8

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.

8.1 Definitions, basic properties, and examples

Definition 8.1. *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 8.1, 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 8.2. *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 8.1, 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 8.1, 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 8.1 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* 8.1.** 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* 8.2.** For 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* 8.3.** The set of non-negative integers under addition does not form an abelian group, since additive inverses do not exist for positive integers. $\square$

***Example* 8.4.** The set of integers under multiplication does not form an abelian group, since inverses do not exist for integers other than ± 1. $\square$

***Example* 8.5.** The set of integers $\{\pm 1\}$ under multiplication forms an abelian group, with 1 being the identity, and -1 its own inverse. $\square$

***Example* 8.6.** 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* 8.7.** 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. □

***Example* 8.8.** 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 $[a]_n$. □

***Example* 8.9.** 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* 8.10.** Continuing the previous example, let us set $n = 15$, and enumerate the elements of $\mathbb{Z}_{15}^*$. They are

$$[1], [2], [4], [7], [8], [11], [13], [14].$$

An alternative enumeration is

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

***Example* 8.11.** As another special case, consider $\mathbb{Z}_5^*$. We can enumerate the elements of this groups as

$$[1], [2], [3], [4]$$

or alternatively as

$$[\pm 1], [\pm 2]. \quad \square$$

***Example* 8.12.** For any 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* 8.13.** The set of all arithmetic functions f, such that $f(1) \neq 0$, with multiplication defined by the Dirichlet product (see §2.6) forms an abelian group, where the special arithmetic function I is the identity, and inverses are provided by the result of Exercise 2.27. □

***Example* 8.14.** 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* 8.15.** 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 8.1, but not property (iv). □

***Example* 8.16.** 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). □

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. 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.

If an abelian group G is written additively, then the identity element is denoted by 0_G (or just 0 if G is clear from context), and the inverse of an element $a \in G$ is denoted by $-a$. For $a, b \in G$, $a - b$ denotes $a + (-b)$. If n is a positive integer, then $n \cdot a$ denotes $a + a + \cdots + a$, where there are n terms in the sum—note that $1 \cdot a = a$. Moreover, $0 \cdot a$ denotes 0_G, and if n is a negative integer, then $n \cdot a$ denotes $(-n)(-a)$.

If an abelian group G is written multiplicatively, then the identity element is denoted by 1_G (or just 1 if G is clear from context), and the inverse of an element $a \in G$ is denoted by a^{-1} or $1/a$. As usual, one may write ab in place of $a \cdot b$. For $a, b \in G$, a/b denotes $a \cdot b^{-1}$. If n is a positive integer, then a^n denotes $a \cdot a \cdot \cdots \cdot a$, where there are n terms in the product—note that $a^1 = a$. Moreover, a^0 denotes 1_G, and if n is a negative integer, then a^n denotes $(a^{-1})^{-n}$.

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* 8.17.** The order of the additive group $\mathbb{Z}_n$ is n. □

***Example* 8.18.** The order of the multiplicative group $\mathbb{Z}_n^*$ is $\phi(n)$, where ϕ is Euler's phi function, defined in §2.4. □

***Example* 8.19.** The additive group $\mathbb{Z}$ has infinite order. □

We now record a few more simple but useful properties of abelian groups.

Theorem 8.3. *Let G be an abelian group. Then for all $a, b, c \in G$ and $n, m \in \mathbb{Z}$, 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) $-(-a) = a$;

(v) $(-n)a = -(na) = n(-a)$;

(vi) $(n + m)a = na + ma$;

(vii) $n(ma) = (nm)a = m(na)$;

(viii) $n(a + b) = na + nb$.

Proof. Exercise. □

If $G_1, \ldots, G_k$ are abelian groups, we can form the **direct product** $G := G_1 \times \cdots \times G_k$, 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 G 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 G is in fact an abelian group.

Exercise 8.1. In this exercise, you are to generalize the Möbius inversion formula, discussed in §2.6, to arbitrary abelian groups. Let $\mathcal{F}$ be the set of all functions mapping positive integers to integers. Let G be an abelian group, and let $\mathcal{G}$ be the set of all functions mapping positive integers to elements of G. For $f \in \mathcal{F}$ and $g \in \mathcal{G}$, we can define the Dirichlet product $f \star g \in \mathcal{G}$ as follows:

$$(f \star g)(n) := \sum_{d|n} f(d)g(n/d),$$

the sum being over all positive divisors d of n. Let $I, J, \mu \in \mathcal{F}$ be as defined in §2.6.

(a) Show that for all $f, g \in \mathcal{F}$ and all $h \in \mathcal{G}$, we have $(f \star g) \star h = f \star (g \star h)$.

(b) Show that for all $f \in \mathcal{G}$, we have $I \star f = f$.

(c) Show that for all $f, F \in \mathcal{G}$, we have $F = J \star f$ if and only if $f = \mu \star F$.

8.2 Subgroups

We next introduce the notion of a subgroup.

Definition 8.4. *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 8.5. *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 8.4, 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, satisfy 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 8.4 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. These are not very interesting subgroups. An easy way to sometimes find other, more interesting, subgroups within an abelian group is by using the following two theorems.

Theorem 8.6. *Let G be an abelian group, and let m be an integer. Then $mG := \{ma : a \in G\}$ is a subgroup of G.*

Proof. For $ma, mb \in mG$, we have $ma + mb = m(a+b) \in mG$, and $-(ma) = m(-a) \in mG$. □

Theorem 8.7. *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. 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* 8.20.** For every integer m, the set $m\mathbb{Z}$ is the subgroup of the additive group $\mathbb{Z}$ consisting of all integer multiples of m. 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* 8.21.** 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, $[b]_n \in m\mathbb{Z}_n$ if and only if there exists $x \in \mathbb{Z}$ such that $mx \equiv b \pmod{n}$. By Theorem 2.7, such an x 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

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

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 $[x]_n$ is in $\mathbb{Z}_n\{m\}$ if and only if $mx \equiv 0 \pmod{n}$. By Theorem 2.7, this happens if and only if $x \equiv 0 \pmod{n/d}$, where $d = \gcd(m, n)$ as above. Thus, $\mathbb{Z}_n\{m\}$ consists precisely of the d residue classes

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

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

***Example* 8.22.** For $n = 15$, consider again the table in Example 2.3. 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 the above examples are the *only* subgroups of these groups.

Theorem 8.8. *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 1.7). The first statement of the theorem then follows from Theorem 1.5. The second statement follows easily from the definitions, as was observed in §1.2. □

Theorem 8.9. *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 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. Let $\rho : \mathbb{Z} \to \mathbb{Z}_n$ be the map that sends $a \in \mathbb{Z}$ to $[a]_n \in \mathbb{Z}_n$. Clearly, ρ is surjective. Consider the pre-image $\rho^{-1}(G) \subseteq \mathbb{Z}$ of G.

We claim that $\rho^{-1}(G)$ is a subgroup of $\mathbb{Z}$. To see this, observe that for $a, b \in \mathbb{Z}$, if $[a]_n$ and $[b]_n$ belong to G, then so do $[a+b]_n = [a]_n + [b]_n$ and $-[a]_n = [-a]_n$, and thus $a + b$ and $-a$ belong to the pre-image.

Since $\rho^{-1}(G)$ is a subgroup of $\mathbb{Z}$, by the previous theorem, we have $\rho^{-1}(G) = d\mathbb{Z}$ for some non-negative integer d. Moreover, it is clear that $n \in \rho^{-1}(G)$, and hence $d \mid n$. That proves the existence part of the theorem.

Next, we claim that for any divisor d of n, we have $\rho^{-1}(d\mathbb{Z}_n) = d\mathbb{Z}$. To see this, note that $\rho^{-1}(d\mathbb{Z}_n)$ consists of all integers b such that $dx \equiv b \pmod{n}$ has an integer solution x, and by Theorem 2.7, this congruence admits a solution if and only if $d \mid b$. That proves the claim.

Now consider any two positive divisors d_1, d_2 of n. Since $d_1\mathbb{Z}_n \subseteq d_2\mathbb{Z}_n$ if and only if $\rho^{-1}(d_1\mathbb{Z}_n) \subseteq \rho^{-1}(d_2\mathbb{Z}_n)$, the remaining statements of the theorem follow from the corresponding statements of Theorem 8.8 and the above claim. □

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

***Example* 8.23.** Consider the group $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. For any non-zero $\alpha \in G$, $\alpha + \alpha = 0_G$. From this, it is easy to see that the set $H = \{0_G, \alpha\}$ is a subgroup of G. However, for any 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* 8.24.** Consider again the group $\mathbb{Z}_n^*$, for $n = 15$, discussed in Example 8.10. As discussed there, we have $\mathbb{Z}_{15}^* = \{[\pm 1], [\pm 2], [\pm 4], [\pm 7]\}$.

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 integer m, write $m = 4q + r$, where $0 \leq r < 4$. Then for any $\alpha \in \mathbb{Z}_{15}^*$, 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* 8.25.** Consider again the group $\mathbb{Z}_5^*$ from Example 8.11. As discussed there, $\mathbb{Z}_5^* = \{[\pm 1], [\pm 2]\}$. Therefore, 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* 8.26.** Consider again the group of arithmetic functions f, such that $f(1) \neq 0$, with multiplication defined by the Dirichlet product, discussed in Example 8.13. By the results of Exercises 2.21 and 2.28, we see that the subset of all multiplicative arithmetic functions is a subgroup of this group. □

The following two theorems may be used to simplify verifying that a subset is a subgroup.

Theorem 8.10. *If G is an abelian group, and H is a non-empty subset of G such that $a - b \in H$ for all $a, b \in H$, then H is a subgroup of G.*

Proof. Since H is non-empty, let c be an arbitrary element of H. Then $0_G = c - c \in H$. It follows that for all $a \in H$, we have $-a = 0_G - a \in H$, and for all $a, b \in H$, we have $a + b = a - (-b) \in H$. □

Theorem 8.11. *If G is an abelian group, and H is a non-empty, finite subset of G such that $a + b \in H$ for all $a, b \in H$, then H is a subgroup of G.*

Proof. We only need to show that $-a \in H$ for all $a \in H$. Let $a \in H$ be given. If $a = 0_G$, then clearly $-a = 0_G \in H$, so assume that $a \neq 0_G$, and consider the set S of all elements of G of the form ma, for $m = 1, 2, \ldots$. Since H is closed under addition, it follows that $S \subseteq H$. Moreover, since H is finite, S must be finite, and hence there must exist integers m_1, m_2 such that $m_1 > m_2 > 0$ and $m_1 a = m_2 a$; that is, $ra = 0_G$, where $r := m_1 - m_2 > 0$. We may further assume that $r > 1$, since otherwise $a = 0_G$, and we are assuming that $a \neq 0_G$. It follows that $a + (r-1)a = 0_G$, and so $-a = (r-1)a \in S$. □

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

Theorem 8.12. *If H_1 and H_2 are subgroups of an abelian group G, then so is*

$$H_1 + H_2 := \{h_1 + h_2 : h_1 \in H_1, h_2 \in H_2\}.$$

Proof. Consider two elements in $H_1 + H_2$, which we can write as $h_1 + h_2$ and $h_1' + h_2'$, where $h_1, h_1' \in H_1$ and $h_2, h_2' \in H_2$. Then by the closure properties of subgroups, $h_1 + h_1' \in H_1$ and $h_2 + h_2' \in H_2$, and hence $(h_1 + h_2) + (h_1' + h_2') = (h_1 + h_1') + (h_2 + h_2') \in H_1 + H_2$. Similarly, $-(h_1 + h_2) = (-h_1) + (-h_2) \in H_1 + H_2$. □

Multiplicative notation: if the abelian group G in the above theorem is written multiplicatively, then the subgroup defined in the theorem is written $H_1 \cdot H_2 := \{h_1 h_2 : h_1 \in H_1,\ h_2 \in H_2\}$.

Theorem 8.13. *If H_1 and H_2 are subgroups of an abelian group G, then so is $H_1 \cap H_2$.*

Proof. If $h \in H_1 \cap H_2$ and $h' \in H_1 \cap H_2$, then since $h, h' \in H_1$, we have $h + h' \in H_1$, and since $h, h' \in H_2$, we have $h + h' \in H_2$; therefore, $h + h' \in H_1 \cap H_2$. Similarly, $-h \in H_2$ and $-h \in H_2$, and therefore, $-h \in H_1 \cap H_2$. □

Exercise 8.2. Show that if H' is a subgroup of an abelian group G, then a set $H \subseteq H'$ is a subgroup of G if and only if H is a subgroup of H'.

Exercise 8.3. Let G be an abelian group with subgroups H_1 and H_2. Show that any subgroup H of G that contains $H_1 \cup H_2$ contains $H_1 + H_2$, and $H_1 \subseteq H_2$ if and only if $H_1 + H_2 = H_2$.

Exercise 8.4. 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 8.5. Let G_1 and G_2 be abelian groups, and let H be a subgroup of $G_1 \times G_2$. Define

$$H_1 := \{h_1 \in G_1 : (h_1, h_2) \in H \text{ for some } h_2 \in G_2\}.$$

Show that H_1 is a subgroup of G_1.

EXERCISE 8.6. Give an example of specific abelian groups G_1 and G_2, along with a subgroup H of $G_1 \times G_2$, such that H cannot be written as $H_1 \times H_2$, where H_1 is a subgroup of G_1 and H_2 is a subgroup of G_2.

8.3 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 $h \in H$.

Analogously 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 8.14. *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. It is easy to see (verify) that for any $a \in G$, the equivalence class containing a is precisely the set $a+H := \{a+h : h \in H\}$, and this set is called the **coset of H in G containing** a, and an element of such a coset is called a **representative** of the coset.

Multiplicative notation: if G is written multiplicatively, then $a \equiv b \pmod{H}$ means $a/b \in H$, and the coset of H in G containing a is $aH := \{ah : h \in H\}$.

***Example* 8.27.** 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 $[a]_n$. □

***Example* 8.28.** Let $G := \mathbb{Z}_4$ and let H be the subgroup $2G = \{[0], [2]\}$ of G. The coset of H containing $[1]$ is $\{[1], [3]\}$. These are all the cosets of H in G. □

Theorem 8.15. *Any two cosets of a subgroup H in an abelian group G have equal cardinality; that is, there is a bijective map from one coset to the other.*

Proof. It suffices to exhibit a bijection between H and $a + H$ for any $a \in G$. The map $f_a : H \to a + H$ that sends $h \in H$ to $a + h$ is easily seen to be just such a bijection. □

An incredibly useful consequence of the above theorem is:

Theorem 8.16 (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 8.17. *Let G be an abelian group and H a subgroup. For $a, a', b, b' \in G$, if $a \equiv a' \pmod{H}$ and $b \equiv b' \pmod{H}$, then $a + b \equiv a' + b' \pmod{H}$.*

Proof. Now, $a \equiv a' \pmod{H}$ and $b \equiv b' \pmod{H}$ means that $a' = a + h_1$ and $b' = b + h_2$ for $h_1, h_2 \in H$. Therefore, $a' + b' = (a + h_1) + (b + h_2) = (a + b) + (h_1 + h_2)$, and since $h_1 + h_2 \in H$, this means that $a + b \equiv a' + b' \pmod{H}$. □

Let G be an abelian group and H a subgroup. Theorem 8.17 allows us to define a binary operation on the collection of cosets of H in G in the following natural way: for $a, b \in G$, define

$$(a + H) + (b + H) := (a + b) + H.$$

The fact that this definition is unambiguous follows immediately from Theorem 8.17. Also, one can easily verify that this operation defines an abelian group, where H acts as the identity element, and the inverse of a coset $a + H$ is $(-a) + H$. The resulting group is called the **quotient group of G modulo H**, and is denoted G/H. The order of the group G/H is sometimes denoted $[G : H]$ and is called the **index of H in G**.

Multiplicative notation: if G is written multiplicatively, then the definition of the group operation of G/H is expressed

$$(aH) \cdot (bH) := (ab)H.$$

Theorem 8.18. *Let G be a finite abelian group and H a subgroup. Then $[G : H] = |G|/|H|$. Moreover, if H' is another subgroup of G with $H \subseteq H'$, then*

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

Proof. The fact that $[G : H] = |G|/|H|$ follows directly from Theorem 8.15. The fact that $[G : H] = [G : H'][H' : G]$ follows from a simple calculation:

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

***Example* 8.29.** For the additive group of integers $\mathbb{Z}$ and the subgroup $n\mathbb{Z}$ for $n > 0$, the quotient group $\mathbb{Z}/n\mathbb{Z}$ is precisely the same as the additive group $\mathbb{Z}_n$ that we have already defined. For $n = 0$, $\mathbb{Z}/n\mathbb{Z}$ is essentially just a "renaming" of $\mathbb{Z}$. $\square$

***Example* 8.30.** Let $G := \mathbb{Z}_6$ and $H = 3G$ be the subgroup of G consisting of the two elements $\{[0], [3]\}$. The cosets of H in G are $\alpha := H = \{[0], [3]\}$, $\beta := [1] + H = \{[1], [4]\}$, and $\gamma := [2] + H = \{[2], [5]\}$. 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 8.17: for any 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* 8.31.** Let us return to Example 8.24. The 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 $\alpha_{00} = \{[1], [4]\}$, $\alpha_{01} = \{[-1], [-4]\}$, $\alpha_{10} = \{[2], [-7]\}$, and $\alpha_{11} = \{[7], [-2]\}$. In the quotient group, α_{00} is the identity; moreover, we have

$$\alpha_{01}^2 = \alpha_{10}^2 = \alpha_{11}^2 = \alpha_{00}$$

and

$$\alpha_{01}\alpha_{10} = \alpha_{11},\ \alpha_{10}\alpha_{11} = \alpha_{01},\ \alpha_{01}\alpha_{11} = \alpha_{10}.$$

This completely describes the behavior of the group operation of the quotient group. Note that this group is essentially just a "renaming" of the group $\mathbb{Z}_2 \times \mathbb{Z}_2$. □

***Example* 8.32.** As we saw in Example 8.25, $(\mathbb{Z}_5^*)^2 = \{[\pm 1]\}$. 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 $\alpha_1 = \{[\pm 2]\}$. In the group $\mathbb{Z}_5^*/(\mathbb{Z}_5^*)^2$, α_0 is the identity, and α_1 is its own inverse, and we see that this group is essentially just a "renaming" of $\mathbb{Z}_2$. □

EXERCISE 8.7. Let H be a subgroup of an abelian group G, and let a and a' be elements of G, with $a \equiv a' \pmod{H}$.

(a) Show that $-a \equiv -a' \pmod{H}$.

(b) Show that $na \equiv na' \pmod{H}$ for all $n \in \mathbb{Z}$.

EXERCISE 8.8. 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 8.9. Let H be a subgroup of an abelian group G.

(a) Show that if H' is a subgroup of G containing H, then H'/H is a subgroup of G/H.

(b) Show that if K is a subgroup of G/H, then the set $H' := \{a \in G : a + H \in K\}$ is a subgroup of G containing H.

8.4 Group homomorphisms and isomorphisms

Definition 8.19. *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 understanding 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: $\mathrm{img}(\rho)$ denotes the image of ρ, and $\ker(\rho)$ denotes the kernel of ρ.

***Example* 8.33.** For any abelian group G and any integer m, the map that sends $a \in G$ to $ma \in G$ is clearly a group homomorphism from G into G, since for $a, b \in G$, we have $m(a+b) = ma + mb$. The image of this homomorphism is mG and the kernel is $G\{m\}$. We call this map the **m-multiplication map on G**. If G is written multiplicatively, we call this the **m-power map on G**, and its image is G^m. □

***Example* 8.34.** Consider the m-multiplication map on $\mathbb{Z}_n$. As we saw in Example 8.21, if $d := \gcd(n, m)$, 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* 8.35.** Let G be an abelian group and let a be a fixed element of G. Let $\rho : \mathbb{Z} \to G$ be the map that sends $z \in \mathbb{Z}$ to $za \in G$. It is easy to see that this is group homomorphism, since

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

***Example* 8.36.** 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 $\alpha^z \in \mathbb{Z}_n^*$. If the multiplicative order of α is equal to k, then as discussed in §2.5, 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 a such that $\alpha^a = [1]_n$. Again by the discussion in §2.5, the kernel of ρ is equal to $k\mathbb{Z}$. □

***Example* 8.37.** We may generalize Example 8.35 as follows. Let G be an abelian group, and let $a_1, \ldots, a_k$ be fixed elements of G. Let $\rho : \mathbb{Z}^{\times k} \to G$

be the map that sends $(z_1, \ldots, z_k) \in \mathbb{Z}^{\times k}$ to $z_1 a_1 + \cdots + z_k a_k \in G$. The reader may easily verify that ρ is a group homomorphism. □

***Example* 8.38.** As a special case of the previous example, let $p_1, \ldots, p_k$ be distinct primes, and let $\rho : \mathbb{Z}^{\times k} \to \mathbb{Q}^*$ be the group homomorphism that sends $(z_1, \ldots, z_k) \in \mathbb{Z}^{\times k}$ to $p_1^{z_1} \cdots p_k^{z_k} \in \mathbb{Q}^*$. The image of ρ is the set of all non-zero fractions whose numerator and denominator are divisible only by the primes $p_1, \ldots, p_k$. The kernel of ρ contains only the all-zero tuple $0^{\times k}$. □

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

Theorem 8.20. *Let ρ be a group homomorphism from G to G'.*

(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) For any subgroup H of G, $\rho(H)$ is a subgroup of G'.

(v) $\ker(\rho)$ *is a subgroup of* G.

(vi) For all $a, b \in G$, $\rho(a) = \rho(b)$ if and only if $a \equiv b \pmod{\ker(\rho)}$.

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

(viii) For any subgroup H' of G', $\rho^{-1}(H')$ is a subgroup of G containing $\ker(\rho)$.

Proof.

(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 (using part (i) of Theorem 8.3).

(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 (v) of Theorem 8.3.

(iv) For any $a, b \in H$, 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) If $\rho(a) = 0_{G'}$ and $\rho(b) = 0_{G'}$, then $\rho(a+b) = \rho(a)+\rho(b) = 0_{G'}+0_{G'} = 0_{G'}$, and $\rho(-a) = -\rho(a) = -0_{G'} = 0_{G'}$.

(vi) $\rho(a) = \rho(b)$ iff $\rho(a) - \rho(b) = 0_{G'}$ iff $\rho(a-b) = 0_{G'}$ iff $a - b \in \ker(\rho)$ iff $a \equiv b \pmod{\ker(\rho)}$.

(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), $\ker(\rho)$ contains the element $a - b$, which is non-zero.

(viii) This is very similar to part (v). If $\rho(a) \in H'$ and $\rho(b) \in H'$, then $\rho(a + b) = \rho(a) + \rho(b) \in H'$, and $\rho(-a) = -\rho(a) \in H'$. Moreover, since H' contains $0_{G'}$, we must have $\rho^{-1}(H') \supseteq \rho^{-1}(\{0_{G'}\}) = \ker(\rho)$.

□

Part (vii) of the above theorem is particular useful: to check that a group homomorphism is injective, it suffices to determine if $\ker(\rho) = \{0_G\}$. 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 $\ker(\rho) = \{0_G\}$;
- ρ is surjective if and only if $\mathrm{img}(\rho) = G'$.

The next three theorems establish some further convenient facts about group homomorphisms.

Theorem 8.21. *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 $a, b \in G$, we have $\rho'(\rho(a + b)) = \rho'(\rho(a) + \rho(b)) = \rho'(\rho(a)) + \rho'(\rho(b))$. □

Theorem 8.22. *Let $\rho_i : G \to G_i$, for $i = 1, \ldots, n$, be group homomorphisms. Then the map $\rho : G \to G_1 \times \cdots \times G_n$ that sends $a \in G$ to $(\rho_1(a), \ldots, \rho_n(a))$ is a group homomorphism with kernel $\ker(\rho_1) \cap \cdots \cap \ker(\rho_n)$.*

Proof. Exercise. □

Theorem 8.23. *Let $\rho_i : G_i \to G$, for $i = 1, \ldots, n$, be group homomorphisms. Then the map $\rho : G_1 \times \cdots \times G_n \to G$ that sends $(a_1, \ldots, a_n)$ to $\rho_1(a_1) + \cdots + \rho_n(a_n)$ is a group homomorphism.*

Proof. Exercise. □

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 8.24. *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 $a', b' \in G'$, we have

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

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

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 of G with G' is essentially just a "renaming" of the group elements — all structural properties of the group are preserved, even though the two groups might look quite different superficially.

***Example* 8.39.** As was shown in Example 8.30, the quotient group G/H discussed in that example is isomorphic to $\mathbb{Z}_3$. As was shown in Example 8.31, 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 8.32, the quotient group $\mathbb{Z}_5^*/(\mathbb{Z}_5^*)^2$ is isomorphic to $\mathbb{Z}_2$. □

***Example* 8.40.** If $\gcd(n, m) = 1$, then the m-multiplication map on $\mathbb{Z}_n$ is a group automorphism. □

The following four theorems provide important constructions of group homomorphisms.

Theorem 8.25. *If H is a subgroup of an abelian group G, then the map $\rho : G \to G/H$ given by $\rho(a) = a + H$ is a surjective group homomorphism whose kernel is H.*

Proof. This really just follows from the definition of the quotient group. To verify that ρ is a group homomorphism, note that

$$\rho(a + b) = (a + b) + H = (a + H) + (b + H) = \rho(a) + \rho(b).$$

Surjectivity follows from the fact that every coset is of the form $a + H$ for some $a \in G$. The fact that $\ker(\rho) = H$ follows from the fact that $a + H$ is the coset of H in G containing a, and so this is equal to H if and only if $a \in H$. □

The homomorphism of the above theorem is called the **natural map** from G to G/H.

Theorem 8.26. *Let ρ be a group homomorphism from G into G'. Then the map $\bar{\rho} : G/\ker(\rho) \to \mathrm{img}(\rho)$ that sends the coset $a + \ker(\rho)$ for $a \in G$ to $\rho(a)$ is unambiguously defined and is a group isomorphism of $G/\ker(\rho)$ with $\mathrm{img}(\rho)$.*

Proof. Let $K := \ker(\rho)$. To see that the definition $\bar{\rho}$ is unambiguous, note that if $a \equiv a' \pmod{K}$, then by part (vi) of Theorem 8.20, $\rho(a) = \rho(a')$. To see that $\bar{\rho}$ is a group homomorphism, note that

$$\begin{aligned}\bar{\rho}((a+K)+(b+K)) &= \bar{\rho}((a+b)+K) = \rho(a+b) = \rho(a)+\rho(b)\\ &= \bar{\rho}(a+K)+\bar{\rho}(b+K).\end{aligned}$$

It is clear that $\bar{\rho}$ maps onto $\mathrm{img}(\rho)$, since any element of $\mathrm{img}(\rho)$ 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 injective, suppose that $\bar{\rho}(a+K) = 0_{G'}$; then we have $\rho(a) = 0_{G'}$, and hence $a \in K$; from this, it follows that $a+K$ is equal to K, which is the zero element of G/K. Injectivity then follows from part (vii) of Theorem 8.20, applied to $\bar{\rho}$. □

The following theorem is an easy generalization of the previous one.

Theorem 8.27. *Let ρ be a group homomorphism from G into G'. Then for any subgroup H contained in $\ker(\rho)$, the map $\bar{\rho} : G/H \to \mathrm{img}(\rho)$ that sends the coset $a + H$ for $a \in G$ to $\rho(a)$ is unambiguously defined and is a group homomorphism from G/H onto $\mathrm{img}(\rho)$ with kernel $\ker(\rho)/H$.*

Proof. Exercise—just mimic the proof of the previous theorem. □

Theorem 8.28. *Let G be an abelian group with subgroups H_1, H_2. Then the map $\rho : H_1 \times H_2 \to H_1 + H_2$ that sends (h_1, h_2) to $h_1 + h_2$ is a surjective group homomorphism. Moreover, if $H_1 \cap H_2 = \{0_G\}$, then ρ is a group isomorphism of $H_1 \times H_2$ with $H_1 + H_2$.*

Proof. The fact that ρ is a group homomorphism is just a special case of Theorem 8.23, applied to the inclusion maps $\rho_1 : H_1 \to H_1 + H_2$ and $\rho_2 : H_2 \to H_1 + H_2$. One can also simply verify this by direct calculation: for $h_1, h_1' \in H_1$ and $h_2, h_2' \in H_2$, we have

$$\begin{aligned}\rho(h_1 + h_1', h_2 + h_2') &= (h_1 + h_1') + (h_2 + h_2')\\ &= (h_1 + h_2) + (h_1' + h_2')\\ &= \rho(h_1, h_2) + \rho(h_1', \rho_2').\end{aligned}$$

Moreover, from the definition of $H_1 + H_2$, we see that ρ is in fact surjective.

Now assume that $H_1 \cap H_2 = \{0_G\}$. To see that ρ is injective, it suffices

to show that $\ker(\rho)$ is trivial; that is, it suffices to show that for all $h_1 \in H_1$ and $h_2 \in H_2$, $h_1 + h_2 = 0_G$ implies $h_1 = 0_G$ and $h_2 = 0_G$. But $h_1 + h_2 = 0_G$ implies $h_1 = -h_2 \in H_2$, and hence $h_1 \in H_1 \cap H_2 = \{0_G\}$, and so $h_1 = 0_G$. Similarly, one shows that $h_2 = 0_G$, and that finishes the proof. □

***Example* 8.41.** For $n \geq 1$, the natural map ρ 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* 8.42.** We may restate the Chinese remainder theorem (Theorem 2.8) in more algebraic terms. Let $n_1, \ldots, n_k$ be pairwise relatively prime, positive integers. Consider the map from the group $\mathbb{Z}$ to the group $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ that sends $x \in \mathbb{Z}$ to $([x]_{n_1}, \ldots, [x]_{n_k})$. It is easy to see that this map is a group homomorphism (this follows from Example 8.41 and Theorem 8.22). In our new language, the Chinese remainder theorem says that this group homomorphism is surjective and that the kernel is $n\mathbb{Z}$, where $n = \prod_{i=1}^{k} n_i$. Therefore, by Theorem 8.26, the map that sends $[x]_n \in \mathbb{Z}_n$ to $([x]_{n_1}, \ldots, [x]_{n_k})$ is a group isomorphism of the group $\mathbb{Z}_n$ with the group $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$. □

***Example* 8.43.** Let n_1, n_2 be positive integers with $n_1 > 1$ and $n_1 \mid n_2$. Then the map $\bar{\rho} : \mathbb{Z}_{n_2} \to \mathbb{Z}_{n_1}$ that sends $[a]_{n_2}$ to $[a]_{n_1}$ is a surjective group homomorphism, and $[a]_{n_2} \in \ker(\bar{\rho})$ if and only if $n_1 \mid a$; that is, $\ker(\bar{\rho}) = n_1\mathbb{Z}_{n_2}$. The map $\bar{\rho}$ can also be viewed as the map obtained by applying Theorem 8.27 with the natural map ρ from $\mathbb{Z}$ to $\mathbb{Z}_{n_1}$ and the subgroup $n_2\mathbb{Z}$ of $\mathbb{Z}$, which is contained in $\ker(\rho) = n_1\mathbb{Z}$. □

***Example* 8.44.** Let us reconsider Example 8.21. Let n be a positive integer, let $m \in \mathbb{Z}$, and consider the subgroup $m\mathbb{Z}_n$ of the additive group $\mathbb{Z}_n$. 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. The kernel of ρ consists of those integers a such that $am \equiv 0 \pmod{n}$, and so Theorem 2.7 implies that $\ker(\rho) = (n/d)\mathbb{Z}$, where $d := \gcd(m, n)$. The image of ρ is $m\mathbb{Z}_n$. Theorem 8.26 therefore implies that the map $\bar{\rho} : \mathbb{Z}_{n/d} \to m\mathbb{Z}_n$ that sends $[a]_{n/d}$ to $[ma]_n$ is a group isomorphism. □

Exercise 8.10. 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 8.11. Let G_1, G_2 be abelian groups, and let $\rho : G_1 \times G_2 \to G_1$ be the map that sends $(a_1, a_2) \in G_1 \times G_2$ to $a_1 \in G_1$. Show that ρ is a surjective group homomorphism whose kernel is $\{0_{G_1}\} \times G_2$.

EXERCISE 8.12. 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

(a) H_1 and H_2 are subgroups of G,

(b) $H_1 + H_2 = G$, and

(c) $H_1 \cap H_2 = \{0_G\}$.

EXERCISE 8.13. Let ρ be a group homomorphism from G into G'. Show that for any subgroup H of G, we have $\rho^{-1}(\rho(H)) = H + \ker(\rho)$.

EXERCISE 8.14. Let ρ be a group homomorphism from G into G'. Show that the subgroups of G containing $\ker(\rho)$ are in one-to-one correspondence with the subgroups of $\mathrm{img}(\rho)$, where the subgroup H of G containing $\ker(\rho)$ corresponds to the subgroup $\rho(H)$ of $\mathrm{img}(\rho)$.

EXERCISE 8.15. Let G be an abelian group with subgroups $H \subseteq H'$.

(a) Show that we have a group isomorphism

$$G/H' \cong \frac{G/H}{H'/H}.$$

(b) Show that if $[G : H]$ is finite (even though G itself may have infinite order), then $[G : H] = [G : H'] \cdot [H' : H]$.

EXERCISE 8.16. 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 $G/(H_1 \times H_2) \cong G_1/H_1 \times G_2/H_2$.

EXERCISE 8.17. Let ρ_1 and ρ_2 be group homomorphisms from G into G'. Show that the map $\rho : G \to G'$ that sends $a \in G$ to $\rho_1(a) + \rho_2(a) \in G'$ is also a group homomorphism.

EXERCISE 8.18. Let G and G' be abelian groups. Consider the set H of all group homomorphisms $\rho : G \to G'$. This set is non-empty, since the map that sends everything in G to $0_{G'}$ is trivially an element of H. We may define an addition operation on H as follows: for $\rho_1, \rho_2 \in H$, let $\rho_1 + \rho_2$ be the map $\rho : G \to G'$ that sends $a \in G$ to $\rho_1(a) + \rho_2(a)$. By the previous exercise, ρ is

also in H, and so this addition operation is a well-defined binary operation on H. Show that H, together with this addition operation, forms an abelian group.

EXERCISE 8.19. This exercise develops an alternative, "quick and dirty" proof of the Chinese remainder theorem, based on group theory and a counting argument. Let $n_1, \ldots, n_k$ be pairwise relatively prime, positive integers, and let $n := n_1 \cdots n_k$. Consider the map $\rho : \mathbb{Z} \to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ that sends $x \in \mathbb{Z}$ to $([x]_{n_1}, \ldots, [x]_{n_k})$.

(a) Using the results of Example 8.41 and Theorem 8.22, show (directly) that ρ is a group homomorphism with kernel $n\mathbb{Z}$.

(b) Using Theorem 8.26, conclude that the map $\bar{\rho}$ given by that theorem, which sends $[x]_n$ to $([x]_{n_1}, \ldots, [x]_{n_k})$, is an injective group homomorphism from $\mathbb{Z}_n$ into $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$.

(c) Since $|\mathbb{Z}_n| = n = |\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}|$, conclude that the map $\bar{\rho}$ is surjective, and so is an isomorphism between $\mathbb{Z}_n$ and $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$.

Although simple, this proof does not give us an explicit formula for computing $\bar{\rho}^{-1}$.

EXERCISE 8.20. Let p be an odd prime; consider the squaring map on $\mathbb{Z}_p^*$.

(a) Using Exercise 2.5, show that the kernel of the squaring map on $\mathbb{Z}_p^*$ consists of the two elements $[\pm 1]_p$.

(b) Using the results of this section, conclude that there are $(p-1)/2$ squares in $\mathbb{Z}_p^*$, each of which has precisely two square roots in $\mathbb{Z}_p^*$.

EXERCISE 8.21. Consider the group homomorphism $\rho : \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \to \mathbb{Q}^*$ that sends (a, b, c) to $2^a 3^b 12^c$. Describe the image and kernel of ρ.

EXERCISE 8.22. This exercise develops some simple—but extremely useful—connections between group theory and probability theory. Let $\rho : G \to G'$ be a group homomorphism, where G and G' are finite abelian groups.

(a) Show that if g is a random variable with the uniform distribution on G, then $\rho(g)$ is a random variable with the uniform distribution on $\mathrm{img}(\rho)$.

(b) Show that if g is a random variable with the uniform distribution on G, and g' is a fixed element in $\mathrm{img}(\rho)$, then the conditional distribution of g, given that $\rho(g) = g'$, is the uniform distribution on $\rho^{-1}(\{g'\})$.

(c) Show that if g_1' is a fixed element of G', g_1 is uniformly distributed

over $\rho^{-1}(\{g_1'\})$, g_2' is a fixed element of G', and g_2 is a fixed element of $\rho^{-1}(\{g_2'\})$, then $g_1 + g_2$ is uniformly distributed over $\rho^{-1}(\{g_1' + g_2'\})$.

(d) Show that if g_1' is a fixed element of G', g_1 is uniformly distributed over $\rho^{-1}(\{g_1'\})$, g_2' is a fixed element of G', g_2 is uniformly distributed over $\rho^{-1}(\{g_2'\})$, and g_1 and g_2 are independent, then $g_1 + g_2$ is uniformly distributed over $\rho^{-1}(\{g_1' + g_2'\})$.

8.5 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 8.35. Moreover, $\langle a \rangle$ is the smallest subgroup of G containing a; that is, $\langle a \rangle$ contains a, and any subgroup H of G that contains a must also contain $\langle a \rangle$. 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 $\langle a_1, \ldots, a_k \rangle := \{z_1 a_1 + \cdots + z_k a_k : z_1, \ldots, z_k \in \mathbb{Z}\}$. One also verifies that $\langle a_1, \ldots, a_k \rangle$ is a subgroup of G, and indeed, is the smallest subgroup of G that contains $a_1, \ldots, a_k$. 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 said to be **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 said to be **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.

Classification of cyclic groups. We can very easily classify all cyclic groups. 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 8.35, this map is a group homomorphism, and since a is a generator for G, it must be surjective.

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

Case 2: $\ker(\rho) \neq \{0\}$. In this case, since $\ker(\rho)$ is a subgroup of $\mathbb{Z}$ different from $\{0\}$, by Theorem 8.8, it must be of the form $n\mathbb{Z}$ for some $n > 0$. Hence, by Theorem 8.26, the map $\bar{\rho} : \mathbb{Z}_n \to G$ that sends $[z]_n$ to za is an isomorphism of $\mathbb{Z}_n$ with G.

So we see that a cyclic group is isomorphic either to the additive group $\mathbb{Z}$

or the additive group $\mathbb{Z}_n$, for some positive integer n. We have thus classified all cyclic groups "up to isomorphism." From this classification, we obtain:

Theorem 8.29. *Let G be an abelian group and let $a \in G$.*

(i) 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 any integer z, $za = 0_G$ if and only if $n \mid z$, and more generally, for integers z_1, z_2, $z_1 a = z_2 a$ if and only if $z_1 \equiv z_2 \pmod{n}$;*
- *the subgroup $\langle a \rangle$ consists of the n distinct elements*

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

(ii) If G has finite order, then $|G| \cdot a = 0_G$ and the order of a divides $|G|$.

Proof. Part (i) follows immediately from the above classification, along with part (vi) of Theorem 8.20. Part (ii) follows from part (i), along with Lagrange's theorem (Theorem 8.16), since $\langle a \rangle$ is a subgroup of G. □

***Example* 8.45.** The additive group $\mathbb{Z}$ is a cyclic group generated by 1. The only other generator is -1. More generally, the subgroup of $\mathbb{Z}$ generated by $m \in \mathbb{Z}$ is $m\mathbb{Z}$. □

***Example* 8.46.** The additive group $\mathbb{Z}_n$ is a cyclic group generated by $[1]_n$. More generally, for $m \in \mathbb{Z}$, the subgroup of $\mathbb{Z}_n$ generated by $[m]_n$ is equal to $m\mathbb{Z}_n$, which by Example 8.21 has order $n/\gcd(m, n)$. In particular, $[m]_n$ 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 $\phi(n)$. □

***Example* 8.47.** Consider the additive group $G := \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, and let $\alpha := ([1]_{n_1}, [1]_{n_2}) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$. For $m \in \mathbb{Z}$, we have $m\alpha = 0_G$ if and only if $n_1 \mid m$ and $n_2 \mid m$. This implies that α generates a subgroup of G of order $\operatorname{lcm}(n_1, n_2)$.

Suppose that $\gcd(n_1, n_2) = 1$. From the above discussion, it follows that G is cyclic of order $n_1 n_2$. One could also see this directly using the Chinese remainder theorem: as we saw in Example 8.42, the Chinese remainder theorem gives us an isomorphism of G with the cyclic group $\mathbb{Z}_{n_1 n_2}$.

Conversely, if $d := \gcd(n_1, n_2) > 1$, then all elements of $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ have order dividing $n_1 n_2/d$, and so $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ cannot be cyclic. □

***Example* 8.48.** For $a, n \in \mathbb{Z}$ with $n > 0$ and $\gcd(a, n) = 1$, the definition in this section of the multiplicative order of $\alpha := [a]_n \in \mathbb{Z}_n^*$ is consistent

with that given in §2.5, and is also the same as the multiplicative order of a modulo n. Indeed, Euler's theorem (Theorem 2.15) is just a special case of part (ii) of Theorem 8.29. Also, α is a generator for $\mathbb{Z}_n^*$ if and only if a is a primitive root modulo n. □

***Example* 8.49.** As we saw in Example 8.24, 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* 8.50.** 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* 8.51.** Based on the calculations in Example 2.6, we may conclude that $\mathbb{Z}_7^*$ is cyclic, with both $[3]$ and $[5]$ being generators. □

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

Theorem 8.30. *Let G be a cyclic group of infinite order.*

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

(ii) The subgroups of G are in one-to-one correspondence with the non-negative integers, where each such integer m corresponds to the cyclic group mG.

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

Proof. That $G \cong \mathbb{Z}$ was established in our classification of cyclic groups, it suffices to prove the other statements of the theorem for $G = \mathbb{Z}$. It is clear that for any integer m, the subgroup $m\mathbb{Z}$ is cyclic, as m is a generator. This fact, together with Theorem 8.8, establish all the other statements. □

Theorem 8.31. *Let G be a cyclic group of finite order n.*

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

(ii) The subgroups of G are in one-to-one correspondence with the positive divisors of n, 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 any two positive divisors d, d' of n, we have $dG \subseteq d'G$ if and only if $d' \mid d$.*

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

(vi) *For any 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 8.9. The fact that $d\mathbb{Z}_n$ is cyclic of order n/d can be seen in a number of ways; indeed, in Example 8.44 we constructed an isomorphism of $\mathbb{Z}_{n/d}$ with $d\mathbb{Z}_n$.

Part (iii) was established in Example 8.21.

Part (iv) was established in Theorem 8.9.

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 8.46, this group has $\phi(d)$ generators.

Part (vi) was established in Example 8.21. □

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

Theorem 8.32. *If G is an abelian group of prime order, then G is cyclic.*

Proof. Let $|G| = p$. 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 8.33. *If G_1 and G_2 are finite cyclic groups of relatively prime order, then $G_1 \times G_2$ is also cyclic.*

Proof. This follows from Example 8.47, together with our classification of cyclic groups. □

Theorem 8.34. *Any subgroup of a cyclic group is cyclic.*

Proof. This is just a restatement of part (ii) of Theorem 8.30 and part (ii) of Theorem 8.31 □

Theorem 8.35. *If $\rho : G \to G'$ is a group homomorphism, and G is cyclic, then* $\mathrm{img}(G)$ *is cyclic.*

Proof. If G is generated by a, then it is easy to see that the image of ρ is generated by $\rho(a)$. □

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

Theorem 8.36. *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. By our classification of cyclic groups, we know that the subgroup $\langle a \rangle$ is isomorphic to $\mathbb{Z}_n$, where under this isomorphism, a corresponds to $[1]_n$ and ma corresponds to $[m]_n$. The theorem then follows from the observations in Example 8.46. □

Theorem 8.37. *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 8.38. *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 m be the order of $a_1 + a_2$. It is clear that $n_1 n_2 (a_1 + a_2) = 0_G$, and hence m divides $n_1 n_2$.

We claim that $\langle a_1 \rangle \cap \langle a_2 \rangle = \{0_G\}$. To see this, suppose $a \in \langle a_1 \rangle \cap \langle a_2 \rangle$. Then since $a \in \langle a_1 \rangle$, the order of a must divide n_1. Likewise, since $a \in \langle a_2 \rangle$, the order of a must divide n_2. From the assumption that $\gcd(n_1, n_2) = 1$, it follows that the order of a must be 1, meaning that $a = 0_G$.

Since $m(a_1 + a_2) = 0_G$, it follows that $ma_1 = -ma_2$. This implies that ma_1 belongs to $\langle a_2 \rangle$, and since ma_1 trivially belongs to $\langle a_1 \rangle$, we see that ma_1 belongs to $\langle a_1 \rangle \cap \langle a_2 \rangle$. From the above claim, it follows that $ma_1 = 0_G$, and hence n_1 divides m. By a symmetric argument, we see that n_2 divides m. Again, since $\gcd(n_1, n_2) = 1$, we see that $n_1 n_2$ divides m. □

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.

We first state some basic properties.

Theorem 8.39. *Let G be an abelian group of exponent m.*

(i) For any integer k such that $kG = \{0_G\}$, we have $m \mid k$.

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

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

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

Proof. Exercise. □

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

Theorem 8.40. *If a finite abelian group G has 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, assume that $m > 1$, and 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 8.37, $(m/p_i^{e_i})a_i$ has order $p_i^{e_i}$ for each $i = 1, \ldots, r$. Finally, by Theorem 8.38, the group element

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

has order m. □

Theorem 8.41. *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 $b + H \in G/H$ 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 8.42. *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, any 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 8.23. 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 8.24. Let G be an abelian group of order mm', where $\gcd(m, m') = 1$. Consider the map $\rho : mG \times m'G$ to G that sends (a, b) to $a + b$. Show that ρ is a group isomorphism.

Exercise 8.25. 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 8.26. Show that for finite abelian groups G_1, G_2 whose exponents are m_1 and m_2, the exponent of $G_1 \times G_2$ is $\operatorname{lcm}(m_1, m_2)$.

Exercise 8.27. Give an example of an abelian group G whose exponent is zero, but where every element of G has finite order.

Exercise 8.28. Show how Theorem 2.11 easily follows from Theorem 8.31.

8.6 The structure of finite abelian groups (∗)

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

Theorem 8.43 (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 are primes (not necessarily distinct) and the e_i 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 8.44. *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.

Exercise 8.29. Show that Theorems 8.43 and 8.44 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 8.43) and sequences of integers $m_1, \ldots, m_t$ (as in Theorem 8.44), and also make use of Example 8.47.

Exercise 8.30. Using the fundamental theorem of finite abelian groups (either form), give short and simple proofs of Theorems 8.40 and 8.41.

We now prove Theorem 8.44, 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 8.45. *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, 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 8.40, 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 $A \cap B = \{0\}$. From this, Theorem 8.28 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 $A \cap B = \{0\}$, assume that B is maximal, meaning that there is no subgroup B' of G such that $B \subsetneq B'$ and $A \cap B' = \{0\}$. 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 $0 = md = (m/r)rd = (m/r)sa + (m/r)b$, and since $A \cap B = \{0\}$, we have $(m/r)sa = 0$, 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 that $d' + C$ also has order r in G/C, but also that $rd' \in B$.

We next show that $A \cap (B + \langle d' \rangle) = \{0\}$, which will yield the contradiction we seek, and thus prove the lemma. Because $A \cap B = \{0\}$, 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 $d' + C$ has order r in G/C. Further, since $rd' \in B$, we have $xd' \in B$, whence $b' + xd' \in B$. □

Lemma 8.46. *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 and n_i are positive integers (possibly 1) such that $m_i \mid m_{i+1}$ 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 m_i and n_i 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. □