s$. That proves the claim. This allows us to define $d' := d - (s/r)a$. Since $d \equiv d' \pmod{C}$, we see not only that $[d']_C \in G/C$ has order r, but also that $rd' \in B$.

We next show that $A \cap (B + \langle d' \rangle) = \{0_G\}$, which will yield the contradiction we seek, and thus prove the lemma. Because $A \cap B = \{0_G\}$, it will suffice to show that $A \cap (B + \langle d' \rangle) \subseteq B$. Now, suppose we have a group element $b' + xd' \in A$, with $b' \in B$ and $x \in \mathbb{Z}$. Then in particular, $xd' \in C$, and so $r \mid x$, since $[d']_C \in G/C$ has order r. Further, since $rd' \in B$, we have $xd' \in B$, whence $b' + xd' \in B$. □

Lemma 6.47. *Suppose that $G := \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t}$ and $H := \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_t}$ are isomorphic, where the m_i's and n_i's are positive integers (possibly 1) such that $m_i \mid m_{i+1}$ and $n_i \mid n_{i+1}$ for $i = 1, \ldots, t-1$. Then $m_i = n_i$ for $i = 1, \ldots, t$.*

Proof. Clearly, $\prod_i m_i = |G| = |H| = \prod_i n_i$. We prove the lemma by induction on the order of the group. If the group order is 1, then clearly all the m_i's and n_i's must be 1, and we are done. Otherwise, let p be a prime dividing the group order. Now, suppose that p divides $m_r, \ldots, m_t$ but not $m_1, \ldots, m_{r-1}$, and that p divides $n_s, \ldots, n_t$ but not $n_1, \ldots, n_{s-1}$, where $r \leq t$ and $s \leq t$. Evidently, the groups pG and pH are isomorphic. Moreover,

$$pG \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_{r-1}} \times \mathbb{Z}_{m_r/p} \times \cdots \times \mathbb{Z}_{m_t/p},$$

and

$$pH \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_{s-1}} \times \mathbb{Z}_{n_s/p} \times \cdots \times \mathbb{Z}_{n_t/p}.$$

Thus, we see that $|pG| = |G|/p^{t-r+1}$ and $|pH| = |H|/p^{t-s+1}$, from which it follows that $r = s$, and the lemma then follows by induction. □

EXERCISE 6.47. Show that Theorems 6.44 and 6.45 are equivalent; that is, show

that each one implies the other. To do this, give a natural one-to-one correspondence between sequences of prime powers (as in Theorem 6.44) and sequences of integers $m_1, \ldots, m_t$ (as in Theorem 6.45).

EXERCISE 6.48. Using the fundamental theorem of finite abelian groups (either form), give short and simple proofs of Theorems 6.41 and 6.42.

EXERCISE 6.49. In our proof of Euler's criterion (Theorem 2.21), we really only used the fact that $\mathbb{Z}_p^*$ has a unique element of multiplicative order 2. This exercise develops a proof of a generalization of Euler's criterion, based on the fundamental theorem of finite abelian groups. Suppose G is an abelian group of even order n that contains a unique element of order 2.

(a) Show that $G \cong \mathbb{Z}_{2^e} \times \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$, where $e > 0$ and the m_i's are odd integers.

(b) Using part (a), show that $2G = G\{n/2\}$.

EXERCISE 6.50. Let G be a non-trivial, finite abelian group. Let s be the smallest positive integer such that $G = \langle a_1, \ldots, a_s \rangle$ for some $a_1, \ldots, a_s \in G$. Show that s is equal to the value of t in Theorem 6.45. In particular, G is cyclic if and only if $t = 1$.

EXERCISE 6.51. Suppose $G \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t}$. Let p be a prime, and let s be the number of m_i's divisible by p. Show that $G\{p\} \cong \mathbb{Z}_p^{\times s}$.

EXERCISE 6.52. Suppose $G \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t}$ with $m_i \mid m_{i+1}$ for $i = 1, \ldots, t-1$, and that H is a subgroup of G. Show that $H \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_t}$, where $n_i \mid n_{i+1}$ for $i = 1, \ldots, t-1$ and $n_i \mid m_i$ for $i = 1, \ldots, t$.

EXERCISE 6.53. Suppose that G is an abelian group such that for all $m > 0$, we have $mG = G$ and $|G\{m\}| = m^2$ (note that G is not finite). Show that $G\{m\} \cong \mathbb{Z}_m \times \mathbb{Z}_m$ for all $m > 0$. Hint: use induction on the number of prime factors of m.