Since $d_1x_1 \in K$, we can subtract a suitable multiple of $d_1x_1$ and then using the minimality of $d_1$ to see that $h_1$ is a multiple of $d_1$, we see we actually have $k_2y_2 + \cdots + k_ny_n$ in $K$. Among all such bases $\{x_1, y_2, \cdots, y_n\}$, we choose one $Y_2$ that leads to some $k_i \neq 0$ of minimal magnitude. (It is possible all $k_i$ are always zero. In this case, $K$ is generated by $d_1x_1$ and we are done.) By renumbering the elements of $Y_2$ we can assume that there is $w_2 \in K$ such that

$$w_2 = d_2y_2 + \cdots + k_ny_n$$

where $d_2 > 0$ and $d_2$ is minimal as just described. Exactly as in the preceding paragraph, we can modify our basis from $Y_2 = \{x_1, y_2, \cdots, y_n\}$ to a basis $\{x_1, x_2, y_3, \cdots, y_n\}$ for $G$ where $d_1x_1 \in K$ and $d_2x_2 \in K$. Writing $d_2 = d_1q + r$ for $0 \leq r < d_1$, we see that $\{x_1 + qx_2, x_2, y_3, \cdots, y_n\}$ is a basis for $G$, and $d_1x_1 + d_2x_2 = d_1(x_1 + qx_2) + rx_2$ is in $K$. By our minimal choice of $d_1$, we see $r = 0$, so $d_1$ divides $d_2$.

We now consider all bases of the form $\{x_1, x_2, y_3, \cdots, y_n\}$ for $G$ and examine elements of $K$ of the form $k_3y_3 + \cdots + k_ny_n$. The pattern is clear. The process continues until we obtain a basis $\{x_1, x_2, \cdots, x_s, y_{s+1}, \cdots, y_n\}$ where the only element of $K$ of the form $k_{s+1}y_{s+1} + \cdots + k_ny_n$ is zero, that is, all $k_i$ are zero. We then let $x_{s+1} = y_{s+1}, \cdots, x_n = y_n$ and obtain a basis for $G$ of the form described in the statement of Theorem 19.11. ◆

We now prove the Invariant Factor version of the Fundamental Theorem, Theorem 9.11. We restate it here for easy reference.

**19.12 Theorem** Every finitely generated abelian group is isomorphic to a group of the form

$$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z},$$

where $m_i$ divides $m_{i+1}$ for $i = 1, \cdots, r-1$.

Furthermore, this representation is unique up to order of the factors.

***Proof*** For the purposes of this proof, it will be convenient to use as notations $\mathbb{Z}/1\mathbb{Z} = \mathbb{Z}/\mathbb{Z} \simeq \mathbb{Z}_1 = \{0\}$. Let $G$ be finitely generated by $n$ elements. Let $F = \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ for $n$ factors. Consider the homomorphism $\phi : F \to G$ of Theorem 19.8, and let $K$ be the kernel of this homomorphism. Then there is a basis for $F$ of the form $\{x_1, \cdots, x_n\}$, where $\{d_1x_1, \cdots, d_sx_s\}$ is a basis for $K$ and $d_i$ divides $d_{i+1}$ for $i = 1, \cdots, s-1$. By Theorem 12.14, $G$ is isomorphic to $F/K$. But

$$\begin{aligned} F/K &\simeq (\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z})/(d_1\mathbb{Z} \times d_2\mathbb{Z} \times \cdots \times d_s\mathbb{Z} \times \{0\} \times \cdots \times \{0\}) \\ &\simeq \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_s} \times \mathbb{Z} \times \cdots \times \mathbb{Z}. \end{aligned}$$

It is possible that $d_1 = 1$, in which case $\mathbb{Z}_{d_1} = \{0\}$ and can be dropped (up to isomorphism) from this product. Similarly, $d_2$ may be 1, and so on. We let $m_1$ be the first $d_i > 1$, $m_2$ be the next $d_i$, and so on, and our theorem follows at once.

We have demonstrated the toughest part of the Fundamental Theorem. Of course, a prime-power decomposition exists since we can break the groups $\mathbb{Z}_{m_i}$ into prime-power factors. The only remaining part of Theorem 9.12 concerns the uniqueness of the Betti number, of the torsion coefficients, and of the prime powers. The Betti number appears as the rank of the free abelian group $G/T$, where $T$ is the torsion subgroup of $G$. This rank is invariant by Theorem 19.6, which shows the uniqueness of the Betti number. The uniqueness of the torsion coefficients and of prime powers is a bit more difficult to show. We give some exercises that indicate their uniqueness (see Exercises 14 through 22). ◆

## EXERCISES 19

### Computations

**1.** Find a basis $\{(a_1, a_2, a_3), (b_1, b_2, b_3), (c_1, c_2, c_3)\}$ for $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ with all $a_i \neq 0$, all $b_i \neq 0$, and all $c_i \neq 0$. (Many answers are possible.)

**2.** Is $\{(2, 1), (3, 1)\}$ a basis for $\mathbb{Z} \times \mathbb{Z}$? Prove your assertion.

**3.** Is $\{(2, 1), (4, 1)\}$ a basis for $\mathbb{Z} \times \mathbb{Z}$? Prove your assertion.

**4.** Find conditions on $a, b, c, d \in \mathbb{Z}$ for $\{(a, b), (c, d)\}$ to be a basis for $\mathbb{Z} \times \mathbb{Z}$. [*Hint:* Solve $x(a, b) + y(c, d) = (e, f)$ in $\mathbb{R}$, and see when the $x$ and $y$ lie in $\mathbb{Z}$.]

### Concepts

In Exercises 5 and 6, correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a form acceptable for publication.

**5.** The *rank* of a free abelian group $G$ is the number of elements in a generating set for $G$.

**6.** A *basis* for a nonzero abelian group $G$ is a generating set $X \subseteq G$ such that $n_1x_1 + n_2x_2 + \cdots + n_mx_m = 0$ for distinct $x_i \in X$ and $n_i \in \mathbb{Z}$ only if $n_1 = n_2 = \cdots = n_m = 0$.

**7.** Show by example that it is possible for a proper subgroup of a free abelian group of finite rank $r$ also to have rank $r$.

**8.** Determine whether each of the following is true or false.

- **a.** Every free abelian group is torsion free.
- **b.** Every finitely generated torsion-free abelian group is a free abelian group.
- **c.** There exists a free abelian group of every positive integer rank.
- **d.** A finitely generated abelian group is free abelian if its Betti number equals the number of elements in some generating set.
- **e.** If $X$ generates a free abelian group $G$ and $X \subseteq Y \subseteq G$, then $Y$ generates $G$.
- **f.** If $X$ is a basis for a free abelian group $G$ and $X \subseteq Y \subseteq G$, then $Y$ is a basis for $G$.
- **g.** Every nonzero free abelian group has an infinite number of bases.
- **h.** Every free abelian group of rank at least 2 has an infinite number of bases.
- **i.** If $K$ is a nonzero subgroup of a finitely generated free abelian group, then $K$ is free abelian.
- **j.** If $K$ is a nonzero subgroup of a finitely generated free abelian group, then $G/K$ is free abelian.

### Theory

**9.** Complete the proof of Theorem 19.5 (See the two sentences preceding the theorem).

**10.** Show that a free abelian group contains no nonzero elements of finite order.

**11.** Show that if $G$ and $G'$ are free abelian groups, then $G \times G'$ is free abelian.

**12.** Show that free abelian groups of finite rank are precisely the finitely generated abelian groups containing no nonzero elements of finite order.

**13.** Show that $\mathbb{Q}$ under addition is not a free abelian group.

Exercises 14 through 19 deal with showing the uniqueness of the prime powers appearing in the prime-power decomposition of the torsion subgroup $T$ of a finitely generated abelian group.

**14.** Let $p$ be a fixed prime. Show that the elements of $T$ having as order some power of $p$, together with zero, form a subgroup $T_p$ of $T$.

**15.** Show that in any prime-power decomposition of $T$, the subgroup $T_p$ in the preceding exercise is isomorphic to the direct product of those cyclic factors of order some power of the prime $p$. [This reduces our problem to showing that the group $T_p$ cannot have essentially different decompositions into products of cyclic groups.]

**16.** Let $G$ be any abelian group and let $n$ be any positive integer. Show that $G[n] = \{x \in G \mid nx = 0\}$ is a subgroup of $G$. (In multiplicative notation, $G[n] = \{x \in G \mid x^n = e\}$.)

**17.** Referring to Exercise 16, show that $\mathbb{Z}_{p^r}[p] \simeq \mathbb{Z}_p$ for any $r \geq 1$ and prime $p$.

**18.** Using Exercise 17, show that

$$(\mathbb{Z}_{p^{r_1}} \times \mathbb{Z}_{p^{r_2}} \times \cdots \times \mathbb{Z}_{p^{r_m}})[p] \simeq \underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{m \text{ factors}}$$

provided each $r_i \geq 1$.

**19.** Let $G$ be a finitely generated abelian group and $T_p$ the subgroup defined in Exercise 14. Suppose $T_p \simeq \mathbb{Z}_{p^{r_1}} \times \mathbb{Z}_{p^{r_2}} \times \cdots \times \mathbb{Z}_{p^{r_m}} \simeq \mathbb{Z}_{p^{s_1}} \times \mathbb{Z}_{p^{s_2}} \times \cdots \times \mathbb{Z}_{p^{s_n}}$, where $1 \leq r_1 \leq r_2 \leq \cdots \leq r_m$ and $1 \leq s_1 \leq s_2 \leq \cdots \leq s_n$. We need to show that $m = n$ and $r_i = s_i$ for $i = 1, \cdots, n$ to complete the demonstration of uniqueness of the prime-power decomposition.

**a.** Use Exercise 18 to show that $n = m$.

**b.** Show $r_1 = s_1$. Suppose $r_i = s_i$ for all $i < j$. Show $r_j = s_j$, which will complete the proof. [*Hint:* Suppose $r_j < s_j$. Consider the subgroup $p^{r_j}T_p = \{p^{r_j}x \mid x \in T_p\}$, and show that this subgroup would then have two prime-power decompositions involving different numbers of nonzero factors. Then argue that this is impossible by part (a) of this exercise.]

Let $T$ be the torsion subgroup of a finitely generated abelian group. Suppose $T \simeq \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r} \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$, where $m_i$ divides $m_{i+1}$ for $i = 1, \cdots, r-1$, and $n_j$ divides $n_{j+1}$ for $n = 1, \cdots, s-1$, and $m_1 > 1$ and $n_1 > 1$. We wish to show that $r = s$ and $m_k = n_k$ for $k = 1, \cdots, r$, demonstrating the uniqueness of the torsion coefficients. This is done in Exercises 20 through 22.

**20.** Indicate how a prime-power decomposition can be obtained from a torsion-coefficient decomposition. (Observe that the preceding exercises show the prime powers obtained are unique.)

**21.** Argue from Exercise 20 that $m_r$ and $n_s$ can both be characterized as follows. Let $p_1, \cdots, p_t$ be the distinct primes dividing $|T|$, and let $p_1^{h_1}, \cdots, p_t^{h_t}$ be the highest powers of these primes appearing in the (unique) prime-power decomposition. Then $m_r = n_s = p_1^{h_1} p_2^{h_2} \cdots p_t^{h_t}$.

**22.** Characterize $m_{r-1}$ and $n_{s-1}$, showing that they are equal, and continue to show $m_{r-i} = n_{s-1}$ for $i = 1, \cdots, r-1$, and then $r = s$.

## SECTION 20 FREE GROUPS

For any group with elements $a$ and $b$ we have certain relations that $a$ and $b$ must satisfy simply because they are elements of a group. For example, $a^n a^m = a^{n+m}$ and $(ab)^{-1} = b^{-1}a^{-1}$. For most of the groups we have studied so far there are relations among the elements other than the relations that all groups possess. For example, the elements $\mu$ and $\rho$ in the dihedral group $D_n$ satisfy relations $\rho\mu = \mu\rho^{-1}$ and $\mu^2 = \rho^n = \iota$. In this section, we construct free groups that have only the relations that are required in the definition of a group. These groups and their factor groups as described in Section 21 are of great interest in the study of algebra and topology.

### Words and Reduced Words

Let $A \neq \emptyset$ be any (not necessarily finite) set of elements $a_i$ for $i \in I$. We think of $A$ as an **alphabet** and of the $a_i$ as **letters** in the alphabet. Any symbol of the form $a_i^n$ with $n \in \mathbb{Z}$ is a **syllable** and a finite string $w$ of syllables written in juxtaposition is a **word.** We also introduce the **empty word** 1, which has no syllables.

**20.1 Example** Let $A = \{a_1, a_2, a_3\}$. Then

$$a_1 a_3^{-4} a_2^2 a_3, \qquad a_2^3 a_2^{-1} a_3 a_1^2 a_1^{-7}, \qquad \text{and} \qquad a_3^2$$

are all words, if we follow the convention of understanding that $a_i^1$ is the same as $a_i$. ▲

There are two natural types of modifications of certain words, the **elementary contractions.** The first type consists of replacing an occurrence of $a_i^m a_i^n$ in a word by $a_i^{m+n}$. The second type consists of replacing an occurrence of $a_i^0$ in a word by 1, that is, dropping it out of the word. By means of a finite number of elementary contractions, every word can be changed to a **reduced word,** one for which no more elementary contractions are possible. Note that these elementary contractions formally amount to the usual manipulations of integer exponents and would have to be satisfied if we wish for the letters to be elements of a group.

**20.2 Example** The reduced form of the word $a_2^3 a_2^{-1} a_3 a_1^2 a_1^{-7}$ of Example 20.1 is $a_2^2 a_3 a_1^{-5}$. ▲

It should be said here once and for all that we are going to gloss over several points that some books spend pages proving, usually by complicated induction arguments broken down into many cases. For example, suppose we are given a word and wish to find its reduced form. There may be a variety of elementary contractions that could be performed first. How do we know that the reduced word we end up with is the same no matter in what order we perform the elementary contractions? The student will probably say this is obvious. Some authors spend considerable effort proving this. The authors agree here with the student. Proofs of this sort we regard as tedious, and they have never made us more comfortable about the situation. However, the authors are the first to acknowledge that we are not great mathematicians. In deference to the fact that many mathematicians feel that these things do need considerable discussion, we shall mark an occasion when we just state such facts by the phrase, "It would seem obvious that," keeping the quotation marks.

## Free Groups

Let the set of all reduced words formed from our alphabet $A$ be $F[A]$. We now make $F[A]$ into a group in a natural way. For $w_1$ and $w_2$ in $F[A]$, define $w_1 \cdot w_2$ to be the reduced form of the word obtained by the juxtaposition $w_1 w_2$ of the two words.

**20.3 Example** If

$$w_1 = a_2^3 a_1^{-5} a_3^2$$

and

$$w_2 = a_3^{-2} a_1^2 a_3 a_2^{-2},$$

then $w_1 \cdot w_2 = a_2^3 a_1^{-3} a_3 a_2^{-2}$. ▲

"It would seem obvious that" this operation of multiplication on $F[A]$ is well defined and associative. The empty word 1 acts as an identity element. "It would seem obvious that" given a reduced word $w \in F[A]$, if we form the word obtained by first writing the syllables of $w$ in the opposite order and second by replacing each $a_i^n$ by $a_i^{-n}$, then the resulting word $w^{-1}$ is a reduced word also, and

$$w \cdot w^{-1} = w^{-1} \cdot w = 1.$$

**20.4 Definition** The group $F[A]$ just described is the **free group generated** by $A$. ■

Look back at Theorem 7.7 and the definition preceding it to see that the present use of the term *generated* is consistent with the earlier use.

Starting with a group $G$ and a generating set $\{a_i \mid i \in I\}$, which we will abbreviate by $\{a_i\}$, we might ask if $G$ is *free* on $\{a_i\}$, that is, if $G$ is essentially the free group generated by $\{a_i\}$. We define precisely what this is to mean.