In this last paragraph of Chapter 2, we determine the structure of finitely generated abelian groups. A complete classification of such groups is given. Complete classification theorems are very rare in mathematics and, in general, they require sophisticated machinery. However, the main theorems in this paragraph are proved by quite elementary methods, chiefly by induction! This is due to the fact that commutativity is a very strong condition.

This paragraph is not needed in the sequel.

28.1 Lemma: Let $G$ be an abelian group. We write $$T(G) := \{ g \in G : o(g) \text{ is finite} \}.$$

1. $T(G)$ is a subgroup of $G$ (called the torsion subgroup of $G$).
2. In $G/T(G)$, every nonidentity element is of infinite order.

**Proof:**

1. Since $o(1) = 1 \in \mathbb{N}$, $1 \in T(G)$ and $T(G) \neq \emptyset$. Suppose now $a,b$ are in $T(G)$, say $o(a) = n$, $o(b) = m$ ($n, m \in \mathbb{N}$). Then $(ab)^{nm} = a^{nm}b^{nm} = 1.1 = 1$, so $o(ab) \leq nm$, thus $ab \in T(G)$; and $o(a^{-1}) = n \in \mathbb{N}$, thus $a^{-1} \in T(G)$. By the subgroup criterion, $T(G) \leq G$.

2. Since $G$ is abelian, we can build the factor group $G/T(G)$. If $T(G)x$ in $G/T(G)$ has finite order, say $n \in \mathbb{N}$, then $(T(G)x)^n = T(G)$, so $T(G)x^n = T(G)$, so $x^n \in T(G)$, so $o(x^n)$ is finite. Let $o(x^n) = m \in \mathbb{N}$. Then $x^{nm} = (x^n)^m = 1$, so $o(x) \leq nm$. Thus $o(x)$ is finite and $x \in T(G)$. It follows that $T(G)x = T(G)$ is the identity element of $G/T(G)$. Hence every nonidentity element of $G/T(G)$ has infinite order.

28.2 Definition: A group $G$ is called a torsion group if every element of $G$ has finite order. A group is said to be without torsion, or torsion-free if every nonidentity element of $G$ has infinite order.
Thus 1 is the only group which is both a torsion group and torsion-free.

Every finite group is a torsion group, but there are also infinite torsion groups, for example $\mathbb{Z}/\mathbb{Z}$.

In view of Lemma 28.1, we are led to investigate two classes of abelian groups: torsion abelian groups and torsion-free abelian groups. When this is done, we will know the structure of $T(G)$ and $G/T(G)$, where $G$ is an abelian group. We must then investigate how $T(G)$ and $G/T(G)$ are combined to build $G$.

We cannot expect to carry out this ambitious program without imposing additional conditions on $G$. We will assume that $G$ is finitely generated (Definition 24.4). Under this assumption, $T(G)$ turns out to be a finite group (Theorem 28.15). The study of finite abelian groups reduces to the study of finite abelian $p$-groups, $p$ being a prime number, whose structures are described in Theorem 28.10. After that, we turn our attention to torsion-free abelian groups (Theorem 28.13). The next step in our program is to put the pieces $T(G)$ and $G/T(G)$ together in the appropriate way to form $G$. The appropriate way proves to be the simplest way: $G$ is isomorphic to the direct product of $T(G)$ and $G/T(G)$. The structure of $G$ will be completely determined by a set of integers.

28.3 Definition: Let $G$ be an abelian group and let $S = \{g_1, g_2, \ldots, g_r\}$ be a finite, nonempty subset of $G$. If, for any integers $a_1, a_2, \ldots, a_r$, the relation $g_1^{a_1}g_2^{a_2}\ldots g_r^{a_r} = 1$ implies that $g_1^{a_1} = g_2^{a_2} = \cdots = g_r^{a_r} = 1$, then $S$ is said to be independent. If $S$ is independent and generates $G$, and if $1 \notin S$, then $S$ is called a basis of $G$.

In the following lemma, we will prove, among other things, that $S = \{g_1, g_2, \ldots, g_r\}$ is a basis of $G$ if and only if $G$ is the direct product of the cyclic groups $\langle g_1 \rangle, \langle g_2 \rangle, \ldots, \langle g_r \rangle$. Lemma 28.4(2) is of especial importance: it states that a finitely generated abelian torsion group is in fact a finite group.
28.4 Lemma: Let $G$ be an abelian group and $g_1, g_2, \ldots, g_r$ be finitely many elements of $G$, not necessarily distinct ($r \geq 1$). Let $B \leq G$.

1. $\langle g_1 g_2 \ldots g_r \rangle = \langle g_1 \rangle \langle g_2 \rangle \ldots \langle g_r \rangle$.
2. If each $g_i$ has finite order, then $|\langle g_1 g_2 \ldots g_r \rangle| = o(g_1)o(g_2)\ldots o(g_r)$.
3. If $G = \langle g_1 g_2 \ldots g_r \rangle$ and $\varphi : G \to A$ is a homomorphism onto $A$, then $A = \langle g_1, g_2, \varphi, \ldots, g_r \varphi \rangle$.
4. If $G = \langle g_1 g_2 \ldots g_r \rangle$, then $G/B = \langle B g_1 B g_2 \ldots B g_r \rangle$.
5. If $G/B = \langle B g_1 B g_2 \ldots B g_r \rangle$, then $G = B \langle g_1 g_2 \ldots g_r \rangle$. If, in addition, $b_1, \ldots, b_s \in B$ and $B = \langle b_1, \ldots, b_s \rangle$, then $G = \langle b_1, \ldots, b_s g_1 g_2 \ldots g_r \rangle$.
6. If $B = \langle g_1 \rangle$ and $G/B = \langle B g_2 \ldots B g_r \rangle$, then $G = \langle g_1 g_2 \ldots g_r \rangle$.
7. $\{g_1 g_2 \ldots g_r\}$ is an independent subset of $G$ and $G = \langle g_1 g_2 \ldots g_r \rangle$ if and only if $G = \langle g_1 \rangle \times \langle g_2 \rangle \times \ldots \times \langle g_r \rangle$. In particular, in case $g_1 g_2 \ldots g_r$ are all distinct from 1, the subset $\{g_1 g_2 \ldots g_r\}$ is a basis of $G$ if and only if $G = \langle g_1 \rangle \times \langle g_2 \rangle \times \ldots \times \langle g_r \rangle$.

Proof: (1) Certainly $\{g_1 g_2 \ldots g_r\} \subseteq \langle g_1 \rangle \langle g_2 \rangle \ldots \langle g_r \rangle \leq G$ by repeated use of Lemma 19.4(3), and so $\langle g_1 g_2 \ldots g_r \rangle \leq \langle g_1 \rangle \langle g_2 \rangle \ldots \langle g_r \rangle$ by the definition of $\langle g_1 g_2 \ldots g_r \rangle$. Also, any element of $\langle g_1 \rangle \langle g_2 \rangle \ldots \langle g_r \rangle$, necessarily of the form $g_1 m_1 g_2 m_2 \ldots g_r m_r$ with suitable integers $m_1, m_2, \ldots, m_r$, is in $\langle g_1 g_2 \ldots g_r \rangle$ by Lemma 24.2 and so $\langle g_1 \rangle \langle g_2 \rangle \ldots \langle g_r \rangle \leq \langle g_1 g_2 \ldots g_r \rangle$. Hence $\langle g_1 g_2 \ldots g_r \rangle = \langle g_1 \rangle \langle g_2 \rangle \ldots \langle g_r \rangle$.

(2) Suppose $o(g_i) = k_i \in \mathbb{N}$ for each $i = 1, 2, \ldots, r$. If $g \in \langle g_1 g_2 \ldots g_r \rangle$, then, by part (1), $g = g_1 m_1 g_2 m_2 \ldots g_r m_r$ with suitable integers $m_i$. Dividing $m_i$ by $k_i$, we may write $m_i = k_i q_i + t_i$ where $q_i, t_i \in \mathbb{Z}$ and $0 \leq t_i < k_i$. Then $g_1 m_i = (g_1 g_i)^{k_i} g_i^{t_i} = g_i^{t_i}$ and $g = g_1^{q_1} g_2^{q_2} \ldots g_r^{q_r}$. Thus

$$\langle g_1 g_2 \ldots g_r \rangle \subseteq \langle g_1^{q_1} g_2^{q_2} \ldots g_r^{q_r} : 0 \leq t_i < k_i \text{ for all } i = 1, 2, \ldots, r \rangle$$

and

$$|\langle g_1 g_2 \ldots g_r \rangle| \leq k_1 k_2 \ldots k_r.$$

(3) If $a \in A$, then $a = g \varphi$ for some $g \in G$ since $\varphi$ is onto and $g = g_1 m_1 g_2 m_2 \ldots g_r m_r$ with suitable integers $m_i$ since $G = \langle g_1 g_2 \ldots g_r \rangle$. Thus

$$a = g \varphi = (g_1 m_1 g_2 m_2 \ldots g_r m_r) \varphi = (g_1 \varphi)^{m_1} (g_2 \varphi)^{m_2} \ldots (g_r \varphi)^{m_r} \in \langle g_1 \varphi, g_2 \varphi, \ldots, g_r \varphi \rangle$$

and $A \subseteq \langle g_1 \varphi, g_2 \varphi, \ldots, g_r \varphi \rangle$.

(4) This follows from part (3) when we take $A$ to be $G/B$ and $\varphi$ to be the natural homomorphism $\nu : G \to G/B$.
(5) Suppose $G/B = \langle B g_1, B g_2, \ldots, B g_r \rangle$. Let $g \in G$. Then $B g \in G/B$ and, by part (1) with $G/B$ in place of $G$ and $B g_i$ in place of $g_i$, we have

$$B g = (B g_1)^{m_1}(B g_2)^{m_2} \cdots (B g_r)^{m_r} = B g_1^{m_1}g_2^{m_2} \cdots g_r^{m_r}$$

for some integers $m_i$.

Hence $g = b g_1^{m_1}g_2^{m_2} \cdots g_r^{m_r}$ for some $b \in B$ and $g \in B < g_1, g_2, \ldots, g_r >$. So $G = B < g_1, g_2, \ldots, g_r >$. If, in addition, $B = \langle b_1, \ldots, b_s \rangle$, then

$$G = \langle b_1, \ldots, b_s \rangle < g_1, g_2, \ldots, g_r > = \langle b_1, \ldots, b_s \rangle g_1 < g_2, \ldots, g_r >$$

= $\langle b_1, \ldots, b_s g_1 g_2 \ldots g_r >$.

(6) This follows from part (5) with a slight change in notation.

(7) Since $G$ is abelian, $G = \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_r \rangle$ if and only if every element of $G$ can be expressed in the form $u_1 u_2 \cdots u_r$, where $u_i \in \langle g_i \rangle$, in a unique manner (Theorem 22.15).

Every element of $G$ has at least one such representation if and only if $G = \langle g_1, g_2, \ldots, g_r \rangle$, that is, if and only if $G = \langle g_1, g_2, \ldots, g_r \rangle$.

We want to show that every element of $G$ has at most one such representation if and only if $\{g_1, g_2, \ldots, g_r\}$ is independent. Equivalently, we will prove that there is an element in $G$ with two different representations if and only if $\{g_1, g_2, \ldots, g_r\}$ is not independent. Indeed, there is an element in $G$ with two different representations if and only if $g_1^{m_1}g_2^{m_2} \cdots g_r^{m_r} = g_1^{m_1}g_2^{m_2} \cdots g_r^{m_r}$ for some integers such that $g_i^{m_i} \neq g_i^{n_i}$ for at least one $i \in \{1, 2, \ldots, r\}$. The latter condition holds if and only if

$$g_1^{m_1 n_1}g_2^{m_2 n_2} \cdots g_r^{m_r n_r} = 1,$$

where not all of $g_1^{m_1 n_1}, g_2^{m_2 n_2}, \ldots, g_r^{m_r n_r}$ are equal to 1, that is, if and only if $\{g_1, g_2, \ldots, g_r\}$ is not independent. □

28.5 Lemma: Let $G$ be a group and $g_1, g_2, \ldots, g_r$ elements of $G$. Let $B = \langle g_i \rangle$ and suppose $o(g_i) = o(B g_i)$ for $i = 2, \ldots, r$.

(1) If $\{B g_2, \ldots, B g_r\}$ is an independent subset of $G/B$, then $\{g_1, g_2, \ldots, g_r\}$ is an independent subset of $G$.

(2) Assume $g_1, g_2, \ldots, g_r$ are all distinct from 1. If $G/B = \langle B g_2 \rangle \times \cdots \times \langle B g_r \rangle$, then $G = \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_r \rangle$. 305
Proof: (1) If \( m_1, m_2, \ldots, m_r \) are integers such that
\[
g_1^{m_1} g_2^{m_2} \ldots g_r^{m_r} = 1,
\]
(\( * \))
then
\[
B = \prod_{i=2}^{r} B g_i^{m_i} = (B g_1)^{m_1} (B g_2)^{m_2} \ldots (B g_r)^{m_r},
\]
so \((B g_2)^{m_2} = \cdots = (B g_r)^{m_r} = B\) since \( \{ B g_2, \ldots, B g_r \} \) is independent. Thus \( o(g_i) = o(B g_i) \) divides \( m_i \) in case \( o(g_i) \) is finite and \( m_i = 0 \) in case \( o(g_i) = o(B g_i) \) is infinite \((i = 2, \ldots, r)\). In both cases \( g_i^{m_i} = 1 \) \((i = 2, \ldots, r)\), and, because of \((*)\), \( g_1^{m_1} = 1 \) as well. Hence \( \{ g_1, g_2, \ldots, g_r \} \) is independent.

(2) If \( G/B = \langle B g_2 \rangle \times \ldots \times \langle B g_r \rangle \), then \( G/B = \langle B g_2 \rangle \ldots \langle B g_r \rangle \) and
\[
\begin{align*}
\{ B g_2, \ldots, B g_r \} & \text{ is independent} \quad \text{(Lemma 28.4(7))}, \\
G = \langle g_1 g_2 \ldots g_r \rangle & \quad \text{(Lemma 28.4(6))}, \\
\{ g_1, g_2, \ldots, g_r \} & \text{ is independent} \quad \text{(Lemma 28.5(1))}, \\
G = \langle g_1 \rangle \times \langle g_2 \rangle \times \ldots \times \langle g_r \rangle & \quad \text{(Lemma 28.4(7))}. \quad \Box
\end{align*}
\]

We now examine the structure of finite abelian groups. A finite abelian group is a direct product of its Sylow \( p \)-subgroups. This follows immediately if the existence of Sylow \( p \)-subgroups is granted. In order to keep this paragraph independent of §26, we give another proof, from which the existence of Sylow \( p \)-subgroups (of finite abelian groups) follows as a bonus. We need a lemma.

28.6 Lemma: Let \( A \) be a finite abelian group and let \( q \) be a prime number. If \( q \) divides \( |A| \), then \( A \) has an element of order \( q \).

Proof: Let \( |A| = n \) and let \( a_1, a_2, \ldots, a_n \) be the \( n \) elements of \( A \). We write \( m_i = o(a_i) \) for \( i = 1, 2, \ldots, n \). We list all products
\[
a_1^{k_1} a_2^{k_2} \ldots a_n^{k_n}
\]
where each \( k_i \) runs through \( 0, 1, \ldots, m_i - 1 \). Our list has thus \( m_1 m_2 \ldots m_n \) entries. Every element of \( A \) appears in our list. Two entries \( a_1^{k_1} a_2^{k_2} \ldots a_n^{k_n} \) and \( a_1^{s_1} a_2^{s_2} \ldots a_n^{s_n} \) are equal if and only if the entry \( a_1^{\delta_1} a_2^{\delta_2} \ldots a_n^{\delta_n} \), where \( \delta_i \)

306
is such that \(0 \leq r_i \leq m_i - 1\) and \(k_i - s_i \equiv r_i \pmod{m_i}\), is equal to the identity element of \(A\). Thus any element of \(A\) appears in our list as many times as 1 does, say \(t\) times. The number of entries is therefore \(m_1m_2\ldots m_n = nt\). Since \(q\) divides \(n\), we see \(q|m_1m_2\ldots m_n\) and \(q\) divides one of the numbers \(m_1, m_2, \ldots, m_n\) (Lemma 5.16), say \(q|m_1\). Let us put \(m_1 = qh, h \in \mathbb{N}\). By Lemma 11.9(2), \(a_1^h\) has order

\[
o(a_1^h) = o(a_1)/(o(a_1), h) = m_1/(m_1, h) = \frac{qh}{(qh, h)} = qh/h = q. \]

\[\square\]

\[28.7 \textbf{Theorem:} \text{ Let } G \text{ be a finite abelian group and let } |G| = p_1^{a_1}p_2^{a_2}\ldots p_s^{a_s}\text{ be the canonical decomposition of } |G| \text{ into prime numbers } (a_i > 0).\]

\[1) \text{ For } n \in \mathbb{N}, \text{ we put } G[n] := \{g \in G : g^n = 1\}. \text{ Then } G[n] \leq G \text{ for any } n \in \mathbb{N}.\]

\[2) \text{ Let } G_i = G[p_i^{a_i}] \text{ for } i = 1, 2, \ldots, s. \text{ Then } G = G_1 \times G_2 \times \ldots \times G_s.\]

\[3) |G| = p_i^{a_i} \text{ (and } G_i \text{ is called a Sylow } p_i\text{-subgroup of } G).\]

\[4) \text{ Let } H \text{ be an abelian group with } |H| = |G| \text{ and } H_i = H[p_i^{a_i}] \text{ (} i = 1, 2, \ldots, s). \text{ Then } G \cong H \text{ if and only if } G_i \cong H_i \text{ for all } i = 1, 2, \ldots, s.\]

\[\textbf{Proof:} \ (1) \text{ Let } n \in \mathbb{N}. \text{ From } 1^n = 1, \text{ we get } 1 \in G[n], \text{ so } G[n] \neq \emptyset. \text{ We use our subgroup criterion.} \]

\[(i) \text{ If } x, y \in G[n], \text{ then } x^n = 1 = y^n \text{ and } (xy)^n = x^n y^n = 1.1 = 1 \text{ and so } xy \in G[n].\]

\[(ii) \text{ If } x \in G[n] \text{ then } x^n = 1 \text{ and } (x^{-1})^n = (x^n)^{-1} = 1^{-1} = 1 \text{ and so } x^{-1} \in G[n].\]

Thus \(G[n] \leq G.\)

\[2) \text{ We must show that } G = G_1G_2\ldots G_s \text{ and } G_1\ldots G_{j-1} \cap G_j = 1 \text{ for all } j = 2, \ldots, s \text{ (Theorem 22.12). We put } |G|/p_i^{a_i} = m_i \text{ (} i = 1, 2, \ldots, s). \text{ Here the integers } m_1, m_2, \ldots, m_s \text{ are relatively prime and there are integers } u_1, u_2, \ldots, u_s \text{ such that } u_1m_1 + u_2m_2 + \cdots + u_sm_s = 1.\]

We now show \(G = G_1G_2\ldots G_s\). \text{ If } g \in G, \text{ then } g = g^{u_1m_1}g^{u_2m_2}\ldots g^{u_sm_s}, \text{ with } g^{u_im_i} \in G_i \text{ since } (g^{u_im_i})^{p_i^{a_i}} = g^{u_i}[1] = 1 \text{ (} i = 1, 2, \ldots, s). \text{ Thus } G \subseteq G_1G_2\ldots G_s \text{ and } G = G_1G_2\ldots G_s.\]

Secondly, let \(j \in \{2, \ldots, s\} \text{ and } g \in G_{1}\ldots G_{j-1} \cap G_j \text{ then } g = g^{1}\ldots g_{j-1}, \text{ where } g_1^{p_1^{a_1}} = \cdots = g_j^{p_j^{a_j}} = 1, \text{ therefore } g^{p_1^{a_1}p_j^{a_j}} = 1 \text{ and } o(g) | p_1^{a_1}p_j^{a_j}. \text{ On the other hand, } g \in G_j \text{ so } g^{p_j^{a_j}} = 1 \text{ and } o(g) | p_j^{a_j}. \text{ Thus } o(g) = 1 \text{ and } g = 1. \text{ Thus } G_{1}\ldots G_{j-1} \cap G_j \subseteq 1 \text{ and } G_{1}\ldots G_{j-1} \cap G_j = 1. \text{ This proves } G = G_1 \times G_2 \times \ldots \times G_s.\]

\[307\]
(3) By the very definition of \(G_i = G[p_i^{a_i}]\), the order of any element in \(G_i\) is a divisor of \(p_i^{a_i}\). Then, by Lemma 28.6, \(|G_i|\) is not divisible by any prime number \(q\) distinct from \(p_i\). Thus \(|G_i| = p_i^{b_i}\) for some \(b_i, 0 \leq b_i < a_i\). From \(p_1^{b_1}p_2^{b_2} \ldots p_s^{b_s} = |G_i|\) \(|G_2| \ldots |G_s| = |G_i| \times G_2 \times \ldots \times G_s| = p_1^{a_1}p_2^{a_2} \ldots p_s^{a_s}\), we get \(p_i^{b_i} = |G_i| = p_i^{a_i}\) for all \(i = 1, 2, \ldots, s\).

(4) Let \(\varphi: G \to H\) be an isomorphism. For any \(g \in G\), we have \(g^{p_i^{a_i}} = 1\), so \((g\varphi)^{p_i^{a_i}} = (g^{p_i^{a_i}})\varphi = 1\varphi = 1\). Thus \(g\varphi \in H_i\) and \(G_i\varphi \leq H_i\). Also, if \(h \in H_i\), then \(h = g\varphi\) for some \(g \in G\) and \((g\varphi)^{p_i^{a_i}} = (g\varphi)^{p_i^{a_i}} = h^{p_i^{a_i}} = 1\). Thus \(g^{p_i^{a_i}} \in \text{Ker } \varphi = 1\), so \(g^{p_i^{a_i}} = 1\), so \(g \in G_i\) and \(h = g\varphi \in G_i\varphi\). Hence \(H_i \leq G_i\varphi\). We obtain \(G_i\varphi = H_i\). Consequently, \(\varphi_i : G_i \to H_i\) is an isomorphism and \(G_i \cong H_i\) for all \(i = 1, 2, \ldots, s\).

Conversely, assume \(|G| = |H|\) and \(G_i \cong H_i\) for all \(i = 1, 2, \ldots, s\). From part (2), we get \(G = G_1 \times G_2 \times \ldots \times G_s\) and \(H = H_1 \times H_2 \times \ldots \times H_s\) and Lemma 22.16 gives \(G \cong H\).

According to Theorem 28.7, the structure of a finite abelian group is completely determined by the structure of its Sylow subgroups. Consequently, we focus our attention on finite abelian \(p\)-groups. After two preparatory lemmas, the structure of finite abelian \(p\)-groups will be described in Theorem 28.10.

### 28.8 Lemma

Let \(G\) be an abelian group and \(g_1, g_2, \ldots, g_r\) elements of \(G\). Let \(n \in \mathbb{N}\). We write \(G^n = \{g^n : g \in G\}\).

1. \(G^n \leq G\).
2. If \(G = \langle g_1, g_2, \ldots, g_r \rangle\), then \(G^n = \langle g_1^n, g_2^n, \ldots, g_r^n \rangle\).
3. If \(G = \langle g_1 \rangle \times \langle g_2 \rangle \times \ldots \times \langle g_r \rangle\), then \(G^n = \langle g_1^n \rangle \times \langle g_2^n \rangle \times \ldots \times \langle g_r^n \rangle\) and \(G/G^n \cong \langle g_1 \rangle/\langle g_1^n \rangle \times \langle g_2 \rangle/\langle g_2^n \rangle \times \ldots \times \langle g_r \rangle/\langle g_r^n \rangle\).
4. Let \(H\) be an abelian group. If \(G \cong H\), then \(G^n \cong H^n\) and \(G/G^n \cong H/H^n\).

**Proof:** (1) and (2) Since \((ab)^n = a^n b^n\) for all \(a, b \in G\), the mapping

\[
\psi : G \to G^n
\]

\[
a \to a^n
\]

308
is a homomorphism onto $G^n$. So $G^n = Im \varphi \leq G$ by Theorem 20.6. Also, if $G = \langle g_1, g_2, \ldots, g_r \rangle$, then $G^n = \langle g_1^n, g_2^n, \ldots, g_r^n \rangle$ by Lemma 28.4(3).

(3) If $G = \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_r \rangle$, then $G = \langle g_1, g_2, \ldots, g_r \rangle$ and $\{g_1, g_2, \ldots, g_r\}$ is independent (Lemma 28.4(7)). Then $G^n = \langle g_1^n, g_2^n, \ldots, g_r^n \rangle$ by part (2). Moreover, $\{g_1^n, g_2^n, \ldots, g_r^n\}$ is independent, for if $m_1, m_2, \ldots, m_r$ are integers and $(g_1^n)^{m_1}(g_2^n)^{m_2}\cdots(g_r^n)^{m_r} = 1$, then $g_1^{nm_1}g_2^{nm_2}\cdots g_r^{nm_r} = 1$, so $(g_i^n)^{m_i} = g_i^{nm_i} = 1$ because $\{g_1^n, g_2^n, \ldots, g_r^n\}$ is independent. From Lemma 28.4(7), we obtain that $G^n = \langle g_1^n \rangle \times \langle g_2^n \rangle \times \cdots \times \langle g_r^n \rangle$. The second assertion follows from Lemma 22.17.

(4) Assume $\varphi : G \to H$ is an isomorphism. For any $g \in G$, $g^n\varphi = (g\varphi)^n \in H^n$, and therefore $G^n\varphi \leq H^n$. Also, if $h_1 \in H^n$, then $h_1 = h^n$ for some $h \in H$ and $h = g\varphi$ for some $g \in G$, so $h_1 = h^n = (g\varphi)^n = g^n\varphi \in G^n\varphi$ and thus $H^n \leq G^n\varphi$. Hence $H^n = G^n\varphi$ and $\varphi|_G : G^n \to H^n$ is an isomorphism: $G^n \cong H^n$. By Theorem 21.1(7), we have also $G/G^n \cong G_\varphi/G^n\varphi = H/H^n$. \hfill \Box

28.9 Lemma: Let $p$ be a prime number and $G$ a finite abelian $p$-group. Let $g_1 \in G$ be such that $o(g_1) \geq o(a)$ for all $a \in G$ and put $B = \langle g_1 \rangle$. If $Bx \in G/B$ and $o(Bx) = p^m$, then $Bx = Bg$ for some $g \in G$ satisfying $o(g) = p^m$.

Proof: Let $o(g_1) = p^s$, $o(Bx) = p^m$ and $o(x) = p^t$. Since $(Bx)^{p^m} = Bx^{p^m} = B = B$, we have $p^m | p^t$ by Lemma 11.6. Also, $Bx^{p^m} = (Bx)^{p^m} = B$, thus $x^{p^m} \in B = \langle g_1 \rangle$ and $x^{p^m} = g_1^n$ for some $n \in \mathbb{Z}$ with $1 \leq n \leq p^s$. We write $n = p^kt$, where $k$ and $t$ are integers, $k \geq 0$ and $(p,t) = 1$. Then $p^k \leq p^kt = n \leq p^s$ and, by Lemma 11.9,

$$p^{u-m} = p^u/p^m = p^{u-1}(p^m, p^m) = o(x)/(o(x), p^m) = o(x^{p^m}) = o(g_1^n) = o(g_1^{p^kt}) = o(g_1)/(o(g_1), p^k t) = p^s/(p^s, t p^k) = p^s/p^k = p^{s-k}$$

So $p^{s+m-k} = p^u = o(x) \leq o(g_1) = p^s$ by hypothesis and $m \leq k$.

We put $z = g_1^{p^km}$ and $g = z^{-1}x$. Then $z \in \langle g_1 \rangle = B$ and $Bg = Bx$ (Lemma 10.2(5)). From $x^{p^m} = g_1^n = g_1^{p^km} = (g_1^{p^km})^{p^m} = z^{p^m}$,

$$g^{p^m} = (z^{-1}x)^{p^m} = (z^{p^m})^{-1}x^{p^m} = 1,$$

we obtain $o(g)|p^m$. Also $p^m = o(Bx) = o(Bg) \leq o(g)$. Thus $o(g) = p^m$. This completes the proof. \hfill \Box

309
We can now describe finite abelian groups.

28.10 Theorem: (1) Let $p$ be a prime number and let $G$ be a nontrivial finite abelian $p$-group. Then $G$ has a basis, that is, there are elements $g_1, g_2, \ldots, g_r$ in $G \setminus \{1\}$ such that

$$G = \langle g_1 \rangle \times \langle g_2 \rangle \times \ldots \times \langle g_r \rangle.$$ 

(2) The number of elements in a basis of $G$, as well as the orders of the elements in a basis of $G$, are uniquely determined by $G$. More precisely, let $\{g_1, g_2, \ldots, g_r\}$ and $\{h_1, h_2, \ldots, h_s\}$ be bases of $G$, let $o(g_i) = p^{m_i} (i = 1, 2, \ldots, r)$ and $o(h_j) = p^{n_j} (j = 1, 2, \ldots, s)$, and suppose the notation is so chosen that $m_1 \geq m_2 \geq \ldots \geq m_r > 0$ and $n_1 \geq n_2 \geq \ldots \geq n_s > 0$. Then $r = s$ and the $r$-tuple $(p^{m_1}, p^{m_2}, \ldots, p^{m_r})$ is equal to the $s$-tuple $(p^{n_1}, p^{n_2}, \ldots, p^{n_s})$. The $r$-tuple $(p^{m_1}, p^{m_2}, \ldots, p^{m_r})$ is called the type of $G$.

(3) Let $H$ be a nontrivial finite abelian $p$-group. Then $G \cong H$ if and only if $G$ and $H$ have the same type.

Proof: (1) We make induction on $u$, where $|G| = p^u$. If $u = 1$, then $|G| = p$, so $G$ is cyclic (Theorem 11.13) and the claim is true. Assume now $G$ is a finite abelian $p$-group, $|G| \geq p^2$ and assume that, whenever $G_1$ is a finite abelian $p$-group with $1 < |G_1| < |G|$, then $G_1$ is a direct product of certain nontrivial cyclic subgroups.

We choose an element $g_1$ of $G$ such that $o(g_1) \geq o(a)$ for all $a \in G$ and put $\langle g_1 \rangle = B$. Since $G \neq 1$, we have $B \neq 1$. If $G = B = \langle g_1 \rangle$, the claim is established, so we suppose $B < G$. Then $G/B$ is a finite abelian $p$-group with $1 < |G/B| < |G|$. By induction, there are elements $Bx_2, \ldots, Bx_r$ of $G/B$, distinct from $B$, such that

$$G/B = \langle Bx_2 \rangle \times \ldots \times \langle Bx_r \rangle.$$ 

Let us put $o(Bx_i) = p^{m_i}$ for $i = 2, \ldots, r$. Using Lemma 28.9, we find $g_i \in G$ such that $Bx_i =Bg_i$ and $o(g_i) = p^{m_i} (i = 2, \ldots, r)$. Let us write $o(g_1) = p^{m_1}$. Then $G/B = \langle Bg_2 \rangle \times \ldots \times \langle Bg_r \rangle$ and, by Lemma 28.5(2),

$$G = \langle g_1 \rangle \times \langle g_2 \rangle \times \ldots \times \langle g_r \rangle,$$

where $g_2, \ldots, g_r$ are distinct from 1 since $Bg_2, \ldots,Bg_r$ are distinct from $B$ and $g_1$ is distinct from 1 since $o(g_1) \geq o(a)$ for all $a \in G$ and $G \neq 1$. This completes the proof of part (1).
Thus there are elements in \( A \) of order \( 1, 2, \ldots \). Thus, \( G \) is a finite abelian \( p \)-group (arising from different bases) are equal.

Let \( G \) and \( H \) be nontrivial finite abelian \( p \)-groups, let \( (p^{m_1}, p^{m_2}, \ldots, p^{m_r}) \) be a type of \( G \), arising from a basis \( \{g_1, g_2, \ldots, g_r\} \) of \( G \) and let \( (p^{n_1}, p^{n_2}, \ldots, p^{n_s}) \) be a type of \( H \), arising from a basis \( \{h_1, h_2, \ldots, h_s\} \) of \( H \).

If \( r = s \) and \( (p^{m_1}, p^{m_2}, \ldots, p^{m_r}) = (p^{n_1}, p^{n_2}, \ldots, p^{n_s}) \), then \( \langle g_1 \rangle \cong \langle p^{m_1} \rangle \cong \langle h_1 \rangle \) for \( i = 1, 2, \ldots, r \) and \( G = \langle g_1 \rangle \times \langle g_2 \rangle \times \ldots \times \langle g_r \rangle \cong \langle h_1 \rangle \times \langle h_2 \rangle \times \ldots \times \langle h_s \rangle = H \) (Lemma 22.16). This proves the "if" part of (3).

Now the "only if" part of (3), which includes (2) as a particular case (when \( G = H \)): we will prove that \( G \cong H \) implies \( r = s \) and \( (p^{m_1}, p^{m_2}, \ldots, p^{m_r}) = (p^{n_1}, p^{n_2}, \ldots, p^{n_s}) \).

Suppose \( G \cong H \). We make induction on \( u \), where \( \mid G \mid = p^u \). If \( u = 1 \), then \( \mid G \mid = p = \mid H \mid \), so \( G \) and \( H \) are both cyclic, hence \( G = \langle g_1 \rangle \) and \( H = \langle h_1 \rangle \). Thus \( r = 1 = s \) and \( p^{m_1} = o(g_1) = p = o(h_1) = p^{n_1} \). The claim is therefore established when \( u = 1 \). Now suppose \( \mid G \mid \geq p^2 \) and suppose inductively that, if \( G_1 \) and \( H_1 \) are isomorphic finite abelian \( p \)-groups with \( 1 \leq \mid G_1 \mid \leq \mid G \) and if \( (p^{a_1}, p^{a_2}, \ldots, p^{a_r}) \) is a type of \( G_1 \) and \( (p^{b_1}, p^{b_2}, \ldots, p^{b_s}) \) is a type of \( H_1 \), then \( r = s \) and \( (p^{a_1}, p^{a_2}, \ldots, p^{a_r}) = (p^{b_1}, p^{b_2}, \ldots, p^{b_s}) \). We distinguish two cases: the case when \( G^p = 1 \) and the case \( G^p \neq 1 \).

In case \( G^p = 1 \), we have \( g^p = 1 \) for all \( g \in G \), in particular \( p^{m_i} = o(g^i) = p \) for all \( i = 1, 2, \ldots, r \). Also \( H^p = 1 \) (Lemma 28.8(4)) and \( p^{n_j} = o(h_j) = p \) for all \( j = 1, 2, \ldots, s \). Hence \( p^r = \langle g_1 \rangle \times \langle g_2 \rangle \times \ldots \times \langle g_r \rangle = \mid G \mid = \mid H \mid = \langle h_1 \rangle \times \langle h_2 \rangle \times \ldots \times \langle h_s \rangle = p^s \), so \( r = s \) and \( (p^{m_1}, p^{m_2}, \ldots, p^{m_r}) = (p, p, \ldots, p) = (p^{n_1}, p^{n_2}, \ldots, p^{n_s}) \), as claimed.

Suppose now \( G^p \neq 1 \). Then \( H^p \neq 1 \). Thus there are elements in \( G \) and \( H \) of order \( > p \), so \( p^{m_i} > p \) and \( p^{n_j} > p \). Assume \( k \) is the greatest index in \{1, 2, \ldots, r\} with \( p^{m_k} > p \), so that (when \( k < r \)) \( p^{m_{k+1}} = \cdots = p^{m_r} = p \). Let the index \( l \in \{1, 2, \ldots, s\} \) have a similar meaning for the group \( H \). Then

\[
(p^{m_1}, p^{m_2}, \ldots, p^{m_r}) = (p^{n_1}, \ldots, p^{n_k}, p, \ldots, p)_{r-k \text{ times}} \tag{†}
\]
\[(p^{n_1}, p^{n_2}, \ldots, p^{n_r}) = (p^{m_1}, \ldots, p^{n_1}p, \ldots, p), \quad (\dagger\dagger)\]

it being understood that the entries \(p\) should be deleted when \(k = r\) or \(s = l\). By Lemma 28.8(3),

\[
G^p = \langle g_1^p \rangle \times \langle g_2^p \rangle \times \ldots \times \langle g_r^p \rangle = \langle g_1^p \rangle \times \ldots \times \langle g_k^p \rangle \times \langle 1 \rangle \times \ldots \times \langle 1 \rangle_{r-k \times \text{times}}
\]

with \(o(g_i^p) = p^{m_i-1} > 1\) for \(i = 1, \ldots, k\). Hence \(\{g_1^p, \ldots, g_k^p\}\) is a basis and

\((p^{m_1-1}, \ldots, p^{m_k-1})\) is a type of \(G^p\). In the same way, \((p^{n_1-1}, \ldots, p^{n_r-1})\) is a type of \(H^p\). Here \(G^p\) is an abelian \(p\)-group with \(1 < |G^p| = p^{(m_1-1)n} \cdots + (m_k-1) < p^{m_1+m_2+\cdots+m_r} = |G|\). Since \(G^p \cong H^p\) by Lemma 28.8(4), our inductive hypothesis gives

\[k = l \quad \text{and} \quad (p^{m_1-1}, \ldots, p^{m_k-1}) = (p^{n_1-1}, \ldots, p^{n_r-1}).\]

Then \(p^{m_i} = p^{n_i}\) for \(i = 1, \ldots, k\). From

\[p^{m_1+\cdots+m_k}p^{r-k} = |G| = |H| = p^{n_1+\cdots+n_r}p^{s-l} = p^{m_1+\cdots+m_n}p^{s-l}\]

we get \(r-k = s-l = s-k\). Thus \(r = s\) and a glance at \((\dagger)\), \((\dagger\dagger)\) shows

\[(p^{m_1}, p^{m_2}, \ldots, p^{m_r}) = (p^{n_1}, p^{n_2}, \ldots, p^{n_r}).\]

This completes the proof. \(\square\)

**28.11 Examples:** (a) We find all abelian groups of order \(p^5\), where \(p\) is a prime number. An abelian group \(A\) of order \(p^5\) is determined by its type \((p^{m_1}, \ldots, p^{m_r})\), where of course \(p^{m_1+\cdots+m_r} = |A| = p^5\). Since \(m_i > 0\) and \(m_1 + \cdots + m_r = 5\), the only possible types are

\[(p^5), (p^4, p), (p^3, p^2), (p^3, p, p), (p^2, p^2, p), (p^2, p, p, p), (p, p, p, p, p)\]

and any abelian group of order \(p^5\) is isomorphic to one of

\[
C_{p^5}, \quad C_{p^4} \times C_p, \quad C_{p^3} \times C_{p^2}, \quad C_{p^3} \times C_{p} \times C_p, \quad C_{p^2} \times C_{p^2} \times C_p, \quad C_{p^2} \times C_{p} \times C_{p} \times C_p, \quad C_{p} \times C_{p} \times C_{p} \times C_{p} \times C_p.
\]

In particular, there are exactly seven nonisomorphic abelian groups of order \(p^5\).

(b) The number of nonisomorphic abelian groups of order \(p^n\) (\(p\) prime) can be found by the same argument. This number is clearly the number of ways of writing \(n\) as a sum of positive integers \(m_1, \ldots, m_r\). If \(n \in \mathbb{N}\), an equation of the form \(n = m_1 + \cdots + m_r\), where \(m_1, m_2, \ldots, m_r\) are natural numbers and \(m_1 \geq m_2 \geq \cdots \geq m_r > 0\), is called a partition of \(n\). Thus
the number of nonisomorphic abelian groups of order $p^n$ is the number of partitions of $n$. Notice that this number depends only on $n$, not on $p$.

The partitions of 6 are

\[ 6, \ 5+1, \ 4+2, \ 4+1+1, \ 3+3, \ 3+2+1, \ 2+2+2, \ 2+2+1+1, \ 2+1+1+1+1, \ 1+1+1+1+1+1 \]

and an abelian group of order $p^6$ is isomorphic to one of

\[ C_{p^6}, \ C_{p^5} \times C_p, \ C_{p^4} \times C_{p^2}, \ C_{p^3} \times C_{p^3}, \ C_{p^4} \times C_{p^2} \times C_p, \ C_{p^3} \times C_{p^2} \times C_p, \ C_{p^2} \times C_p \times C_p \times C_p \times C_p, \ C_p \times C_p \times C_p \times C_p \times C_p \times C_p, \]

(c) Let us find all abelian groups of order 324,000 = $2^5 \cdot 3^4 \cdot 5^3$ (to within isomorphism). An abelian group $A$ of this order is the direct product $A_2 \times A_3 \times A_5$, where $A_p$ denotes the Sylow $p$-subgroup of $A$ ($p = 2, 3, 5$). Here $A_2$ has order $2^5$ and is isomorphic to one of the seven groups of type

\[ (2^5), \ (2^4, 2), \ (2^3, 2^2), \ (2^3, 2, 2), \ (2^2, 2^2, 2), \ (2, 2, 2, 2, 2). \]

Likewise there are five possibilities for $A_3$:

\[ (3^4), \ (3^3, 3), \ (3^2, 3^2), \ (3^2, 3, 3), \ (3, 3, 3, 3) \]

and three possibilities for $A_5$:

\[ (5^3), \ (5^2, 5), \ (5, 5, 5) \]

The 7·3·5 various direct products $A_2 \times A_3 \times A_5$ gives us a complete list of nonisomorphic abelian groups of order 324,000.

Now that we obtained a complete classification of finite abelian groups, we turn our attention to torsion-free ones.

**28.12 Lemma:** Let $G$ be an abelian group, $B$ a subgroup of $G$ and assume that $G/B$ is a direct product of $k$ infinite cyclic groups ($k \geq 1$), say

\[ G/B = \langle y^1 \rangle \times \langle y^2 \rangle \times \ldots \times \langle y^k \rangle \]

($y^1, y^2, \ldots, y^k \in G$). Then $\langle y^1 \rangle, \langle y^2 \rangle, \ldots, \langle y^k \rangle$ are infinite cyclic groups and

\[ G = B \times \langle y^1 \rangle \times \langle y^2 \rangle \times \ldots \times \langle y^k \rangle. \]
Proof: Let $Y := \langle y_1, y_2, \ldots, y_k \rangle \leq G$. Then $G/B = \langle By_1, By_2, \ldots, By_k \rangle$ and, from Lemma 28.4(5), we obtain $G = BY$. We will show that $G = B \times Y$ and $Y = \langle y_1 \rangle \times \langle y_2 \rangle \times \ldots \times \langle y_k \rangle$.

To establish $G = B \times Y$, we need only prove $B \cap Y = 1$. Let $g \in B \cap Y$. Then $g = a_1 \cdot y_1^{a_2} \cdot \ldots \cdot y_k^{a_k}$ for some integers $a_1, a_2, \ldots, a_k$ (Lemma 28.4(1)) and $B = Bg = (By_1)^{a_1}(By_2)^{a_2} \cdot \ldots \cdot (By_k)^{a_k}$. Since $\{By_1, By_2, \ldots, By_k\}$ is an independent subset of $G/B$ (Lemma 28.4(7)), we get $(By_1)^{a_1} = (By_2)^{a_2} = \ldots = (By_k)^{a_k} = B$. But $o(By_1) = o(By_2) = \ldots = o(By_k) = \infty$ by hypothesis, so $a_1 = a_2 = \ldots = a_k = 0$ and thus $g = y_1^0 y_2^0 \cdot \ldots \cdot y_k^0 = 1$. This proves $B \cap Y = 1$. Hence $G = B \times Y$.

We now prove $Y = \langle y_1 \rangle \times \langle y_2 \rangle \times \ldots \times \langle y_k \rangle$. In view of Lemma 28.4(7), we must only show that $\{y_1, y_2, \ldots, y_k\}$ is an independent subset of $Y$. Suppose $m_1, m_2, \ldots, m_k$ are integers with

$$y_1^{m_1} y_2^{m_2} \cdot \ldots \cdot y_k^{m_k} = 1.$$  

Then

$$(By_1)^{m_1} (By_2)^{m_2} \cdot \ldots \cdot (By_k)^{m_k} = B,$$

so

$$m_1 = m_2 = \ldots = m_k = 0$$

and

$$y_1^{m_1} y_2^{m_2} = \ldots = y_k^{m_k} = 1.$$  

Hence $\{y_1, y_2, \ldots, y_k\}$ is independent and $Y = \langle y_1 \rangle \times \langle y_2 \rangle \times \ldots \times \langle y_k \rangle$.

Finally, since $By_i$ has infinite order, we see that $y_i$ has also infinite order and $\langle y_i \rangle$ is an infinite cyclic group $(i = 1, 2, \ldots, k)$.

\[ \square \]

28.13 Theorem: Let $G$ be a finitely generated nontrivial torsion-free abelian group.

(1) $G$ has a basis, that is, there are elements $g_1, g_2, \ldots, g_r$ in $G \setminus 1$ such that $G = \langle g_1 \rangle \times \langle g_2 \rangle \times \ldots \times \langle g_r \rangle$.

(2) The number of elements in a basis of $G$ is uniquely determined by $G$. More precisely, if $\{g_1, g_2, \ldots, g_r\}$ and $\{h_1, h_2, \ldots, h_s\}$ are bases of $G$, then $r = s$. The number of elements in a basis of $G$ is called the rank of $G$.

(3) Let $H$ be a finitely generated nontrivial torsion-free abelian group. Then $G \cong H$ if and only if $G$ and $H$ have the same rank.

Proof: (1) Let $G$ be a nontrivial torsion-free abelian group and assume that $G = \langle u_1, u_2, \ldots, u_n \rangle$. We prove the claim by induction on $n$. If $n = 1$,
then \( G = \langle u_1 \rangle \) is a nontrivial cyclic group and the claim is true (with \( r = 1 \), \( g_1 = u_1 \)).

Suppose now \( n \geq 2 \) and suppose inductively: if \( G_1 \) is a nontrivial torsion-free abelian group generated by a set of \( m \) elements, where \( m \leq n - 1 \), then \( G_1 \) is a direct product of a finitely many cyclic subgroups of \( G \).

If \( u_1 = 1 \), then \( G = \langle u_1, u_2, \ldots, u_n \rangle = \langle u_2 \rangle, \ldots, \langle u_n \rangle \) is generated by a set of \( n - 1 \) elements and, by induction, \( G \) has a basis. Let us assume therefore \( u_1 \neq 1 \). Then \( o(u_1) = \infty \). We put \( B/\langle u_1 \rangle = T(G/\langle u_1 \rangle) \).

For any \( b \in B \), the element \( \langle u_1 \rangle b \) of \( B/\langle u_1 \rangle \) has finite order, thus there is a natural number \( n \) with \( b^n \in \langle u_1 \rangle \). Consequently, for any \( b \in B \), there is an \( n \in \mathbb{N} \) and \( m \in \mathbb{Z} \) such that \( b^n = u_1^m \).

We define a mapping \( \varphi : B \to \mathbb{Q} \) by declaring \( b\varphi = m/n \) for any \( b \in B \), where \( n \in \mathbb{N}, m \in \mathbb{Z} \) are such that \( b^n = u_1^m \). This mapping is well defined, for if \( n' \in \mathbb{N} \) and \( m' \in \mathbb{Z} \) are also such that \( b^{n'} = u_1^{m'} \), then \( u_1^{m \cdot n - m \cdot n'} = (u_1^{m})^{n \cdot n'-1} = b^{n}(b^{m \cdot n'-1}) = 1 \), so \( m \cdot n - m \cdot n' = 0 \) (because \( o(u_1) = \infty \)) and \( m/n = m'/n' \).

\( \varphi \) is in fact a homomorphism. To see this, let \( b, c \in B \) and \( b\varphi = m/n \), \( c\varphi = m'/n' \) (where \( n, n', m, m' \in \mathbb{Z} \)). Then \( b^n = u_1^m \) and \( c^n = u_1^{m'} \), so

\[
(bc)^{mn} = (b^n)^m (c^n)^m = u_1^{mn} u_1^{mn} = u_1^{mn+mn}
\]

and

\[
(bc)\varphi = (mn + m'n)/mn' = m/n + m'/n' = b\varphi + c\varphi.
\]

Thus \( \varphi \) is a homomorphism.

Since \( \text{Ker} \varphi = \{ b \in B : b\varphi = 0/1 \} = \{ b \in B : b^1 = u_1^0 \} = 1 \), the homomorphism \( \varphi \) is one-to-one and \( \varphi : B \to \text{Im} \varphi \) is an isomorphism: \( B \cong \text{Im} \varphi \).

Claim: if \( B \) is finitely generated, then \( B \) is cyclic. To prove this, assume \( B = \langle b_1, b_2, \ldots, b_t \rangle \) and let \( b_i\varphi = m_i/n_i \) (\( i = 1, 2, \ldots, t \)). Using Lemma 28.4(3), we see that \( \text{Im} \varphi = \langle b_1\varphi, b_2\varphi, \ldots, b_t\varphi \rangle = \langle m_1/n_1, m_2/n_2, \ldots, m_t/n_t \rangle \) is a subgroup of the additive cyclic group \( \langle 1/n_1 n_2 \ldots n_t \rangle \). Hence \( \text{Im} \varphi \) is cyclic and \( B \) is cyclic.

If \( B = G \), then \( B \) is finitely generated by hypothesis, so \( B = G \) is cyclic and (1) is proved. We assume therefore \( B \neq G \). Then

\[
G/B = \langle Bu_1, Bu_2, \ldots, Bu_n \rangle = \langle Bu_2, \ldots, Bu_n \rangle
\]
(see Lemma 28.4(4)) is a nontrivial abelian group, generated by \( n - 1 \) elements. Moreover, \( G/B = G/\langle u_1 \rangle / B/\langle u_1 \rangle = G/\langle u_1 \rangle / T(G/\langle u_1 \rangle) \) is torsion-free by Lemma 28.1(2). So, by induction,

\[
G/B = \langle B g_2 \rangle \times \ldots \times \langle B g_r \rangle
\]

with suitable \( g_i \in G \), where \( B g_i \) is distinct from \( B \) \((i = 2, \ldots , r)\). Thus \( o(B g_i) = \infty \), and this forces \( o(g_i) = \infty (i = 2, \ldots , r) \). Lemma 28.12 yields

\[
G = B \times \langle g_2 \rangle \times \ldots \times \langle g_r \rangle.
\]

We put \( \langle g_2, \ldots , g_r \rangle = A \). Then \( G = B \times A \) and \( B \cong G/A \) is finitely generated by Theorem 22.7(2), Lemma 28.4(4). Hence, by the claim above, \( B \) is cyclic, say \( B = \langle g_1 \rangle \). Since \( 1 \not\subseteq \langle u_1 \rangle \subseteq \langle g_1 \rangle \), we have \( o(g_1) \neq 1 \), so \( o(g_1) = \infty \) and

\[
G = \langle g_1 \rangle \times \langle g_2 \rangle \times \ldots \times \langle g_r \rangle.
\]

This completes the proof of (1).

(2) and (3) For convenience, a natural number \( r \) will be called a \textit{rank} of a finitely generated nontrivial torsion-free abelian group \( A \) if \( A \) has a basis of \( r \) elements. We cannot say \textit{the} rank of \( A \), for part (2) is not proved yet. The claim in part (2) is that all ranks of a finitely generated nontrivial torsion-free abelian group (arising from different bases) are equal.

Let \( G \) and \( H \) be finitely generated nontrivial torsion-free abelian groups, let \( r \) be a rank of \( G \) and \( s \) be a rank of \( H \), say \( G = \langle g_1 \rangle \times \langle g_2 \rangle \times \ldots \times \langle g_r \rangle \) and \( H = \langle h_1 \rangle \times \langle h_2 \rangle \times \ldots \times \langle h_s \rangle \).

If \( r = s \), then \( \langle g_i \rangle \cong \mathbb{Z} \cong \langle h_i \rangle \) for \( i = 1, 2, \ldots , r \) and

\[
G = \langle g_1 \rangle \times \langle g_2 \rangle \times \ldots \times \langle g_r \rangle \cong \langle h_1 \rangle \times \langle h_2 \rangle \times \ldots \times \langle h_r \rangle \cong H
\]

by Lemma 22.16. This proves the "if" part of (3).

Now the "only if" part of (3), which includes (2) as a particular case (when \( G = H \)): we will prove that \( G \cong H \) implies \( r = s \). This is easy. Now

\[
G/G^2 \cong \langle g_1 \rangle / \langle g_1^2 \rangle \times \langle g_2 \rangle / \langle g_2^2 \rangle \times \ldots \times \langle g_r \rangle / \langle g_r^2 \rangle \cong C_2 \times C_2 \times \ldots \times C_2
\]

is a finite group of order \( 2^r \) by Lemma 28.8(3). Also

\[
H/H^2 \cong \langle h_1 \rangle / \langle h_1^2 \rangle \times \langle h_2 \rangle / \langle h_2^2 \rangle \times \ldots \times \langle h_s \rangle / \langle h_s^2 \rangle \cong C_2 \times C_2 \times \ldots \times C_2
\]

This completes the proof of (1).
is a finite group of order $2^s$. If $G \cong H$, then $G/G^2 \cong H/H^2$ (Lemma 28.8(4)), so $2^r = |G/G^2| = |H/H^2| = 2^s$. Hence $r = s$.

\[ \square \]

**28.14 Remark:** Theorem 28.13 states essentially that a direct sum $\mathbb{Z}^r := \mathbb{Z} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}$ of $r$ copies of $\mathbb{Z}$ cannot be isomorphic to a direct sum $\mathbb{Z}^s := \mathbb{Z} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}$ of $s$ copies of $\mathbb{Z}$ unless $r = s$. This is not obvious: there are many one-to-one mappings from $\mathbb{Z}^r$ onto $\mathbb{Z}^s$, and there is no a priori reason why one of these mappings should not be an isomorphism. The proof of $\mathbb{Z}^r \cong \mathbb{Z}^s \Rightarrow r = s$ does not and cannot consist in cancelling one $\mathbb{Z}$ at a time from both sides of $\mathbb{Z}^r \cong \mathbb{Z}^s$. In general, it does not follow from $A \times B \cong A \times C$ that $B \cong C$. As a matter of fact, there are abelian groups $G$ such that $G \cong G \times G \times G$ but $G \not\cong G \times G$.

**28.15 Theorem:** Let $G$ be a finitely generated abelian group. Then $T(G)$ is a finite group and there is a subgroup $I$ of $G$ such that $G = T(G) \times I$.

**Proof:** $G/T(G)$ is a finitely generated abelian group (Lemma 28.4(4)), and is torsion-free (Lemma 28.1(2)). Thus either $G/T(G) \cong 1$; or $G/T(G) \cong \langle T(G)g_1 \rangle \times \langle T(G)g_2 \rangle \times \ldots \times \langle T(G)g_r \rangle$ with suitable $g_1, g_2, \ldots, g_r \in G$ (Theorem 28.13(1)) and therefore $G = T(G) \times \langle g_1 \rangle \times \langle g_2 \rangle \times \ldots \times \langle g_r \rangle$ (Lemma 28.12). Putting $I = 1$ in the first case and $I = \langle g_1 \rangle \times \langle g_2 \rangle \times \ldots \times \langle g_r \rangle$ in the second case, we obtain $G = T(G) \times I$.

Then $T(G) \cong G/I$ by Theorem 22.7(2). Since $G$ is finitely generated, so is $G/I$ (Lemma 28.4(4)) and $T(G)$ is also finitely generated. From Lemma 28.4(2), it follows that $T(G)$ is a finite group.

\[ \square \]

The subgroup $I$ in Theorem 28.15 is not uniquely determined by $G$. However, its rank $r(I)$, which is the rank of $G/T(G)$ is completely determined by $G$ when $G/T(G) \not\cong 1$. Let us define the rank of the trivial group $1$ to be $0$ and let us call $\emptyset$ a basis of $1$. Then the rank of any finitely generated torsion-free abelian group is the number of elements in a basis of that group, and $r(I)$ is completely determined by $G$, also in case $G/T(G) \cong 1$.  

317
As $G = T(G) \times I$, the finitely generated abelian group $G$ is determined uniquely to within isomorphism by $T(G)$ and $I$. Now $I$ is determined uniquely to within isomorphism by the integer $r(I)$ (Theorem 28.13(3) and the definition $r(1) = 0$); and $T(G)$, being a finite abelian group (Theorem 28.15), is determined uniquely to within isomorphism by its Sylow subgroups (Theorem 28.7(4)). Let $s$ be the number of distinct prime divisors of $|T(G)|$ (so $s = 0$ when $T(G) \cong 1$). Each one of the $s$ Sylow subgroups (corresponding to the $s$ distinct prime divisors) is determined uniquely to within isomorphism by its type (Theorem 28.10(3)). Thus the finitely generated abelian group $G$ gives rise to the following system of nonnegative integers.

(i) A nonnegative integer $r$, namely the rank of $G/T(G)$. Here $r = 0$ means that $G$ is a finite group. If $r > 0$, then $T(G) \times I$, where $I$ is a direct product of $r$ cyclic groups of infinite order. The subgroup $I$ is not, but its isomorphism type is uniquely determined by $G$.

(ii) A nonnegative integer $s$, namely the number of distinct prime divisors of $|T(G)|$. Here $s = 0$ means that $T(G) \cong 1$ and $G$ is a torsion-free group.

(iii) In case $s > 0$, a system $p_1, p_2, \ldots, p_s$ of prime numbers, namely the distinct prime divisors of $|T(G)|$; and for each $i = 1, 2, \ldots, s$, a positive integer $t_i$ and $t_i$ positive integers $m_{i1}, m_{i2}, \ldots, m_{it_i}$, so that $(p_1^{m_{i1}}, p_2^{m_{i2}}, \ldots, p_s^{m_{it_i}})$ is the type of the Sylow $p_i$-subgroup of $T(G)$.

With this information, $G$ is a direct product of $r + t_1 + t_2 + \cdots + t_s$ cyclic subgroups. $r$ of them are infinite cyclic; and (in case $s > 0$) $t_i$ of them have orders equal to a prime number $p_i$, more specifically, $t_i$ of them have orders $p_i^{m_{i1}}, p_i^{m_{i2}}, \ldots, p_i^{m_{it_i}}$. Furthermore, two finitely generated abelian groups are isomorphic if and only if they give rise to the same system of integers.

Exercises

1. Let $G$ be an abelian group and $H \leq G$. Prove that

   (a) $T(H) = T(G) \cap H$
(b) \( T(G)/T(H) \cong HT(G)/H \leq T(G/H) \)
and that \( HT(G)/H \) need not be equal to \( T(G/H) \).

2. Let \( G \) be an abelian group. Show that
(a) if \( G \) is finite, then \( G/G^n \cong G/[n] \) for all \( n \in \mathbb{N} \);
(b) if \( G \) is infinite, then \( G/G^n \cong G/[n] \) need not hold for any \( n \in \mathbb{N}\setminus\{1\} \).

3. Let \( G \) be a finite abelian group. The exponent of \( G \) is defined to be the largest number in \( \{ o(a) : a \in G \} \), i.e., the largest possible order of the elements in \( G \). Show that
(a) the exponent of \( G \) divides \( |G| \);
(b) for any \( g \in G \), \( o(g) \) divides the exponent of \( G \);
(c) the exponent of \( G \) is the least common multiple of the order of the elements in \( G \);
(d) \( G \) is cyclic if and only if the exponent of \( G \) is \( |G| \).

4. Let \( G \) be a finite abelian group and \( H \trianglelefteq G \). Let \( K \trianglelefteq G \) such that \( H \cap K = 1 \) and \( H \cap L \neq 1 \) for any \( L \trianglelefteq G \) satisfying \( K \trianglelefteq L \). Let \( g \in G \).

(a) Assume \( g^n \in K \) for some prime number \( p \). Prove that, if \( g \notin K \), then there are \( h \in H \), \( k \in K \) and an integer \( r \) relatively prime to \( p \) such that \( h = kg^r \). Conclude that \( g \notin HK \).

(b) Prove that \( G = H \times K \) if and only if, for any prime number \( p \) and elements \( g \in G \), \( h \in H \), \( k \in K \) such that \( g^n = hk \), there is an element \( h' \in H \) satisfying \( h = (h')^p \).

5. Let \( G \) be a finite abelian group of exponent \( e \) and let \( g \in G \) be of order \( e \), so that \( o(g) = e \). Put \( H = \langle g \rangle \). Show that \( G = H \times K \) for some \( K \trianglelefteq G \). (Hint: Use Ex. 4. Consider the cases \( p \mid e \) and \( p \nmid e \) separately.

6. Let \( G \) be a nontrivial finite abelian group. Using Ex. 5, prove by induction on \( |G| \) that there are non-trivial elements \( g_1, g_2, \ldots, g_r \) in \( G \) such that \( G = \langle g_1 \rangle \times \langle g_2 \rangle \times \ldots \times \langle g_r \rangle \) and (in case \( r > 1 \)) \( o(g_i) \) divides \( o(g_{i+1}) \) for \( i = 1, 2, \ldots, r - 1 \).

7. Keep the notation of Ex. 6. Prove that the integers \( o(g_1), o(g_2), \ldots, o(g_r) \) determine the types of the Sylow \( p \)-subgroups of \( G \) uniquely, and conversely the types of the Sylow \( p \)-subgroups of \( G \) completely determine the integers \( o(g_1), o(g_2), \ldots, o(g_r) \). (The integers \( o(g_1), o(g_2), \ldots, o(g_r) \) are
called the *invariant factors of* $G$. Two finite abelian groups are thus isomorphic if and only if they have the same invariant factors.

8. Find the invariant factors of the finite abelian groups $C_6 \times C_9$, $C_6 \times C_8 \times C_{15} \times C_{30}$, $C_4 \times C_6 \times C_{15} \times C_{20}$. 