Proof Let G have a basis $\{x_1, x_2, \cdots, x_r\}$. Then G is isomorphic to $\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ for r factors. Let $2G = \{2g \mid g \in G\}$. It is readily checked that $2G$ is a subgroup of G. Since $G \simeq \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ for r factors, we have

$$\begin{aligned} G/2G &\simeq (\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z})/(2\mathbb{Z} \times 2\mathbb{Z} \times \cdots \times 2\mathbb{Z}) \\ &\simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2 \end{aligned}$$

for r factors. Thus $|G/2G| = 2^r$, so the number of elements in any finite basis X is $\log_2 |G/2G|$. Thus any two finite bases have the same number of elements.

It remains to show that G cannot also have an infinite basis. Let Y be any basis for G, and let $\{y_1, y_2, \cdots, y_s\}$ be distinct elements in Y. Let H be the subgroup of G generated by $\{y_1, y_2, \cdots, y_s\}$, and let K be the subgroup of G generated by the remaining elements of Y. It is readily checked that $G \simeq H \times K$, so

$$G/2G \simeq (H \times K)/(2H \times 2K) \simeq (H/2H) \times (K/2K).$$

Since $|H/2H| = 2^s$, we see $|G/2G| \geq 2^s$. Since we have $|G/2G| = 2^r$, we see that $s \leq r$. Then Y cannot be an infinite set, for we could take $s > r$. ◆

19.7 Definition If G is a free abelian group, the **rank** of G is the number of elements in a basis for G. (All bases have the same number of elements.) ■

Proof of the Fundamental Theorem

We shall prove the Invariant Factor version of the Fundamental Theorem (Theorem 9.14) by showing that any finitely generated abelian group is isomorphic to a factor group of the form

$$(\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z})/(d_1\mathbb{Z} \times d_2\mathbb{Z} \times \cdots \times d_s\mathbb{Z} \times \{0\} \times \cdots \times \{0\}),$$

where both "numerator" and "denominator" have n factors, and d_1 divides d_2, which divides $d_3 \cdots$, which divides d_s. The Prime Factor version, Theorem 9.12, will then follow.

To show that G is isomorphic to such a factor group, we will show that there is a homomorphism of $\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ onto G with kernel of the form $d_1\mathbb{Z} \times d_2\mathbb{Z} \times \cdots \times d_s\mathbb{Z} \times \{0\} \times \cdots \times \{0\}$. The result will then follow by Theorem 12.14. The theorems that follow give the details of the argument. Our purpose in these introductory paragraphs is to let us see where we are going as we read what follows.

19.8 Theorem Let G be a finitely generated abelian group with generating set $\{a_1, a_2, \cdots, a_n\}$. Let

$$\phi : \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{n \text{ factors}} \to G$$

be defined by $\phi(h_1, h_2, \cdots, h_n) = h_1a_1 + h_2a_2 + \cdots + h_na_n$. Then ϕ is a homomorphism onto G.

Proof From the meaning of h_ia_i for $h_i \in \mathbb{Z}$ and $a_i \in G$, we see at once that

$$\begin{aligned} \phi[(h_1, \cdots, h_n) + (k_1, \cdots, k_n)] &= \phi(h_1 + k_1, \cdots, h_n + k_n) \\ &= (h_1 + k_1)a_1 + \cdots + (h_n + k_n)a_n \\ &= (h_1a_1 + k_1a_1) + \cdots + (h_na_n + k_na_n) \\ &= (h_1a_1 + \cdots + h_na_n) + (k_1a_1 + \cdots + k_na_n) \\ &= \phi(k_1, \cdots, k_n) + \phi(h_1, \cdots, h_n). \end{aligned}$$

Since $\{a_1, \cdots, a_n\}$ generates G, clearly the homomorphism ϕ is onto G. ◆

We now prove a "replacement property" that makes it possible for us to adjust a basis.

19.9 Theorem If $X = \{x_1, \cdots, x_r\}$ is a basis for a free abelian group G and $t \in \mathbb{Z}$, then for $i \neq j$, the set

$$Y = \{x_1, \cdots, x_{j-1}, x_j + tx_i, x_{j+1}, \cdots, x_r\}$$

is also a basis for G.

Proof Since $x_j = (-t)x_i + (1)(x_j + tx_i)$, we see that x_j can be recovered from Y, which thus also generates G. Suppose

$$n_1x_1 + \cdots + n_{j-1}x_{j-1} + n_j(x_j + tx_i) + n_{j+1}x_{j+1} + \cdots + n_rx_r = 0.$$

Then

$$n_1x_1 + \cdots + (n_i + n_jt)x_i + \cdots + n_jx_j + \cdots + n_rx_r = 0.$$

and since X is a basis, $n_1 = \cdots = n_i + n_jt = \cdots = n_j = \cdots = n_r = 0$. From $n_j = 0$ and $n_i + n_jt = 0$, it follows that $n_i = 0$ also, so $n_1 = \cdots = n_i = \cdots = n_j = \cdots = n_r = 0$, and Condition 2 of Theorem 19.1 is satisfied. Thus Y is a basis. ◆

19.10 Example A basis for $\mathbb{Z} \times \mathbb{Z}$ is $\{(1, 0), (0, 1)\}$. Another basis is $\{(1, 0), (4, 1)\}$ for $(4, 1) = 4(1, 0) + (0, 1)$. However, $\{(3, 0), (0, 1)\}$ is not a basis. For example, we cannot express $(2, 0)$ in the form $n_1(3, 0) + n_2(0, 1)$, for $n, n_2 \in \mathbb{Z}$. Here $(3, 0) = (1, 0) + 2(1, 0)$, and a multiple of a basis element was added to *itself*, rather than to a *different* basis element. ▲

A free abelian group G of finite rank may have many bases. We show that if $K \leq G$, then K is also free abelian with rank not exceeding that of G. Equally important, there exist bases of G and K nicely related to each other.

19.11 Theorem Let G be a nonzero free abelian group of finite rank n, and let K be a nonzero subgroup of G. Then K is free abelian of rank $s \leq n$. Furthermore, there exists a basis $\{x_1, x_2, \cdots, x_n\}$ for G and positive integers, $d_1, d_2, \cdots, d_s$ where d_i divides d_{i+1} for $i = 1, \cdots, s-1$, such that $\{d_1x_1, d_2x_2, \cdots, d_sx_s\}$ is a basis for K.

Proof We show that K has a basis of the described form, which will show that K is free abelian of rank at most n. Suppose $Y = \{y_1, \cdots, y_n\}$ is a basis for G. All nonzero elements in K can be expressed in the form

$$k_1y_1 + \cdots + k_ny_n,$$

where some $|k_i|$ is nonzero. Among *all* bases Y for G, select one Y_1 that yields the minimal such nonzero value $|k_i|$ as all nonzero elements of K are written in terms of the basis elements in Y_1. By renumbering the elements of Y_1 if necessary, we can assume there is $w_1 \in K$ such that

$$w_1 = d_1y_1 + k_2y_2 + \cdots + k_ny_n$$

where $d_1 > 0$ and d_1 is the minimal attainable coefficient as just described. Using the division algorithm, we write $k_j = d_1q_j + r_j$ where $0 \leq r_j < d_1$ for $j = 2, \cdots, n$. Then

$$w_1 = d_1(y_1 + q_2y_2 + \cdots + q_ny_n) + r_2y_2 + \cdots + r_ny_n. \tag{1}$$

Now let $x_1 = y_1 + q_2y_2 + \cdots + q_ny_n$. By Theorem 19.9 $\{x_1, y_2, \cdots, y_n\}$ is also a basis for G. From Eq. (1) and our choice of Y_1 for minimal coefficient d_1, we see that $r_2 = \cdots = r_n = 0$. Thus $d_1x_1 \in K$.

We now consider bases for G of the form $\{x_1, y_2, \cdots, y_n\}$. Each element of K can be expressed in the form

$$h_1x_1 + k_2y_2 + \cdots + k_ny_n.$$