Chapter 5
Direct Products and the Classification of Finite Abelian Groups

We can now determine the structure of finite abelian groups. In particular, every such group is isomorphic to a direct product of cyclic groups, each having prime power order. The proof of this result is our main goal in the present chapter.

5.1 Direct Products

We defined the direct product of two groups in Definition 3.3. There is no particular reason that we need to restrict ourselves to two.

Definition 5.1. Let $G_1, \ldots, G_k$ be any groups. Then the **(external) direct product** $G_1 \times G_2 \times \cdots \times G_k$ is the Cartesian product of the groups G_i under the operation $(a_1, \ldots, a_k)(b_1, \ldots, b_k) = (a_1b_1, \ldots, a_kb_k)$, for all $a_i, b_i \in G_i$. (We allow $k = 1$ here, in which case $G = G_1$.)

Theorem 5.1. *If $G_1, \ldots, G_k$ are groups, then $G_1 \times \cdots \times G_k$ is a group.*

Proof. The proof is essentially identical to that of Theorem 3.1. □

The reason we used the word "external" in the above definition is that the groups G_i are not subgroups of the direct product; indeed, they are not even subsets. However, G_1 is, for instance, isomorphic in a natural way to $G_1 \times \{e\} \times \cdots \times \{e\}$, which is a subgroup of the direct product. What we would like is a way of showing that a group is isomorphic to the direct product of certain subgroups. To this end, let us consider the following.

Definition 5.2. Let G be a group, and let $N_1, \ldots, N_k$ be subgroups of G. Then we say that G is the **internal direct product** of $N_1, \ldots, N_k$ if

© Springer International Publishing AG, part of Springer Nature 2018

G. T. Lee, *Abstract Algebra*, Springer Undergraduate Mathematics Series,
https://doi.org/10.1007/978-3-319-77649-1_5

1. each N_i is normal;
2. $N_1 N_2 \cdots N_k = G$; and
3. for each i, $1 \le i < k$, we have $(N_1 N_2 \cdots N_i) \cap N_{i+1} = \{e\}$.

(Again, we allow $k = 1$, in which case $G = N_1$.)

In particular, G is the internal direct product of normal subgroups N_1 and N_2 if and only if $N_1 N_2 = G$ and $N_1 \cap N_2 = \{e\}$.

Example 5.1. Let $G = \mathbb{Z}_{20}$, $N_1 = \langle 4 \rangle$ and $N_2 = \langle 5 \rangle$. As G is abelian, every subgroup is normal. Also, $N_1 = \{0, 4, 8, 12, 16\}$ and $N_2 = \{0, 5, 10, 15\}$. Thus, $N_1 \cap N_2 = \{0\}$. For each $a \in G$, we could find $n_1 \in N_1$ and $n_2 \in N_2$ such that $a = n_1 + n_2$ but, in fact, we can avoid this by noting that $|N_1 + N_2| = |N_1||N_2|/|N_1 \cap N_2| = 5 \cdot 4/1 = 20$ (see Theorem 4.4). Thus, $N_1 + N_2 = G$, and G is the internal direct product of N_1 and N_2.

Note that if there are more than two groups, then we need to check more than just that each $N_i \cap N_j = \{e\}$ for the final part of the definition.

Example 5.2. Let $G = \mathbb{Z}_{30}$, $N_1 = \langle 15 \rangle$, $N_2 = \langle 10 \rangle$ and $N_3 = \langle 6 \rangle$. Again, normality is not an issue. It is easy to see that $N_1 \cap N_2 = \{0\}$. Thus, $|N_1 + N_2| = |N_1||N_2| = 2 \cdot 3 = 6$. As every element of $N_1 + N_2$ is in $\langle 5 \rangle$, we see immediately that $N_1 + N_2 = \langle 5 \rangle$. But now we observe that $(N_1 + N_2) \cap N_3 = \{0\}$. Then the same argument shows that $|N_1 + N_2 + N_3| = 30$, and we know that $N_1 + N_2 + N_3 = G$. Therefore, G is the internal direct product of N_1, N_2 and N_3.

Let us see how internal direct products behave. Here are some highly useful facts.

Lemma 5.1. *Let G be a group with normal subgroups K and N. If $K \cap N = \{e\}$, then $kn = nk$ for all $k \in K$, $n \in N$.*

Proof. Let $h = (nk)^{-1}(kn) = k^{-1}n^{-1}kn$. As K is normal, $n^{-1}kn \in K$, so $h \in K$. As N is normal, $k^{-1}n^{-1}k \in N$, so $h \in N$. Since $K \cap N = \{e\}$, we have $(nk)^{-1}(kn) = e$, and therefore $kn = nk$, as required. □

Lemma 5.2. *If G is the internal direct product of $N_1, \ldots, N_k$, then every element of G can be written in exactly one way as $n_1 n_2 \cdots n_k$, with each $n_i \in N_i$.*

Proof. Since $G = N_1 \cdots N_k$, we know that every element of G can be written in such a way. We only need to show uniqueness. Our proof is by induction on k. If $k = 1$, there is nothing to do, as $G = N_1$. Assume that $k > 1$ and the result holds for groups written as an internal direct product of a smaller number of subgroups. Suppose that $n_1 \cdots n_{k-1} n_k = h_1 \cdots h_{k-1} h_k$, with $n_i, h_i \in N_i$. Then

$$h_k n_k^{-1} = (h_1 \cdots h_{k-1})^{-1}(n_1 \cdots n_{k-1}) \in N_k \cap (N_1 \cdots N_{k-1}) = \{e\}.$$

Therefore, $n_k = h_k$, and we have $n_1 \cdots n_{k-1} = h_1 \cdots h_{k-1}$ in $N_1 N_2 \cdots N_{k-1}$, which is an internal direct product of $k-1$ subgroups. By our inductive hypothesis, $n_i = h_i$ for all i. □

Example 5.3. As we saw in Example 5.2, $\mathbb{Z}_{30}$ is the internal direct product of $\langle 15\rangle$, $\langle 10\rangle$ and $\langle 6\rangle$. Note, for instance, that $23 = 15 + 20 + 18$. By the above lemma, there is no other way to write 23 as a sum of elements in $\langle 15\rangle$, $\langle 10\rangle$ and $\langle 6\rangle$.

And now, the big reason why we are interested in these internal direct products.

Theorem 5.2. *Let G be a group, and suppose that it is the internal direct product of normal subgroups $N_1, \ldots, N_k$. Then G is isomorphic to the external direct product $N_1 \times \cdots \times N_k$.*

Proof. Define $\alpha : N_1 \times \cdots \times N_k \to G$ via $\alpha((n_1, \ldots, n_k)) = n_1 \cdots n_k$. We claim that α is an isomorphism. In view of Lemma 5.2, α is bijective. Thus, it remains to show that it is a homomorphism. Take $n_i, h_i \in N_i$. Then

$$\alpha((n_1, \ldots, n_k)(h_1, \ldots, h_k)) = \alpha((n_1h_1, \ldots, n_kh_k)) = n_1h_1n_2h_2n_3h_3 \cdots n_kh_k.$$

As N_1 and N_2 are normal subgroups, and $N_1 \cap N_2 = \{e\}$, Lemma 5.1 says that $h_1n_2 = n_2h_1$. Thus,

$$n_1h_1n_2h_2n_3h_3 \cdots n_kh_k = n_1n_2h_1h_2n_3h_3 \cdots n_kh_k.$$

By Theorem 4.5, N_1N_2 is a normal subgroup of G, and we know that $(N_1N_2) \cap N_3 = \{e\}$. Therefore, $h_1h_2n_3 = n_3h_1h_2$. We now have

$$n_1h_1n_2h_2n_3h_3 \cdots n_kh_k = n_1n_2n_3h_1h_2h_3n_4h_4 \cdots n_kh_k.$$

Repeating this procedure, we find that

$$\alpha((n_1, \ldots, n_k)(h_1, \ldots, h_k)) = n_1n_2 \cdots n_kh_1h_2 \cdots h_k = \alpha((n_1, \ldots, n_k))\alpha((h_1, \ldots, h_k)).$$

Thus, α is a homomorphism, and the proof is complete. □

As a result of this theorem, we will engage in a small abuse of notation and write $G = N_1 \times N_2 \times \cdots \times N_k$ when G is the internal direct product of $N_1, \ldots, N_k$, as well as for the external direct product.

Example 5.4. By Example 5.2, $\mathbb{Z}_{30} = \langle 15\rangle \times \langle 10\rangle \times \langle 6\rangle$.

Example 5.5. We claim that $U(8) = \langle 3\rangle \times \langle 7\rangle$. As the group is abelian, normality is not an issue. Also, $|3| = |7| = 2$, so the intersection of these cyclic subgroups must be trivial. Furthermore, $1 = 1 \cdot 1$, $3 = 3 \cdot 1$, $7 = 1 \cdot 7$ and $5 = 3 \cdot 7$, so $U(8) = \langle 3\rangle\langle 5\rangle$ (or just use an order argument). Thus, we have an internal direct product.

Exercises

5.1. Write $U(32)$ as the internal direct product of two proper subgroups.

5.2. Let $G = H \times K$. If $h \in H$ has order m and $k \in K$ has order n, what is the order of (h, k)?

5.3. How many elements of order 5 are there in $\mathbb{Z}_5 \times \mathbb{Z}_{25}$? How many elements of order 25?

5.4. How many cyclic subgroups of order 5 are there in $\mathbb{Z}_5 \times \mathbb{Z}_{25}$? How many cyclic subgroups of order 25?

5.5. Show that D_8 is not the internal direct product of two proper subgroups.

5.6. Let $|a| = 4$ and $|b| = 2$. Write $\langle a \rangle \times \langle b \rangle$ as the internal direct product of two proper subgroups in every possible way.

5.7. Show that in Definition 5.2, it is not sufficient to replace the third condition with the stipulation that $N_i \cap N_j = \{e\}$ whenever $i \neq j$. In particular, find a group G with normal subgroups N_1, N_2 and N_3 such that $N_1 N_2 N_3 = G$ and $N_i \cap N_j = \{e\}$ whenever $i \neq j$, but $G \neq N_1 \times N_2 \times N_3$.

5.8. Let $G = \langle a \rangle$ be cyclic of order 84. Show that $G = \langle a^{12} \rangle \times \langle a^{21} \rangle \times \langle a^{28} \rangle$.

5.9. Suppose that $G = N_1 \times N_2$ is an internal direct product. If $\alpha : G \to H$ is an onto homomorphism, does it follow that $H = \alpha(N_1) \times \alpha(N_2)$? Prove that it does, or give an explicit counterexample.

5.10. Let G be a group having finite normal subgroups $N_1, \ldots, N_k$, such that the gcd of $|N_i|$ and $|N_j|$ is 1 whenever $i \neq j$. Show that $N_1 N_2 \cdots N_k = N_1 \times N_2 \times \cdots \times N_k$.

5.2 The Fundamental Theorem of Finite Abelian Groups

Let us now classify the finite abelian groups. We will break our proof down into stages. For the first stage, we need a definition.

Definition 5.3. Let p be a prime number. Furthermore, let G be a group and $a \in G$. We say that a is a ***p*-element** if the order of a is p^n for some integer $n \geq 0$. If every element of G is a p-element, then G is a ***p*-group**.

Example 5.6. The dihedral group D_8 is a 2-group, as every element has order 1, 2 or 4. On the other hand, $\mathbb{Z}_{24}$ is not a p-group. Indeed, 12 and 18 are both 2-elements and 8 is a 3-element, so it cannot be a p-group. In fact, 1 is not a p-element, for any prime p.

Lemma 5.3. *Let p be a prime and G an abelian group. Then the p-elements of G form a subgroup.*

Proof. Let H be the set of all p-elements of G. As e has order p^0, we have $e \in H$. Let $a, b \in H$. Then say that $|a| = p^n$ and $|b| = p^m$. Let k be the larger of m and n. Then as G is abelian, $(ab)^{p^k} = a^{p^k} b^{p^k} = e^2 = e$, as $|a|$ and $|b|$ both divide p^k. Thus, $|ab|$ divides p^k, and therefore $ab \in H$. Finally, if $a \in H$, then $|a| = |a^{-1}|$, so $a^{-1} \in H$. Thus, H is indeed a subgroup of G. □

Note that the preceding lemma does not work for nonabelian groups. Indeed, in S_3, we can see that $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ both have order 2, but their product, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, has order 3.

The following result is also very handy.

Lemma 5.4. *Let G be any group and let $e \neq a \in G$ be such that a has finite order. Then $a = a^{n_1} a^{n_2} \cdots a^{n_k}$ for some integers $n_1, \ldots, n_k$, where each a^{n_i} is a p_i-element, for some prime p_i dividing $|a|$.*

Proof. Our proof is by induction on the number of distinct primes, l, dividing $|a|$. If $l = 1$, then a is a p-element, so just let $n_1 = 1$. Suppose that $l > 1$ and that the result is true for smaller values of l. Let p be a prime dividing $|a|$, and say that $|a| = p^m q$, with $(p, q) = 1$. By Corollary 2.1, there exist $u, v \in \mathbb{Z}$ such that $p^m u + qv = 1$. Then

$$a = a^1 = a^{p^m u + qv} = (a^{p^m})^u (a^q)^v.$$

Now, $(a^q)^{p^m} = a^{p^m q} = e$; hence, a^q is a p-element and so is $(a^q)^v$. So, let $p_1 = p$ and $n_1 = qv$. Similarly, the order of $(a^{p^m})^u$ divides q, and q has fewer primes dividing it than $|a|$. Thus, by our inductive hypothesis, a^{up^m} can be written as a product of powers (which are also powers of a) in the manner stated in the theorem. The proof is complete. □

We can now simplify our task by breaking a finite abelian group down into a direct product of p-groups.

Lemma 5.5. *Let G be a nontrivial finite abelian group, and let $p_1, \ldots, p_k$ be the distinct primes dividing $|G|$. Then $G = H_1 \times H_2 \times \cdots \times H_k$, where H_i is the subgroup of G consisting of all of the p_i-elements of G.*

Proof. Lemma 5.3 tells us that the H_i are subgroups and, as G is abelian, we do not have to worry about normality. Let us show that $G = H_1 H_2 \cdots H_k$. But taking any $a \in G$, we see from Lemma 5.4 that a can be written as a product of elements from various H_i. (If $a = e$, there is obviously nothing to worry about.) Finally, we must show that for each i, $1 \leq i < k$, we have $(H_1 \cdots H_i) \cap H_{i+1} = \{e\}$. But suppose that $a \in H_{i+1}$ and, simultaneously, $a = a_1 \cdots a_i$, with $a_j \in H_j$. Then letting $|a_j| = p_j^{m_j}$, and $m = p_1^{m_1} \cdots p_i^{m_i}$, we have $a^m = a_1^m \cdots a_i^m$, and since each $|a_j|$ divides m, we conclude that $a^m = e$. Thus, $|a|$ divides m. But also, a is a p_{i+1}-element. As $(m, p_{i+1}) = 1$, the only possible conclusion is that $a = e$, and we have an internal direct product. □

We can now focus our attention on finite abelian p-groups. The following lemma does the biggest part of the work. It is the most difficult proof we have encountered so far, and will take some time to absorb.

Lemma 5.6. *Let G be a finite abelian p-group, and let $a \in G$ be an element of largest possible order. Then $G = \langle a \rangle \times H$, for some subgroup H of G.*

Proof. Our proof is by strong induction on $|G|$. If $|G| = 1$, then $a = e$ and using $H = \langle e \rangle$ will work. So, assume that $|G| > 1$ and that the lemma holds for groups of smaller order.

Let $|a| = p^n$, with n a positive integer. If $\langle a \rangle = G$, then we can use $H = \langle e \rangle$, so assume that $\langle a \rangle \neq G$. Take $b \in G$ such that $b \notin \langle a \rangle$. As b is a p-element, we know that $b^{p^k} = e \in \langle a \rangle$, for some positive integer k. Let m be the smallest positive integer such that $b^{p^m} \in \langle a \rangle$, and let $c = b^{p^{m-1}}$. Then $c \notin \langle a \rangle$, but $c^p = b^{p^m} \in \langle a \rangle$. In particular, let us say that $c^p = a^i$, with $i \in \mathbb{Z}$.

Now, as G is a p-group, and the largest element order is p^n, we must have $c^{p^n} = e$. Thus, $|c^p|$ divides p^{n-1}. Suppose that $(p, i) = 1$. Then by Corollary 3.2, $|c^p| = |a^i| = p^n$, which is impossible. Thus, p divides i; let us say that $i = pj$. Then let $d = a^{-j}c$. Note that $a^j \in \langle a \rangle$; thus, if $d \in \langle a \rangle$, then $c = a^j d \in \langle a \rangle$, which is a contradiction. Therefore, $d \notin \langle a \rangle$. However, $d^p = a^{-jp}c^p = (a^i)^{-1}c^p = e$; thus, $|d| = p$.

Now, let us consider the group $M = G/\langle d \rangle$. (As G is abelian, we do not have to worry about $\langle d \rangle$ being normal.) We note that M is still abelian (by Theorem 4.7), its order is $[G : \langle d \rangle] = |G|/p$ and it is a p-group with the orders of elements dividing orders of elements of G (by Theorem 4.7). Also, we claim that $|a\langle d \rangle| = p^n$. As its order must divide p^n, suppose that $a^{p^{n-1}} \in \langle d \rangle$. Since $a^{p^{n-1}} \neq e$, we must have $a^{p^{n-1}} = d^s$, with $0 < s < p$. But then $(s, p) = 1$, so by Corollary 2.1, there exist $u, v \in \mathbb{Z}$ such that $su + pv = 1$. Thus, $d = d^{su+pv} = (d^s)^u (d^p)^v = a^{p^{n-1}u} e \in \langle a \rangle$, giving us a contradiction. Therefore, $|a\langle d \rangle| = p^n$, as claimed.

It now follows that $a\langle d \rangle$ is an element of largest order in M. As M is an abelian p-group of smaller order than G, our inductive hypothesis tells us that there is a subgroup K of M such that $M = N \times K$, where N is the subgroup of M generated by $a\langle d \rangle$. By Theorem 4.8, $K = H/\langle d \rangle$, where H is a subgroup of G containing $\langle d \rangle$.

We claim that $G = \langle a \rangle \times H$. Normality is not an issue. Suppose that $a^i \in \langle a \rangle \cap H$. Then $a^i \langle d \rangle \in N \cap K$, and as the product $N \times K$ is direct, this means that $a^i \langle d \rangle = e\langle d \rangle$. But we demonstrated above that the order of $a\langle d \rangle$ is p^n, which means that p^n divides i, and therefore $a^i = e$. Thus, $\langle a \rangle \cap H = \{e\}$.

Now, take any $g \in G$. Then as $M = N \times K$, we have $g\langle d \rangle = xy$, for some $x \in N$, $y \in K$. Let us write $x = a^t \langle d \rangle$ and $y = w\langle d \rangle$, with $t \in \mathbb{Z}$ and $w \in H$. Then $g = a^t w d^l$, for some $l \in \mathbb{Z}$. As $a^t \in \langle a \rangle$ and $wd^l \in H$, we now see that $\langle a \rangle H = G$. Thus, we have the required direct product, and our proof is complete. □

And now, the payoff for our hard work!

Theorem 5.3 (Fundamental Theorem of Finite Abelian Groups). *Let G be a finite abelian group. Then G is the direct product of subgroups, $H_1 \times \cdots \times H_k$, with* *each H_i cyclic of order $p_i^{n_i}$, where the p_i are (not necessarily distinct) primes, and the n_i are nonnegative integers.*

Proof. If G is the trivial group, there is nothing to do. Otherwise, by Lemma 5.5, G is the direct product of p-subgroups. Therefore, we may as well assume that G is a finite abelian p-group. Our proof is by strong induction on $|G|$. If $|G| = 1$, again, there is nothing to do, so let G be nontrivial and suppose that our theorem holds for groups of smaller order. Let a be an element of largest possible order in G. Then by Lemma 5.6, $G = \langle a \rangle \times H$, for some subgroup H. But then $|H| = |G|/|a|$, so H has smaller order, and by our inductive hypothesis, H is a direct product of cyclic groups of prime power order. However, $\langle a \rangle$ is also a cyclic group of prime power order, and we are done. □

We can express this slightly differently.

Corollary 5.1. *Let G be a nontrivial finite abelian group. Then G is isomorphic to $\mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}$, where the p_i are some (not necessarily distinct) primes, and the n_i are positive integers.*

Proof. Combine Theorems 5.2 and 5.3 with Theorem 4.14. □

Example 5.7. Up to isomorphism, the abelian groups of order 16 are $\mathbb{Z}_{16}$, $\mathbb{Z}_8 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_4$, $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Example 5.8. Note that $U(32)$ is an abelian group of order $\varphi(32) = 16$, so it must be isomorphic to one of the groups in the preceding example. But which one? Examining the orders of the elements, we find that there is no element of order 16, so it is not $\mathbb{Z}_{16}$. However, $|3| = 8$. As none of the other groups in the preceding example have an element of order 8, $U(32)$ is isomorphic to $\mathbb{Z}_8 \times \mathbb{Z}_2$.

Example 5.9. As $200 = 2^3 5^2$, the finite abelian groups of order 200 are all isomorphic to one of the following, namely $\mathbb{Z}_8 \times \mathbb{Z}_{25}$, $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$, $\mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_5$, $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$.

We might be momentarily concerned about the absence of $\mathbb{Z}_{200}$ in the preceding example. However, it is isomorphic to $\mathbb{Z}_8 \times \mathbb{Z}_{25}$, as the following theorem shows us.

Theorem 5.4. *Let $G = H_1 \times \cdots \times H_k$, where each H_i is cyclic of order n_i. Then G is cyclic if and only if $(n_i, n_j) = 1$ whenever $i \neq j$.*

Proof. Let $H_i = \langle a_i \rangle$. If the n_i are all relatively prime, then we claim that $(a_1, \ldots, a_k)$ has order $n_1 \cdots n_k = |G|$, and therefore G is cyclic. Suppose that $(a_1, \ldots, a_k)^m = (e, \ldots, e)$. Then each $a_i^m = e$, so $n_i | m$. As the n_i are relatively prime, $n_1 \cdots n_k | m$, by Corollary 2.3. Since $|G| = n_1 \cdots n_k$, the largest possible order of an element is $n_1 \cdots n_k$, and the claim is proved.

On the other hand, suppose that the n_i are not relatively prime. Without loss of generality, say that some prime p divides both n_1 and n_2. Then for any $r_i \in \mathbb{Z}$, we have $(a_1^{r_1}, \ldots, a_k^{r_k})^{n_1 \cdots n_k / p} = (e, \ldots, e)$, since each n_i divides $n_1 \cdots n_k / p$. (For $i = 1$, we have $n_1(n_2/p)n_3 \cdots n_k$, and for $i \geq 2$, we have $(n_1/p)n_2n_3 \cdots n_k$.) Thus, every element of G has order dividing $n_1n_2 \cdots n_k/p$, and therefore there is no element of order $|G|$, so G is not cyclic. □

As a result of our classification, we can prove a special case of a famous result due to Augustin-Louis Cauchy.

Theorem 5.5 (Cauchy's Theorem for Abelian Groups). *Let G be a finite abelian group, and suppose that p is a prime dividing $|G|$. Then G has an element of order p.*

Proof. If $|G|$ is divisible by a prime, then G is not the trivial group. Letting G be as in Corollary 5.1, we see that $|G| = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$. If p divides $|G|$, then $p = p_i$, for some i. But then G has a subgroup isomorphic to $\mathbb{Z}_{p^{n_i}}$, for some $n_i > 0$. However, in $\mathbb{Z}_{p^{n_i}}$, the element p^{n_i-1} has order p. The proof is complete. □

Corollary 5.2. *A finite abelian p-group has order p^n, for some $n \geq 0$.*

Proof. Let G be a finite abelian p-group. If the corollary is false, then the order of G is divisible by q, for some prime $q \neq p$. But then G has an element of order q, which is impossible. □

Exercises

5.11. Give a list of abelian groups of each of the following orders, such that every abelian group of that order is isomorphic to one of the groups in the list.

1. 21
2. 81
3. 9800

5.12. Give a list of abelian groups of each of the following orders, such that every abelian group of that order is isomorphic to one of the groups in the list.

1. 144
2. 243
3. 55125

5.13. Write $U(56)$ as an external direct product of cyclic groups of prime power order, as in Corollary 5.1.

5.14. Write $(\mathbb{Z}_{20} \times \mathbb{Z}_6)/\langle(10, 2)\rangle$ as an external direct product of cyclic groups of prime power order, as in Corollary 5.1.

5.15. Let p be a prime. Suppose that G is a nontrivial finite abelian group in which every element has order 1 or p. Show that G is isomorphic to a group of the form $\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$.

5.16. Suppose that n is an integer that is a product of distinct primes. If G is a finite abelian group, and $|G|$ is divisible by n, show that G has a cyclic subgroup of order n.

5.17. If $\langle a \rangle$ is a cyclic group of order 35, write a as the product of a 5-element and a 7-element.

5.18. If $\langle a \rangle$ is a cyclic group of order 90, write a as the product of p-elements, for various primes p.

5.19. Prove Theorem 5.5 in a different way, as follows. Let p be a prime dividing $|G|$. Show that G has an element a of some prime order, say q. If $q = p$, we are done. Otherwise, what can be said about $G/\langle a \rangle$? Complete the proof.

5.20. Let G be a finite abelian group and let n be a positive integer dividing $|G|$. Show that G has a subgroup of order n.

5.3 Elementary Divisors and Invariant Factors

For any positive integer n, we now know all possible abelian groups of order n, up to isomorphism. Indeed, we determine the prime factorization of n, and then proceed as in Examples 5.7 and 5.9. But we have not yet made certain that the groups we found are not isomorphic to each other. Let us work on that.

Definition 5.4. Let G be a nontrivial finite abelian group, and say that $G = H_1 \times H_2 \times \cdots \times H_k$, where each H_i is cyclic of order $p_i^{n_i}$, for some prime p_i and positive integer n_i. Then the **elementary divisors** of G are the numbers $p_1^{n_1}, p_2^{n_2}, \ldots, p_k^{n_k}$, where the order in this list is irrelevant, but each number must be listed as many times as it occurs. The trivial group has no elementary divisors.

Example 5.10. The elementary divisors of $\mathbb{Z}_9 \times \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_{125}$ are 9, 9, 3, 125.

Example 5.11. To find the elementary divisors of $\mathbb{Z}_{300} \times \mathbb{Z}_3$, we use Theorem 5.4 to see that the group is isomorphic to $\mathbb{Z}_{25} \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3$, so the elementary divisors are 4, 3, 3, 25.

Definition 5.5. Let G be an abelian group and n a positive integer. Then we write $G^n = \{a^n : a \in G\}$.

Lemma 5.7. *Let G and H be abelian groups and n a positive integer. Then*

1. *G^n is a subgroup of G; and.*
2. *if $\alpha : G \to H$ is an onto homomorphism, then $\alpha(G^n) = H^n$.*

Proof. (1) See Exercise 3.40.

(2) If $g^n \in G^n$, then $\alpha(g^n) = (\alpha(g))^n \in H^n$. Also, if $h^n \in H^n$, then as α is onto, write $h = \alpha(g)$, with $g \in G$. Then $h^n = (\alpha(g))^n = \alpha(g^n) \in \alpha(G^n)$, completing the proof. □

The elementary divisors are very important, as they uniquely determine a finite abelian group, up to isomorphism.

Theorem 5.6. *Let G and H be finite abelian groups. Then G and H are isomorphic if and only if they have the same elementary divisors.*

Proof. If G and H have the same elementary divisors, then each is isomorphic to a direct product of cyclic groups, and the groups appearing in the direct product in G have the same order as those appearing in H, so they are isomorphic. (We must be a bit careful, as the cyclic groups may appear in a different order in the direct product, but $M \times N$ is always isomorphic to $N \times M$, so this is not a problem. See Exercise 4.36.) Note that if neither G nor H has any elementary divisors, then each is the trivial group, so they are isomorphic.

On the other hand, let $\alpha : G \to H$ be an isomorphism. Take any prime p. Now, by Lemma 5.3, the p-elements of G form a subgroup, as do those of H. Furthermore, as isomorphisms preserve the orders of group elements, α provides an isomorphism from one of these p-subgroups to the other. As the elementary divisors come from these p-subgroups, we may as well assume to begin with that G and H are both p-groups. We proceed by strong induction on $|G|$. If $|G| = 1$, then G and H are both the trivial group, so neither has elementary divisors. Therefore, assume that $|G| > 1$ and the result holds for groups of smaller order.

In particular, say $G = G_1 \times \cdots \times G_k$ and $H = H_1 \times \cdots \times H_l$, where $G_i = \langle g_i \rangle$ is cyclic of order p^{n_i}, and $H_i = \langle h_i \rangle$ is cyclic of order p^{m_i}. Rearranging the terms if necessary, we may assume that $n_1 \geq n_2 \geq \cdots \geq n_k > 0$ and $m_1 \geq m_2 \geq \cdots \geq m_l > 0$. By the above lemma, $\alpha(G^p) = H^p$. Thus, $\alpha(G_1^p \times \cdots \times G_k^p) = H_1^p \times \cdots \times H_l^p$. But $G_i^p = \langle g_i^p \rangle$, and since $|g_i| = p^{n_i}$, we have $|g_i^p| = p^{n_i - 1}$, by Corollary 3.2. Similarly, $|h_i^p| = p^{m_i - 1}$. Thus, G^p is a p-group of strictly smaller order than G, and by our inductive hypothesis, the elementary divisors of G^p and H^p are the same. But the elementary divisors of G^p are $p^{n_1-1}, p^{n_2-1}, \ldots, p^{n_r-1}$, where $n_r > 1$ but $n_u = 1$ whenever $u > r$. (When $n_u = 1$, we have $p^{n_u-1} = 1$, which does not count as an elementary divisor. If $n_1 = 1$, then G^p has no elementary divisors.) Similarly, the elementary divisors of H^p are $p^{m_1-1}, \ldots, p^{m_s-1}$, where $m_s > 1$ but $m_v = 1$ whenever $v > s$. Therefore, $r = s$ and $m_i - 1 = n_i - 1$ whenever $i \leq r$. But then $m_i = n_i$, for all $i \leq r$. Also, $n_i = 1$ for all $i > r$ and $m_i = 1$ for all $i > s$. In order to prove that G and H have the same elementary divisors, it remains only to show that $k = l$. But $|G| = p^{n_1} \cdots p^{n_r} p^{k-r}$ and $|H| = p^{n_1} \cdots p^{n_r} p^{l-r}$. As isomorphic groups have the same order, $p^{k-r} = p^{l-r}$, and therefore $k = l$. If G^p has no elementary divisors, then neither does H^p, and we simply get $p^k = p^l$, hence $k = l$. □

Example 5.12. The five abelian groups of order 16 listed in Example 5.7 are all non-isomorphic, as they have different elementary divisors. Similarly for the six abelian groups of order 200 given in Example 5.9.

Example 5.13. Let $G = \mathbb{Z}_{200} \times \mathbb{Z}_8 \times \mathbb{Z}_6$, $H = \mathbb{Z}_{120} \times \mathbb{Z}_{10} \times \mathbb{Z}_4 \times \mathbb{Z}_2$ and $K = \mathbb{Z}_{25} \times \mathbb{Z}_{24} \times \mathbb{Z}_8 \times \mathbb{Z}_2$. These are all abelian groups of order 9600. However, using Theorem 5.4, we see that G is isomorphic to $\mathbb{Z}_8 \times \mathbb{Z}_{25} \times \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_2$, so its elementary divisors are 8, 8, 2, 3, 25. Similarly, H is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_2$, so its elementary divisors are 8, 4, 2, 2, 3, 5, 5 and K is isomorphic to $\mathbb{Z}_{25} \times \mathbb{Z}_3 \times \mathbb{Z}_8 \times \mathbb{Z}_8 \times \mathbb{Z}_2$, so its elementary divisors are 8, 8, 2, 3, 25. Therefore, G and K are isomorphic, but H is not isomorphic to either of them.

There is another interesting way to express a finite abelian group as a direct product of cyclic groups.

Theorem 5.7 (Invariant Factor Decomposition). *Suppose that G is a nontrivial finite abelian group. Then $G = H_1 \times H_2 \times \cdots \times H_k$, where each H_i is a cyclic subgroup of G of order m_i, with $m_1 > 1$ and $m_i | m_{i+1}$, for $1 \leq i < k$.*

Proof. We will explain how to construct the H_i, assuming that G has been expressed as a direct product of cyclic groups of prime power order, as in Corollary 5.1. Let $p_1, \ldots, p_r$ be the primes dividing $|G|$. For each j, find the largest power $p_j^{n_j}$ such that $\mathbb{Z}_{p_j^{n_j}}$ appears in Corollary 5.1. Letting $m_k = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$, Theorem 5.4 says that $H_k = \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_r^{n_r}}$ is isomorphic to $\mathbb{Z}_{m_k}$. Now, delete all of the terms from the direct product in Corollary 5.1 that we have used (deleting only one copy, if multiple copies of the same group appear). For each j, let $p_j^{s_j}$ be the largest power appearing in the remaining terms (where $s_j = 0$ is entirely possible). Let $m_{k-1} = p_1^{s_1} \cdots p_r^{s_r}$. By construction, each $s_j \leq n_j$, so $m_{k-1} | m_k$. Again, $H_{k-1} = \mathbb{Z}_{p_1^{s_1}} \times \cdots \times \mathbb{Z}_{p_r^{s_r}}$ is isomorphic to $\mathbb{Z}_{m_{k-1}}$. Delete all of these terms that we have just used, and repeat until we exhaust the entire direct product in Corollary 5.1. □

Definition 5.6. If G is isomorphic to $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$, where $m_1 > 1$ and $m_i | m_{i+1}$, for $1 \leq i < k$, then the numbers $m_1, \ldots, m_k$ are called the **invariant factors** of G.

Example 5.14. Let us use our work in Example 5.9 to find the invariant factors of the abelian groups of order 200. We apply the method from Theorem 5.7. Considering $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$, we see that the highest power of 2 that appears is 4, and the highest power of 5 is 25. Therefore, $m_k = 4 \cdot 25 = 100$. Deleting $\mathbb{Z}_4$ and $\mathbb{Z}_{25}$, we are left with $\mathbb{Z}_2$, so $m_{k-1} = 2$, and we are finished. Thus, our group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{100}$, so the invariant factors are 2, 100. When we examine $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$, we see that $m_k = 2 \cdot 5 = 10$. Deleting $\mathbb{Z}_2$ and $\mathbb{Z}_5$, we are left with $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$. Thus, $m_{k-1} = 2 \cdot 5 = 10$. Deleting $\mathbb{Z}_2$ and $\mathbb{Z}_5$, we are left only with $\mathbb{Z}_2$. Thus, $m_{k-2} = 2$, and we are finished. Therefore, our group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{10} \times \mathbb{Z}_{10}$, which gives invariant factors of 2, 10, 10. Considering $\mathbb{Z}_8 \times \mathbb{Z}_{25}$, we simply get $\mathbb{Z}_{200}$, so 200 is the only invariant factor. Looking at $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$, we have $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{50}$, so the invariant factors are 2, 2, 50. When we examine $\mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_5$, we obtain $\mathbb{Z}_5 \times \mathbb{Z}_{40}$, so the invariant factors are 5, 40. Finally, if we take $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$, then we get $\mathbb{Z}_{10} \times \mathbb{Z}_{20}$, so the invariant factors are 10, 20.

In the above example, the nonisomorphic groups produced different lists of invariant factors. As it turns out, this always happens.

Theorem 5.8. *Let G and H be nontrivial finite abelian groups. Then G and H are isomorphic if and only if they have the same invariant factors.*

Proof. Let G be isomorphic to $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$ with $m_1 > 1$ and $m_i | m_{i+1}$, $1 \le i < k$. Similarly, write H as $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_l}$, with $n_1 > 1$ and $n_i | n_{i+1}$, $1 \le i < l$. If G and H have the same invariant factors, then they are both isomorphic to the same direct product, and therefore to each other.

On the other hand, suppose that G and H are isomorphic. We will show that they have the same invariant factors. Our proof is by strong induction on $|G|$. If $|G| = 2$, then the only possible invariant factor list is 2 for both G and H, so there is nothing to do. Assume that $|G| > 2$ and that the result is true for groups of smaller order. If we take $(g_1, \ldots, g_k) \in G$, then each g_i has order dividing m_i, and therefore all g_i have order dividing m_k. On the other hand $(0, 0, \ldots, 0, 1)$ has order m_k. Thus, m_k is the largest possible order of an element of G. Similarly, n_l is the largest possible order of any element of H. Therefore, as isomorphisms preserve orders of group elements, $m_k = n_l$. Now, expressing each m_i as a product of prime powers, we note that the elementary divisors of G are those that come from $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_{k-1}}$ together with those from $\mathbb{Z}_{m_k}$. Similarly, the elementary divisors of H are those coming from $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_{l-1}}$ together with those from $\mathbb{Z}_{n_l} = \mathbb{Z}_{m_k}$. As G and H are isomorphic, Theorem 5.6 tells us that they have the same elementary divisors. Deleting those from $\mathbb{Z}_{m_k}$, the groups $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_{k-1}}$ and $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_{l-1}}$ have the same elementary divisors. Thus, by Theorem 5.6, these groups are isomorphic. As they have smaller order than G, our inductive hypothesis tells us that $k - 1 = l - 1$ and each $m_i = n_i$. Therefore, the invariant factors are identical.

(We have to be a bit careful if either $k = 1$ or $l = 1$, as then we have nothing left when we remove the term $\mathbb{Z}_{m_k}$ or $\mathbb{Z}_{n_l}$. But in this case, comparing orders, we must have $k = l = 1$, and the only invariant factor is m_1 for both groups.) □

Exercises

5.21. Find the elementary divisors for each of the following groups.

1. $\mathbb{Z}_{42} \times \mathbb{Z}_{4200}$
2. $\mathbb{Z}_6 \times \mathbb{Z}_{18} \times \mathbb{Z}_{54}$

5.22. Find the invariant factors for each of the following groups.

1. $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_{25} \times \mathbb{Z}_{11} \times \mathbb{Z}_{121}$
2. $\mathbb{Z}_4 \times \mathbb{Z}_8 \times \mathbb{Z}_8 \times \mathbb{Z}_{16} \times \mathbb{Z}_5 \times \mathbb{Z}_{25} \times \mathbb{Z}_{49}$

5.23. Let p, q and r be distinct primes. Give the list of elementary divisors for every possible abelian group of order p^3q^2r.

5.24. Let p, q and r be distinct primes. Give the list of invariant factors for every possible abelian group of order p^3q^2r.

5.25. For which positive integers n are all abelian groups of order n isomorphic?

5.26. Find the smallest positive integer n such that there are exactly four nonisomorphic abelian groups of order n.

5.27. Let G_1, G_2 and G_3 be finite abelian groups, and suppose that $G_1 \times G_2$ is isomorphic to $G_1 \times G_3$. Show that G_2 and G_3 are isomorphic.

5.28. Let a finite abelian group G have invariant factors $n_1, n_2, \ldots, n_k$. What are the invariant factors of $G \times G$?

5.29. Let G be a nontrivial finite abelian 2-group. Show that the number of elements of order 2 in G is $2^k - 1$, for some positive integer k.

5.30. Let G be a finite abelian group. Suppose that, for every $n \in \mathbb{N}$, there are at most n elements $a \in G$ satisfying $a^n = e$. Show that G is cyclic.

5.4 A Word About Infinite Abelian Groups

Unfortunately, that word is "messy". We have seen that finite abelian groups behave very nicely. To be sure, we cannot possibly expect every infinite abelian group to be a direct product of cyclic groups of prime power order. But even if we allow direct products of infinite cyclic groups such as $\mathbb{Z} \times \mathbb{Z}$, that does not come close to covering all of the possibilities. While a deep discussion of infinite abelian groups is beyond the scope of an introductory abstract algebra course, we can make a few remarks.

Definition 5.7. Let G be a nontrivial group. We say that G is **decomposable** if it is the direct product of two proper subgroups. If not, then it is **indecomposable**.

We can easily classify the indecomposable finite abelian groups.

Theorem 5.9. *Let G be a finite abelian group. Then G is indecomposable if and only if G is a cyclic group of order p^n, for some prime p and positive integer n.*

Proof. In view of Theorem 5.3, an indecomposable finite abelian group must indeed be cyclic of prime power order. If G is cyclic of order p^n, then suppose that $G = H \times K$, for some subgroups H and K. Then by Lagrange's theorem, H and K are both p-groups. Furthermore, by Theorem 3.16, they are both cyclic. But since $G = H \times K$ is cyclic, it follows from Theorem 5.4 that $(|H|, |K|) = 1$. As the orders are both powers of p, this means that either H or K is trivial, so either K or H is all of G. Thus, H and K are not both proper and G is indecomposable. □

What about infinite abelian groups?

Example 5.15. The additive group $\mathbb{Q}$ is indecomposable. Indeed, suppose that $\mathbb{Q} = H \times K$, where H and K are proper subgroups. Then neither H nor K is $\{0\}$, so take $a/b \in H$, $c/d \in K$, where a, b, c and d are nonzero integers. Note that $bc(a/b) = ac \in H$ and $ad(c/d) = ac \in K$. Then $H \cap K$ is not trivial, so we do not have a direct product. Also, $\mathbb{Q}$ is not cyclic. Indeed, if $a, b \in \mathbb{Z}$ and $b > 0$, it is clear that $1/(b+1) \notin \langle a/b \rangle$. Thus, $\mathbb{Q} \neq \langle a/b \rangle$.

Now, every element of $\mathbb{Q}$ other than the identity has infinite order. What about infinite abelian groups where every element has finite order?

Example 5.16. Consider the group $\mathbb{Q}/\mathbb{Z}$. Exercise 5.31 asks us to examine some properties of this group. In particular, the distinct elements of the group are precisely of the form $q + \mathbb{Z}$, where $q \in \mathbb{Q}$ and $0 \leq q < 1$. Also, every element has finite order. But this group is decomposable. Indeed, fix any prime p. Then let $H = \{a/b + \mathbb{Z} : a, b \in \mathbb{Z}, b = p^n, n \geq 0\}$ and $K = \{c/d + \mathbb{Z} : c, d \in \mathbb{Z}, (d, p) = 1\}$. In Exercise 5.32, we also demonstrate that $\mathbb{Q}/\mathbb{Z} = H \times K$.

The group H from the preceding example is named for E.P. Heinz Prüfer.

Definition 5.8. Let p be a prime. Then the **Prüfer p-group** is the subgroup $\{a/p^n + \mathbb{Z} : a, n \in \mathbb{Z}, n \geq 0\}$ of the additive group $\mathbb{Q}/\mathbb{Z}$.

Example 5.17. Let H be the Prüfer p-group. We note that H is an abelian p-group; indeed, $p^n(a/p^n + \mathbb{Z}) = a + \mathbb{Z} = 0 + \mathbb{Z}$; thus, the order of $a/p^n + \mathbb{Z}$ divides p^n. But H is not cyclic; indeed, $1/p^n + \mathbb{Z}$ has order p^n, so H has elements of arbitrarily large order. So if it were cyclic, what order could its generator possibly have? However, Exercise 5.36 asks us to show that every nontrivial subgroup of H contains $1/p + \mathbb{Z}$. Thus, H is surely indecomposable.

In fact, $\mathbb{Q}$ and the Prüfer p-group share another interesting property.

Definition 5.9. Let G be an abelian group written additively. We say that G is **divisible** if, for every element a of G and every positive integer n, there exists a $b \in G$ such that $nb = a$.

Note that if G is a nontrivial finite abelian group, then it cannot be divisible. Indeed, if G has order n, then $nb = 0$ for every $b \in G$. Thus, if $0 \neq a \in G$, then $nb = a$ has no solution. So, we must look to infinite abelian groups.

Example 5.18. The group $\mathbb{Q}$ is divisible. Indeed, if $a \in \mathbb{Q}$ and n is a positive integer, then $n(a/n) = a$.

Example 5.19. For any prime p, the Prüfer p-group is divisible. Indeed, to see this, we note that if G is divisible, so is any factor group of G. (See Exercise 5.35.) Thus, $\mathbb{Q}/\mathbb{Z}$ is divisible. As in Example 5.16, write $\mathbb{Q}/\mathbb{Z} = H \times K$, where H is the Prüfer p-group. If $a \in H$, then by the divisibility of $\mathbb{Q}/\mathbb{Z}$, for any positive integer n, there exist $h \in H, k \in K$ such that $n(h, k) = (a, 0)$. But then $nh = a$.

Exercises

5.31. Let $G = \mathbb{Q}/\mathbb{Z}$.

1. Show that the elements of G can be uniquely written in the form $q + \mathbb{Z}$, where $q \in \mathbb{Q}$ and $0 \leq q < 1$.
2. If $a, b \in \mathbb{Z}, b > 0$ and $(a, b) = 1$, what is the order of $a/b + \mathbb{Z}$ in G?

5.32. Show that for any prime p, $\mathbb{Q}/\mathbb{Z} = H \times K$, where H is the Prüfer p-group and $K = \{c/d + \mathbb{Z} : c, d \in \mathbb{Z}, (d, p) = 1\}$.

5.33. Let G be a divisible group, written additively. Show that for every positive integer n, the function $\alpha : G \to G$ given by $\alpha(a) = na$ is an onto homomorphism. Is it necessarily an automorphism?

5.34. Let G and H be abelian groups, written additively. Show that $G \times H$ is divisible if and only if G and H are both divisible.

5.35. Show that if G is a divisible group, then every factor group of G is divisible, but subgroups need not be.

5.36. Let G be the Prüfer p-group, for some prime p. Show that every nontrivial subgroup of G contains $1/p + \mathbb{Z}$.

5.37. Let G be an abelian group having a subgroup N such that G/N is infinite cyclic. Show that G has a subgroup H such that H is infinite cyclic and $G = H \times N$.

5.38. For any prime p, show that every proper subgroup of the Prüfer p-group is finite.