

Chapter 6. The Classification of Finite Abelian Groups

6.1 Note: In this chapter we will use additive notation for all abelian groups.

6.2 Definition: A **free abelian group** of **rank** n is an abelian group isomorphic to \mathbb{Z}^n .

6.3 Theorem: The rank of a free abelian group G is unique, that is if $G \cong \mathbb{Z}^n$ and $G \cong \mathbb{Z}^m$ then $n = m$.

Proof: Suppose that $G \cong \mathbb{Z}^n$ and $G \cong \mathbb{Z}^m$ so that $\mathbb{Z}^n \cong \mathbb{Z}^m$. Let $\phi : \mathbb{Z}^n \rightarrow \mathbb{Z}^m$ be an isomorphism. Note that ϕ sends $2\mathbb{Z}^n$ bijectively to $2\mathbb{Z}^m$, so it induces an isomorphism $\psi : \mathbb{Z}^n/2\mathbb{Z}^n \rightarrow \mathbb{Z}^m/2\mathbb{Z}^m$ given by $\psi(k+2\mathbb{Z}^n) = \phi(k)+2\mathbb{Z}^m$. Also note that $\mathbb{Z}^n/2\mathbb{Z}^n \cong \mathbb{Z}_2^n$ and $\mathbb{Z}^m/2\mathbb{Z}^m \cong \mathbb{Z}_2^m$, so we have $\mathbb{Z}_2^n \cong \mathbb{Z}_2^m$. Thus $2^n = |\mathbb{Z}_2^n| = |\mathbb{Z}_2^m| = 2^m$ so $n = m$.

6.4 Definition: Let G be an additive abelian group. Let $u_1, u_2, \dots, u_\ell \in G$ be distinct and let $U = \{u_1, u_2, \dots, u_\ell\}$. A **linear combination** of elements in U (over \mathbb{Z}) is an element of G of the form

$$a = t_1u_1 + t_2u_2 + \dots + t_\ell u_\ell \text{ for some } t_i \in \mathbb{Z}.$$

The **span** of U (over \mathbb{Z}) is the set of all linear combinations, that is

$$\text{Span}_{\mathbb{Z}}(U) = \langle U \rangle = \{t_1u_1 + t_2u_2 + \dots + t_\ell u_\ell \mid \text{each } t_i \in \mathbb{Z}\}$$

We say that U is **linearly independent** (over \mathbb{Z}) when for all $t_i \in \mathbb{Z}$,

$$\text{if } t_1u_1 + t_2u_2 + \dots + t_\ell u_\ell = 0 \text{ then every } t_i = 0.$$

We say that U is a **basis** for G (over \mathbb{Z}) when U is linearly independent and $\text{Span}_{\mathbb{Z}}(U) = G$. An **ordered basis** for G (over \mathbb{Z}) is an ordered n -tuple (u_1, u_2, \dots, u_n) of distinct elements $u_i \in G$ such that $U = \{u_1, u_2, \dots, u_n\}$ is a basis for G (over \mathbb{Z}). Note that if U is a basis for G over \mathbb{Z} , every element in G can be written uniquely (up to the order of the terms) as a linear combination of elements in U over \mathbb{Z} .

6.5 Example: Let $e_k = (0, \dots, 0, 1, 0, \dots, 0) \in \mathbb{Z}^n$ where the 1 is in the k^{th} position. Then $\{e_1, e_2, \dots, e_n\}$ is a basis, which we call the **standard basis** for \mathbb{Z}^n over \mathbb{Z} .

6.6 Theorem: Let G be an abelian group. Then G is a free abelian group of rank n if and only if G has a basis over \mathbb{Z} with n -elements.

Proof: Suppose that $G \cong \mathbb{Z}^n$ and let $\phi : \mathbb{Z}^n \rightarrow G$ is a group isomorphism. Verify that the set $U = \{\phi(e_1), \phi(e_2), \dots, \phi(e_n)\}$ is a basis for G over \mathbb{Z} . Conversely, suppose that $U = \{u_1, u_2, \dots, u_n\}$ is a basis for G over \mathbb{Z} . Verify that the map $\phi : \mathbb{Z}^n \rightarrow G$ given by

$$\phi(t_1, t_2, \dots, t_n) = (t_1u_1 + t_2u_2 + \dots + t_nu_n)$$

is a group isomorphism.

6.7 Theorem: Let $U = (u_1, u_2, \dots, u_n)$ be an ordered basis over \mathbb{Z} for the free abelian group G . Then we can perform any of the following operations to the elements in the basis to obtain a new ordered basis for G over \mathbb{Z} .

- (1) $u_i \leftrightarrow u_j$: interchange two elements,
- (2) $u_i \mapsto \pm u_i$: multiply an element by ± 1 ,
- (3) $u_i \mapsto u_i + ku_j$: add an integer multiple of one element to another.

Proof: The proof is left as an exercise.

6.8 Theorem: (Subgroups and Quotient Groups of \mathbb{Z}^n) Let G be a free abelian group of rank n . Let $H \leq G$. Then H is a free abelian group of rank r for some $0 \leq r \leq n$ and

$$G/H \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$$

for some $d_i \in \mathbb{Z}^+$ with $d_1 | d_2, d_2 | d_3, \dots, d_{r-1} | d_r$.

Proof: We claim that there exists a basis $\{u_1, u_2, \dots, u_n\}$ for G and there exist r and d_1, d_2, \dots, d_r with $0 \leq r \leq n$ and $d_1 | d_2, d_2 | d_3, \dots, d_{r-1} | d_r$ such that $\{d_1 u_1, d_2 u_2, \dots, d_r u_r\}$ is a basis for H . Once we have proven this claim, it is not hard to check that the map $\phi : G \rightarrow \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$ given by $\phi(t_1 u_1 + \cdots + t_n u_n) = (t_1, \dots, t_n)$ is a surjective group homomorphism with $\text{Ker}(\phi) = H$, so that

$$G/H \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$$

by the First Isomorphism Theorem.

When $n = 1$ so $G \cong \mathbb{Z}$, we have $G = \langle a \rangle = \text{Span}_{\mathbb{Z}}\{a\}$ for some $a \in G$ with $|a| = \infty$, and $H = \langle ka \rangle$ for some $k \geq 0$. If $k = 0$ so $H = \{0\}$ (so the empty set is a basis for H), the claim holds with $u_1 = a$ and $r = 0$. If $k > 0$, the claim holds with $u_1 = a$, $r = 1$, $d_1 = k$.

Let $n \geq 2$ and suppose, inductively, that the claim holds for free abelian groups of rank $n - 1$. Let $G \cong \mathbb{Z}^n$ with $H \leq G$. If $H = \{0\}$ (so the empty set is a basis for H), the claim holds with $r = 0$. Suppose that $H \neq \{0\}$. Let T be the set of all coefficients t_i in all linear combinations $a = t_1 v_1 + t_2 v_2 + \cdots + t_n v_n$ over all elements $a \in H$ and all possible choices of basis $\{v_1, v_2, \dots, v_n\}$ for G . Let $d_1 \in \mathbb{Z}^+$ be the smallest positive integer in T . Choose a basis $\{v_1, v_2, \dots, v_n\}$ for G and an element $a = d_1 v_1 + t_2 v_2 + t_3 v_3 + \cdots + t_n v_n \in H$. Note that $d_1 | t_i$ for all $i \geq 2$ because if we write $t_i = q_i d_1 + r_i$ with $0 \leq r_i < d_i$ then

$$\begin{aligned} a &= d_1 v_1 + (q_2 d_1 + r_2) v_2 + (q_3 d_1 + r_3) v_3 + \cdots + (q_n d_1 + r_n) v_n \\ &= d_1 (v_1 + q_2 v_2 + q_3 v_3 + \cdots + q_n v_n) + r_2 v_2 + r_3 v_3 + \cdots + r_n v_n \end{aligned}$$

and so each $r_i = 0$ by the choice of d_1 since $\{v_1 + \sum q_i v_i, v_2, v_3, \dots, v_n\}$ is a basis for G . Let $u_1 = v_1 + \sum q_i v_i$ so that $\{u_1, v_2, v_3, \dots, v_n\}$ is a basis for G and $a = d_1 u_1 \in H$.

Let $G_0 = \text{Span}\{v_2, v_3, \dots, v_n\}$ and let $H_0 = H \cap G_0$. Let $a \in H$. Since $\{u_1, v_2, \dots, v_n\}$ is a basis for G , we know that a can be written uniquely in the form $a = t_1 u_1 + t_2 v_2 + \cdots + t_n v_n$. Note that we must have $d_1 | t_1$ because if we write $t_1 = q_1 d_1 + r_1$ with $0 \leq r_1 < d_1$ then since $a = (q_1 d_1 + r_1) u_1 + t_2 v_2 + \cdots + t_n v_n \in H$, we have $r_1 u_1 + t_2 v_2 + \cdots + t_n v_n = a - q_1 d_1 u_1 \in H$, and so $r_1 = 0$ by the choice of d_1 . Also note that for $b = a - t_1 u_1 = t_2 v_2 + \cdots + t_n v_n$ we have $b \in \text{Span}\{v_2, \dots, v_n\} = G_0$ and since $d_1 | t_1$ and $d_1 u_1 \in H$ we have $t_1 u_1 \in H$, and so $b \in H \cap G_0 = H_0$. Thus every $a \in H$ can be written uniquely as $a = t_1 u_1 + b$ with $d_1 | t_1$ and $b \in H_0$.

By the induction hypothesis, we can find a basis $\{u_2, u_3, \dots, u_n\}$ for G_0 and we can find r and d_2, d_3, \dots, d_n with $1 \leq r \leq n$ and $d_2 | d_3, d_3 | d_4, \dots, d_{r-1} | d_r$ such that $\{d_2 u_2, \dots, d_r u_r\}$ is a basis for H_0 . Since each $a \in H$ can be written uniquely as $a = t_1 u_1 + b$ with $d_1 | t_1$ and $b \in H_0 = \text{Span}\{d_2 u_2, \dots, d_n u_n\}$, it follows that $\{d_1 u_1, d_2 u_2, \dots, d_n u_n\}$ is a basis for H . Finally, note that we must have $d_1 | d_2$ because if we write $d_2 = q_2 d_1 + r_2$ with $0 \leq r_2 < d_1$ then we have $d_1 u_1 + d_2 u_2 \in H$, so that $d_1 u_1 + (q_2 d_1 + r_2) u_2 \in H$, hence $d_1 (u_1 + q_2 u_2) + r_2 u_2 \in H$ and so $r_2 = 0$ by the choice of d_1 , since $\{u_1 + q_2 u_2, u_2, \dots, u_n\}$ is another basis for G .

6.9 Theorem: (*The Classification of Finite Abelian Groups*) Every finite abelian group is isomorphic to a unique group of the form

$$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_l}$$

for some integer $l \geq 0$ and some integers n_i with $2 \leq n_1, n_1 | n_2, n_2 | n_3, \dots, n_{l-1} | n_l$.

Alternatively, every finite abelian group is isomorphic to a unique group of the form

$$\mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}}$$

for some integer $m \geq 0$ and some primes p_i with $p_1 \leq p_2 \leq \cdots \leq p_m$ and some positive integers k_i with $k_i \leq k_{i+1}$ whenever $p_i = p_{i+1}$.

Proof: First we prove that every finite abelian group is isomorphic to a group of the first form. Let G be a finite additive abelian group, say $|G| = n$ and $G = \{a_1, a_2, \dots, a_n\}$. Define $\phi : \mathbb{Z}^n \rightarrow G$ by $\phi(t_1, t_2, \dots, t_n) = t_1 a_1 + \cdots + t_n a_n$. Then ϕ is a group homomorphism since G is abelian, and ϕ is clearly onto. By the First Isomorphism Theorem we have $G \cong \mathbb{Z}^n / \text{Ker}(\phi)$. By the previous theorem,

$$G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$$

for some integers r and d_1, d_2, \dots, d_r with $0 \leq r \leq n$ and $d_1 | d_2, d_2 | d_3, \dots, d_{r-1} | d_r$. Since G is finite we must have $r = n$. Say $d_1 = d_2 = \cdots = d_k = 1$ and $d_{k+1} > 1$. Then we have

$$G = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_l}$$

as required, by taking $n_i = d_{k+i}$.

Next we describe a bijective correspondence between groups of the first form and groups of the second form. Given a group $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_l}$ of the first form, we can obtain an isomorphic group H of the second form as follows. For each $j = 1, 2, \dots, l$, decompose n_j into its prime factorization $n_j = \prod p_{ji}^{k_{ji}}$, replace the group \mathbb{Z}_{n_j} by the isomorphic group $\prod \mathbb{Z}_{p_{ji}^{k_{ji}}}$, and then let H be the product of all the groups $p_{ji}^{k_{ji}}$ arranged in the required order. For example, for $G = \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{24} \times \mathbb{Z}_{720}$, we have

$$\begin{aligned} G &= \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{24} \times \mathbb{Z}_{720} \\ &\cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times (\mathbb{Z}_4 \times \mathbb{Z}_3) \times (\mathbb{Z}_8 \times \mathbb{Z}_3) \times (\mathbb{Z}_{16} \times \mathbb{Z}_9 \times \mathbb{Z}_5) \\ &\cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_8 \times \mathbb{Z}_{16} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5 = H. \end{aligned}$$

Conversely, given the group $H = \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}}$ of the second form, we can recover the group G of the first form as follows. First rewrite the list of (not necessarily distinct) primes p_1, p_2, \dots, p_m as $q_1, q_1, \dots, q_1, q_2, q_2, \dots, q_2, \dots, q_r, q_r, \dots, q_r$ where the q_i are distinct primes, where say q_i occurs s_i times in the list, and rewrite the list $p_1^{k_1}, \dots, p_m^{k_m}$ in the form $q_1^{k_{1,1}}, \dots, q_1^{k_{1,s_1}}, q_2^{k_{2,1}}, \dots, q_2^{k_{2,s_2}}, \dots, q_r^{k_{r,1}}, \dots, q_r^{k_{r,s_r}}$. Then let $s = \max\{s_1, s_2, \dots, s_r\}$, and replace each of the products $\mathbb{Z}_{q_i^{k_{i,1}}} \times \cdots \times \mathbb{Z}_{q_i^{k_{i,s_i}}}$ by the isomorphic product $\mathbb{Z}_{q_i^{l_{i,1}}} \times \cdots \times \mathbb{Z}_{q_i^{l_{i,s}}}$ where $l_{i,1} = l_{i,2} = \cdots = l_{i,s-s_i} = 0$ and $l_{i,s-s_i+j} = k_{i,j}$ for $j = 1, 2, \dots, s_i$. We then have

$$H = \prod_{i=1}^r \prod_{j=1}^{s_i} \mathbb{Z}_{q_i^{l_{ij}}} \cong \prod_{j=1}^s \prod_{i=1}^r \mathbb{Z}_{q_i^{l_{ij}}} \cong \prod_{j=1}^s \mathbb{Z}_{n_j} = G, \text{ where } n_j = \prod_{i=1}^r q_i^{l_{ij}}.$$

For example, for $H = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_9 \times \mathbb{Z}_{81} \times \mathbb{Z}_5 \times \mathbb{Z}_{25} \times \mathbb{Z}_7$ we have

$$\begin{aligned}
H &= \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_9 \times \mathbb{Z}_{81} \times \mathbb{Z}_5 \times \mathbb{Z}_{25} \times \mathbb{Z}_7 \\
&\cong (\mathbb{Z}_1 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_8) \times (\mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_9 \times \mathbb{Z}_{81}) \\
&\quad \times (\mathbb{Z}_1 \times \mathbb{Z}_1 \times \mathbb{Z}_5 \times \mathbb{Z}_{25}) \times (\mathbb{Z}_1 \times \mathbb{Z}_1 \times \mathbb{Z}_1 \times \mathbb{Z}_7) \\
&\cong (\mathbb{Z}_1 \times \mathbb{Z}_3 \times \mathbb{Z}_1 \times \mathbb{Z}_1) \times (\mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_1 \times \mathbb{Z}_1) \\
&\quad \times (\mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_1) \times (\mathbb{Z}_8 \times \mathbb{Z}_{81} \times \mathbb{Z}_{25} \times \mathbb{Z}_7) \\
&\cong \mathbb{Z}_3 \times \mathbb{Z}_{18} \times \mathbb{Z}_{90} \times \mathbb{Z}_{113400} = G.
\end{aligned}$$

You should convince yourself that the above two procedures give a bijective correspondence between groups of the two forms described in the statement of the theorem.

Finally, we show uniqueness for groups G of the second form. To do this, we shall show that the primes p_i and the exponents k_i are uniquely determined by the isomorphism class of the group G . Suppose that

$$G \cong \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}}$$

where the p_i are prime and each $k_i \in \mathbb{Z}^+$. Let p be a prime number. Let n_k be the number of elements in G whose order divides p^k . Let a_k be the number of indices i such that $p_i = p$ and $k_i = k$. Let b_k be the number of indices i such that $p_i = p$ and $k_i \geq k$. Note that $a_k = b_k - b_{k+1}$. Using the fact that for $x_i \in \mathbb{Z}_{p_i^{k_i}}$ we have $|(x_1, x_2, \dots, x_m)| = \text{lcm}(|x_1|, |x_2|, \dots, |x_m|)$, verify that

$$\begin{aligned}
n_1 &= p^{b_1} \\
n_2 &= p^{a_1} p^{2b_2} \\
n_3 &= p^{a_1} p^{2a_2} p^{3b_3} \\
&\vdots \\
n_k &= p^{a_1} p^{2a_2} p^{3a_3} \cdots p^{(k-1)a_{k-1}} p^{kb_k}
\end{aligned}$$

so we have

$$\begin{aligned}
\frac{n_k}{n_{k-1}} &= \frac{p^{(k-1)a_{k-1}} p^{kb_k}}{p^{(k-1)b_{k-1}}} = \frac{p^{(k-1)a_{k-1}} p^{kb_k}}{p^{(k-1)(a_{k-1}+b_k)}} = p^{b_k}, \text{ and so} \\
p^{a_k} &= p^{b_k - b_{k+1}} = p^{b_k} / p^{b_{k+1}} = \frac{n_k}{n_{k-1}} \bigg/ \frac{n_{k+1}}{n_k} = \frac{n_k^2}{n_{k-1} n_{k+1}}.
\end{aligned}$$

This formula shows that the number of elements of each order in G determines the values of each prime p_i and each exponent k_i .

6.10 Corollary: Let G and H be finite abelian groups. If G and H have the same number of elements of each order then $G \cong H$.

6.11 Corollary: Let $n = \prod p_i^{k_i}$ where the p_i are distinct primes and each $k_i \in \mathbb{Z}^+$. Then the number of distinct abelian groups of order n (up to isomorphism) is equal to $\prod P(k_i)$ where $P(k_i)$ is the number of partitions of k_i .

Proof: The abelian groups of order p^k are the groups $\prod \mathbb{Z}_{p^{j_i}}$ where the j_i partition k .