Our next aim is to illustrate how to pass from a list of invariant factors of a finite abelian group to its list of elementary divisors and vice versa. We show how to determine these invariants of the group no matter how it is given as a direct product of cyclic groups. We need the following proposition.

Proposition 6. Let $m, n \in \mathbb{Z}^+$.
  (1) $Z_m \times Z_n \cong Z_{mn}$ if and only if $(m, n) = 1$.
  (2) If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ then $Z_n \cong Z_{p_1^{\alpha_1}} \times Z_{p_2^{\alpha_2}} \times \cdots \times Z_{p_k^{\alpha_k}}$.

Proof: Since (2) is an easy exercise using (1) and induction on k, we concentrate on proving (1). Let $Z_m = \langle x \rangle$, $Z_n = \langle y \rangle$ and let $l = $ l.c.m.(m, n). Note that $l = mn$ if and only if $(m, n) = 1$. Let $x^a y^b$ be a typical element of $Z_m \times Z_n$. Then (as noted in Example 1, Section 1)

$$(x^a y^b)^l = x^{la} y^{lb}$$
$$= 1^a 1^b = 1 \qquad \text{(because } m \mid l \text{ and } n \mid l\text{).}$$

If $(m, n) \neq 1$, every element of $Z_m \times Z_n$ has order at most l, hence has order strictly less than mn, so $Z_m \times Z_n$ cannot be isomorphic to Z_{mn}.

Conversely, if $(m, n) = 1$, then $|xy| = $ l.c.m.$(|x|, |y|) = mn$. Thus, by order considerations, $Z_m \times Z_n = \langle xy \rangle$ is cyclic, completing the proof.

Obtaining Elementary Divisors from Invariant Factors

Suppose G is given as an abelian group of type $(n_1, n_2, \ldots, n_s)$, that is

$$G \cong Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_s}.$$

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = n_1 n_2 \cdots n_s$. Factor each n_i as

$$n_i = p_1^{\beta_{i1}} p_2^{\beta_{i2}} \cdots p_k^{\beta_{ik}}, \quad \text{where } \beta_{ij} \geq 0.$$

By the proposition above,

$$Z_{n_i} \cong Z_{p_1^{\beta_{i1}}} \times \cdots \times Z_{p_k^{\beta_{ik}}},$$

for each i. If $\beta_{ij} = 0$, $Z_{p_j^{\beta_{ij}}} = 1$ and this factor may be deleted from the direct product without changing the isomorphism type. Then the elementary divisors of G are precisely the integers

$$p_j^{\beta_{ij}}, \qquad 1 \leq j \leq k, \quad 1 \leq i \leq s \text{ such that } \beta_{ij} \neq 0.$$

For example, if $|G| = 2^3 \cdot 3^2 \cdot 5^2$ and G is of type $(30, 30, 2)$, then

$$G \cong Z_{30} \times Z_{30} \times Z_2.$$

Since $Z_{30} \cong Z_2 \times Z_3 \times Z_5$, $G \cong Z_2 \times Z_3 \times Z_5 \times Z_2 \times Z_3 \times Z_5 \times Z_2$. The elementary divisors of G are therefore 2, 3, 5, 2, 3, 5, 2, or, grouping like primes together (note that rearranging the order of the factors in a direct product does not affect the isomorphism type (Exercise 7 of Section 1)), 2, 2, 2, 3, 3, 5, 5. In particular, G is isomorphic to the last group in the list in the example above.

If for each j one collects all the factors $Z_{p_j^{\beta_{ij}}}$ together, the resulting direct product forms the Sylow p_j-subgroup, A_j, of G. Thus the Sylow 2-subgroup of the group in the preceding paragraph is isomorphic to $Z_2 \times Z_2 \times Z_2$ (i.e., the elementary abelian group of order 8).

Obtaining Elementary Divisors from any cyclic decomposition

The same process described above will give the elementary divisors of a finite abelian group G whenever G is given as a direct product of cyclic groups (not just when the orders of the cyclic components are the invariant factors). For example, if $G = Z_6 \times Z_{15}$, the list 6, 15 is neither that of the invariant factors (the divisibility condition fails) nor that of elementary divisors (they are not prime powers). To find the elementary divisors, factor $6 = 2 \cdot 3$ and $15 = 3 \cdot 5$. Then the prime powers 2, 3, 3, 5 are the elementary divisors and

$$G \cong Z_2 \times Z_3 \times Z_3 \times Z_5.$$

Obtaining Invariant Factors from Elementary Divisors

Suppose G is an abelian group of order n, where $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ and we are given the elementary divisors of G. The invariant factors of G are obtained by following these steps:
(1) First group all elementary divisors which are powers of the same prime together. In this way we obtain k lists of integers (one for each p_j).
(2) In each of these k lists arrange the integers in nonincreasing order.
(3) Among these k lists suppose that the longest (i.e., the one with the most terms) consists of t integers. Make each of the k lists of length t by appending an appropriate number of 1's at the end of each list.
(4) For each $i \in \{1, 2, \ldots, t\}$ the ith invariant factor, n_i, is obtained by taking the product of the ith integer in each of the t (ordered) lists.

The point of ordering the lists in this way is to ensure that we have the divisibility condition $n_{i+1} \mid n_i$.

Suppose, for example, that the elementary divisors of G are given as 2, 3, 2, 25, 3, 2 (so $|G| = 2^3 \cdot 3^2 \cdot 5^2$). Regrouping and increasing each list to have 3 $(= t)$ members gives:

$p = 2$	$p = 3$	$p = 5$
2	3	25
2	3	1
2	1	1

so the invariant factors of G are $2 \cdot 3 \cdot 25$, $2 \cdot 3 \cdot 1$, $2 \cdot 1 \cdot 1$ and

$$G \cong Z_{150} \times Z_6 \times Z_2.$$

Note that this is the penultimate group in the list classifying abelian groups of order 1800 computed above.

The invariant factor decompositions of the abelian groups of order 1800 are as follows, where the ith group in this list is isomorphic to the ith group computed in the

previous list:

$$Z_{1800}$$
$$Z_{360} \times Z_5$$
$$Z_{600} \times Z_3$$
$$Z_{120} \times Z_{15}$$
$$Z_{900} \times Z_2$$
$$Z_{180} \times Z_{10}$$

$$Z_{300} \times Z_6$$
$$Z_{60} \times Z_{30}$$
$$Z_{450} \times Z_2 \times Z_2$$
$$Z_{90} \times Z_{10} \times Z_2$$
$$Z_{150} \times Z_6 \times Z_2$$
$$Z_{30} \times Z_{30} \times Z_2.$$

Using the uniqueness statements of the Fundamental Theorems 3 and 5, we can use these processes to determine whether any two direct products of finite cyclic groups are isomorphic. For instance, if one wanted to know whether $Z_6 \times Z_{15} \cong Z_{10} \times Z_9$, first determine whether they have the same order (both are of order 90) and then (the easiest way in general) determine whether they have the same elementary divisors:

$Z_6 \times Z_{15}$ has elementary divisors 2, 3, 3, 5 and is isomorphic to $Z_2 \times Z_3 \times Z_3 \times Z_5$

$Z_{10} \times Z_9$ has elementary divisors 2, 5, 9 and is isomorphic to $Z_2 \times Z_5 \times Z_9$.

The lists of elementary divisors are different so (by Theorem 5) they are not isomorphic. Note that $Z_6 \times Z_{15}$ has no element of order 9 whereas $Z_{10} \times Z_9$ does (cf. Exercise 5).

The processes we described above (with some elaboration) form a proof (via Proposition 6) that for finite abelian groups Theorems 3 and 5 are equivalent (i.e., one implies the other). We leave the details to the reader.

One can now better understand some of the power and some of the limitations of classification theorems. On one hand, given any positive integer n one can explicitly describe all abelian groups of order n, a significant achievement. On the other hand, the amount of information necessary to determine which of the isomorphism types of groups of order n a particular group belongs to may be considerable (and is large if n is divisible by large powers of primes).

We close this section with some terminology which will be useful in later sections.

Definition.
(1) If G is a finite abelian group of type $(n_1, n_2, \ldots, n_t)$, the integer t is called the *rank* of G (the free rank of G is 0 so there will be no confusion).
(2) If G is any group, the *exponent* of G is the smallest positive integer n such that $x^n = 1$ for all $x \in G$ (if no such integer exists the exponent of G is ∞).

EXERCISES

1. In each of parts (a) to (e) give the number of nonisomorphic abelian groups of the specified order — do not list the groups: (a) order 100, (b) order 576, (c) order 1155, (d) order 42875, (e) order 2704.
2. In each of parts (a) to (e) give the lists of invariant factors for all abelian groups of the specified order:
(a) order 270, (b) order 9801, (c) order 320, (d) order 105, (e) order 44100.
3. In each of parts (a) to (e) give the lists of elementary divisors for all abelian groups of the specified order and then match each list with the corresponding list of invariant factors

found in the preceding exercise:
(a) order 270, **(b)** order 9801, **(c)** order 320, **(d)** order 105, **(e)** order 44100.

4. In each of parts (a) to (d) determine which pairs of abelian groups listed are isomorphic (here the expression $\{a_1, a_2, \ldots, a_k\}$ denotes the abelian group $Z_{a_1} \times Z_{a_2} \times \cdots \times Z_{a_k}$).
   (a) $\{4, 9\}$, $\{6, 6\}$, $\{8, 3\}$, $\{9, 4\}$, $\{6, 4\}$, $\{64\}$.
   (b) $\{2^2, 2 \cdot 3^2\}$, $\{2^2 \cdot 3, 2 \cdot 3\}$, $\{2^3 \cdot 3^2\}$, $\{2^2 \cdot 3^2, 2\}$.
   (c) $\{5^2 \cdot 7^2, 3^2 \cdot 5 \cdot 7\}$, $\{3^2 \cdot 5^2 \cdot 7, 5 \cdot 7^2\}$, $\{3 \cdot 5^2, 7^2, 3 \cdot 5 \cdot 7\}$,
   $\{5^2 \cdot 7, 3^2 \cdot 5, 7^2\}$.
   (d) $\{2^2 \cdot 5 \cdot 7, 2^3 \cdot 5^3, 2 \cdot 5^2\}$, $\{2^3 \cdot 5^3 \cdot 7, 2^3 \cdot 5^3\}$, $\{2^2, 2 \cdot 7, 2^3, 5^3, 5^3\}$,
   $\{2 \cdot 5^3, 2^2 \cdot 5^3, 2^3, 7\}$.

5. Let G be a finite abelian group of type $(n_1, n_2, \ldots, n_t)$. Prove that G contains an element of order m if and only if $m \mid n_1$. Deduce that G is of exponent n_1.

6. Prove that any finite group has a finite exponent. Give an example of an infinite group with finite exponent. Does a finite group of exponent m always contain an element of order m?

7. Let p be a prime and let $A = \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_n \rangle$ be an abelian p-group, where $|x_i| = p^{\alpha_i} > 1$ for all i. Define the pth-*power map*

$$\varphi : A \to A \qquad \text{by} \qquad \varphi : x \mapsto x^p.$$

   (a) Prove that φ is a homomorphism.
   (b) Describe the image and kernel of φ in terms of the given generators.
   (c) Prove both $\ker \varphi$ and $A/\text{im } \varphi$ have rank n (i.e., have the same rank as A) and prove these groups are both isomorphic to the elementary abelian group, E_{p^n}, of order p^n.

8. Let A be a finite abelian group (written multiplicatively) and let p be a prime. Let

$$A^p = \{a^p \mid a \in A\} \qquad \text{and} \qquad A_p = \{x \mid x^p = 1\}$$

   (so A^p and A_p are the image and kernel of the pth-power map, respectively).
   (a) Prove that $A/A^p \cong A_p$. [Show that they are both elementary abelian and they have the same order.]
   (b) Prove that the number of subgroups of A of order p equals the number of subgroups of A of index p. [Reduce to the case where A is an elementary abelian p-group.]

9. Let $A = Z_{60} \times Z_{45} \times Z_{12} \times Z_{36}$. Find the number of elements of order 2 and the number of subgroups of index 2 in A.

10. Let n and k be positive integers and let A be the free abelian group of rank n (written additively). Prove that A/kA is isomorphic to the direct product of n copies of $\mathbb{Z}/k\mathbb{Z}$ (here $kA = \{ka \mid a \in A\}$). [See Exercise 14, Section 1.]

11. Let G be a nontrivial finite abelian group of rank t.
   (a) Prove that the rank of G equals the maximum of the ranks of its Sylow subgroups.
   (b) Prove that G can be generated by t elements but no subset with fewer than t elements generates G. [One way of doing this is by using part (a) together with Exercise 7.]

12. Let n and m be positive integers with $d = (n, m)$. Let $Z_n = \langle x \rangle$ and $Z_m = \langle y \rangle$. Let A be the central product of $\langle x \rangle$ and $\langle y \rangle$ with an element of order d identified, which has presentation $\langle x, y \mid x^n = y^m = 1, \ xy = yx, \ x^{\frac{n}{d}} = y^{\frac{m}{d}} \rangle$. Describe A as a direct product of two cyclic groups.

13. Let $A = \langle x_1 \rangle \times \cdots \times \langle x_r \rangle$ be a finite abelian group with $|x_i| = n_i$ for $1 \le i \le r$. Find a presentation for A. Prove that if G is any group containing commuting elements $g_1, \ldots, g_r$ such that $g_i^{n_i} = 1$ for $1 \le i \le r$, then there is a unique homomorphism from A to G which sends x_i to g_i for all i.