Cyclic groups were among the first examples of groups which you have studied. Amazingly, it turns out that an arbitrary finite abelian group is isomorphic to a direct product of cyclic groups of prime power order. Not only this, these prime power orders are uniquely determined, forming a complete system of invariants. This result is known as the Structure Theorem for Finite Abelian Groups. It was first developed in the 1879 paper of the mathematicians Georg Frobenius and Ludwig Stickelberger. Later it was both simplified and generalised to finitely generated abelian groups.

In this unit, we will first discuss the structure of finite abelian groups, in Sec.5.2. Then, in Sec.5.3, we will focus on finitely generated abelian groups. Here you will also see what a free abelian group is.

In the next section, Sec.5.4, we put together what you have studied in the previous two sections. The aim is to understand what any finitely generated abelian group looks like.

Thus, studying this unit will give you a way of obtaining any finite, or finitely generated, abelian group, up to isomorphism.

We now list the particular objectives of this unit.

Objectives

After studying this unit, you should be able to:

• state, prove and apply, the Structure Theorem for Finite Abelian Groups;
• obtain all abelian groups (upto isomorphism) of a given order;
• describe, and give examples of, free abelian groups;
• state, prove and apply, the Structure Theorem for Finitely Generated Abelian Groups;
• give the rank, invariant factors and elementary divisors of any given finitely generated abelian group;
• obtain all finitely generated abelian groups (up to isomorphism) of a given rank and with torsion subgroup of a given order.
5.2 FINITE ABELIAN GROUPS

In Unit 3 you studied what a direct product of groups, or of subgroups, is. You have also seen that any finite cyclic group of order \(n\) is isomorphic to \(\mathbb{Z}_n\). Here we will use this knowledge to classify finite abelian groups. In fact, the focus of this section is the following very fundamental theorem.

Structure Theorem of Finite Abelian Groups: Every non-trivial finite abelian group \(G\) is isomorphic to a direct product of cyclic groups of prime power order:

\[ G \cong \mathbb{Z}_{q_1^{e_1}} \times \mathbb{Z}_{q_2^{e_2}} \times \cdots \times \mathbb{Z}_{q_k^{e_k}}, \]

where \(q_1, q_2, \cdots, q_k\) are primes (not necessarily distinct) and \(e_i \geq 1\) for all \(i\). Moreover, the prime powers \(q_1^{e_1}, q_2^{e_2}, \ldots, q_k^{e_k}\) are uniquely determined by \(G\).

Let us try and understand the amazing power of this theorem. It says that given any finite abelian group, of any order whatsoever, it can be written as a direct product of cyclic groups of a certain order.

So, for example, an abelian group of order \(7 \times 5 \times 2^2\) can basically have the structure \(\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_7\), or \(\mathbb{Z}_7 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5\), or another such break up of the prime powers.

Let us, now, try and prove the Structure Theorem. For this, we first need to prove certain results that will be used in the main proof.

**Theorem 1:** Let \(G\) be an abelian group of order \(n > 1\). For each prime \(p\) dividing the order of \(G\), define \(G(p) = \{a \in G \mid o(a)\text{ is a power of } p\}\). Then \(G(p)\) is a subgroup of \(G\) and \(G(p)\) is the unique Sylow \(p\)-subgroup of \(G\).

**Proof:** From Unit 3, you know that for each prime \(p\) dividing \(o(G)\), \(G\) has an element of order \(p\). So \(G(p) \neq \emptyset\).

Let \(a, b \in G(p)\). Then \(a^{p^m} = e\) and \(b^{p^n} = e\) for some \(m, n \in \mathbb{N}\).

Therefore, \((ab^{-1})^{p^{m+n}} = (a^{p^m})^{p^n} ((b^{p^n})^{p^m})^{-1} = e\). Thus, \(ab^{-1} \in G(p)\), that is, \(G(p)\) is a subgroup of \(G\).

We will now prove that the order of \(G(p)\) is a power of \(p\), by contradiction.

So, suppose \(q\) is a prime different from \(p\) dividing \(o(G(p))\). Then you know, by Cauchy’s theorem, there is an element \(b \in G(p)\) of order \(q\), which contradicts the definition of \(G(p)\). Hence, we reach a contradiction. Thus, our assumption must be wrong. Hence, \(o(G(p))\) is a power of \(p\).

Now we will show that any Sylow \(p\)-subgroup of \(G\) must be \(G(p)\). So, let \(S\) be a Sylow \(p\)-subgroup of \(G\). As the order of any element of \(S\) is a power of \(p\), it follows that \(S \subseteq G(p)\). Also, from Unit 3, you know that any \(p\)-subgroup of \(G\) cannot contain a Sylow \(p\)-subgroup properly. Consequently, \(S = G(p)\).

This proves the result.

Theorem 1 tells us what the Sylow subgroups of a finite abelian group look like. What happens if \(G\) is not abelian? Consider the following remark.
Remark 1: Note that if $G$ is not abelian, $G(p)$ need not be a subgroup of $G$.

For instance, take $G(2) = \{e, (1 2), (2 3), (1 3)\}$ in $S_3$. Since $(1 2)(1 3) \not\in G(2), G(2) \not\subseteq S_3$.

Hence, Theorem 1 doesn’t hold if $G$ is not abelian.

The next result tells us that a **finite abelian group is a direct product of its Sylow $p$-subgroups**.

**Theorem 2:** Let $G$ be an abelian group of order $n = p_1^{n_1}p_2^{n_2} \cdots p_k^{n_k}$, where the $p_i$’s are distinct primes and $n_i \geq 1$ for $i = 1, \ldots, k$. Then $G \cong G(p_1) \times G(p_2) \times \cdots \times G(p_k)$.

**Proof:** We will prove this in two steps.

**Step 1:** To show that $G = G(p_1)G(p_2)\ldots G(p_k)$:

First, we note that since $G$ is abelian, $G(p_1)G(p_2)\ldots G(p_k) \leq G$.

Next, suppose $a \in G(p_i)$. By Lagrange’s Theorem, $a^n = 1$.

Set $m_i = n/p_i^{n_i}, 1 \leq i \leq k$.

As $\text{g.c.d}(m_1, \ldots, m_k) = 1$, we can find integers $\alpha_1, \ldots, \alpha_k$ such that

$$\alpha_1m_1 + \cdots + \alpha_km_k = 1.$$  \hspace{1cm} (1)

Hence $a = a^{\alpha_1m_1} \cdots a^{\alpha_km_k}$, where $a_i = a^{\alpha_im_i}$.

As $a_i^{p_i^{n_i}} = (a_i)^{n_i} = 1$, we see that $a_i \in G(p_i)$.

Consequently, it follows from Equation (1), that $G = G(p_1)G(p_2)\ldots G(p_k)$.

**Step 2:** To show that $G(p_i) \cap G(p_j) = G(p_i)\ldots G(p_{i+1})G(p_{i+1})\ldots G(p_k)$.

Suppose $x \in G(p_i) \cap G(p_j)$. Then $x = x_{i} \cdots x_{i+1}x_{i+1} \cdots x_k$, where $x_{i} \in G(p_i)$.

Since $o(G(p_i)) = p_i^{n_i}, x_{j}^{p_i^{n_i}} = 1$, and hence $x^{p_i^{n_i} \cdots p_{i+1}^{n_{i+1}} \cdots p_k^{n_k}} = e$.  \hspace{1cm} (3)

Also $x \in G(p_i)$, so that $x_{i}^{p_i^{n_i}} = 1$.  \hspace{1cm} (4)

Since $\text{g.c.d}(p_i^{n_i}, p_j^{n_j} \cdots p_{i+1}^{n_{i+1}} \cdots p_k^{n_k}) = 1$, (3) and (4) give us $x = e$, which proves that $G(p_i) \cap G(p_j) \cdots G(p_{i+1})G(p_{i+1})\ldots G(p_k) = \{e\}$.  \hspace{1cm} (5)

Now, from Steps 1 and 2, and noting that $G(p_i) \triangleleft G \forall i = 1, \ldots, k$ (as $G$ is abelian), we get $G \cong G(p_1) \times G(p_2) \times \cdots \times G(p_k)$.

From this theorem, we know that to study a finite abelian group, we need to look at the structure of each of its Sylow $p$-subgroups. So, let us temporarily restrict our attention to studying the structure of an abelian $p$-group, that is, an abelian group $G$ of order $p^n, n \geq 1$. Firstly, for such a $G$, the order of its elements cannot exceed $p^n$. So, there exists $a \in G$ of **maximal order in $G$**, i.e., $\exists a \in G$ such that $o(a) \leq o(x) \forall x \in G$. Also, note that in this case $o(x) \mid o(a) \forall x \in G$. We will be using such an element in the following result.
**Theorem 3:** Let $G$ be a finite abelian $p$-group, $G \neq \{e\}$, and let $a \in G$ be of maximal order in $G$. Then $G$ is cyclic or there is a subgroup $H$ of $G$, such that $G \cong \langle a \rangle \times H$.

**Proof:** Let $o(a) = p^k$. If $G = \langle a \rangle$, then $G$ is cyclic.

Suppose $G \neq \langle a \rangle$. Consider the set $\mathcal{A} = \{K \leq G | \langle a \rangle \cap K = \{e\}\}$.

Let $H$ be maximal in $\mathcal{A}$, that is, $H$ belongs to $\mathcal{A}$, and if $K$ is any element of $\mathcal{A}$, then $K$ cannot properly contain $H$. We will prove that $G \cong \langle a \rangle \times H$.

Since $G$ is abelian, all its subgroups are normal. Moreover, by definition, $\langle a \rangle \cap H = \{e\}$. Therefore, in order to prove that $G \cong \langle a \rangle \times H$, we only need to show that $G = \langle a \rangle H$. We will prove this by contradiction.

So, suppose that $G \neq \langle a \rangle H$. Then $G/(\langle a \rangle H)$ is a $p$-group, and hence contains an element of order $p$. In other words, there exists $x \in G/(\langle a \rangle H)$ such that $x^p = e$, that is, $\exists x \in G$ such that $x \notin \langle a \rangle H$ but $x^p \in \langle a \rangle H$. So, $x^p = a^pb$, for some $q \in \mathbb{Z}$ and $b \in H$.

Now, since the order of every element of $G$ divides $p^k$, $e = x^k = (x^p)^{k^{-1}} = a^{w^{-1}} b^{k^{-1}}$.

$\Rightarrow a^{w^{-1}} \in \langle a \rangle \cap H = \{e\}$

$\Rightarrow p | q$

$\Rightarrow q = ps$, for some $s \in \mathbb{Z}$.

Recall that $x \notin \langle a \rangle H$, so $xa^{-1} \notin H$. However,

$\langle xa^{-1} \rangle^p = x^pa^{-p} = x^a^a^{-1} = b \in H$.

...(6)

Now, take $K = \langle xa^{-1} \rangle H$. Note that $H \subseteq K$. Moreover $xa^{-1} \in K$, but $xa^{-1} \notin H$, so $H \neq K$.

Therefore, by the maximality of $H$ in $\mathcal{A}$, $\langle a \rangle \cap K = \{e\}$.

Let $a \in \langle a \rangle \cap K$, where $a \neq e$.

Then there exist $t, u, h \in \mathbb{Z}, h \in H$ such that $a = a^t$ and $a = (xa^{-1})^uh$.

Now, could $p$ divide $u$? Suppose it does. Then $u = pv$ for some $v \in \mathbb{Z}$.

So $\alpha = (xa^{-1})^v = ((xa^{-1})^p)^v \in H$, by (6), i.e., $\alpha \in H$.

But $\alpha \in \langle a \rangle$ as well, and $\langle a \rangle \cap H = \{e\}$. We reach a contradiction, since $\alpha \neq e$. Therefore, $p$ does not divide $u$.

Next, since $p$ is prime, $g.c.d(p, u) = 1$. So there exist integers $w$ and $d$ such that $1 = pw + ud$. Therefore, $x = (x^p)^w (x^u)^d$.

Now, you know that $x^p \in \langle a \rangle H$.

Also $\alpha = a^t = (xa^{-1})^v \Rightarrow x^u = a^{aw^{-1}} \in \langle a \rangle H$. Therefore, $x \notin \langle a \rangle H$. This is a contradiction to how $x$ was chosen.

Therefore, our assumption that $G \neq \langle a \rangle H$ must be wrong.
Thus, \( G = \langle a \rangle > H \).

Therefore, \( G = \langle a \rangle > H. \)

This result has an immediate corollary about the structure of a finite abelian p-group.

**Corollary 1:** Any finite abelian p-group \( G \) can be expressed as an internal direct product of cyclic subgroups. (Note that the order of each of these subgroups is a power of \( p \).)

**Proof:** From Theorem 3, \( \exists a \in G \) such that \( G = \langle a \rangle > H \).

If \( H \neq \{e\} \), we can repeat this process on \( H \) to get \( H = \langle b \rangle > K \), where \( b \in H \) is of maximal order in \( H \), and \( K \) is a proper subgroup of \( H \), so that \( G = \langle a \rangle > \langle b \rangle > K \).

Since \( G \) is finite, eventually this process will end. Consequently, we have \( G \) as a direct product of cyclic groups, each of order some power of \( p \).

With Theorem 2 and Corollary 1 put together, you may have got some idea of the structure of finite abelian groups. This is the fundamental result we had mentioned at the beginning of this section.

**Theorem 4 (Structure Theorem for Finite Abelian Groups):** Every non-trivial finite abelian group \( G \) is isomorphic to a direct product of cyclic groups of prime power order, that is,

\[
G \cong \mathbb{Z}_{q_1^{e_1}} \times \mathbb{Z}_{q_2^{e_2}} \times \cdots \times \mathbb{Z}_{q_s^{e_s}},
\]

where \( q_1, q_2, \ldots, q_s \) are primes (not necessarily distinct) and \( e_i \geq 1 \) for all \( i \).

Moreover, the prime powers \( q_1^{e_1}, q_2^{e_2}, \ldots, q_s^{e_s} \) are uniquely determined by \( G \).

**Proof:** The proof is in two steps – first we write \( G \) as a direct product of its Sylow p-subgroups, and then we show that each of these Sylow p-subgroups is expressible as a direct product of cyclic groups (of course of prime power order).

Let \( \sigma(G) = p_1^{n_1}p_2^{n_2} \cdots p_k^{n_k} \), where the \( p_k \)s are distinct primes.

By Theorem 2, you know that \( G = G(p_1) \times G(p_2) \times \cdots \times G(p_k) \).

Further, by Corollary 1, \( G(p_i) \) can be decomposed further as a direct product of cyclic groups of order some power of \( p_i \), \( i = 1, \ldots, k \). Therefore, we see that \( G \) is isomorphic to a direct product of cyclic groups each of prime power order.

The proof of this theorem will be complete once you prove the uniqueness of the decomposition (see E1 and E2 below).

The uniqueness of the decomposition in the Structure Theorem leads us to the following definition.

**Definition:** The orders \( q_1^{e_1}, q_2^{e_2}, \ldots, q_s^{e_s} \) of the cyclic subgroups in the structural decomposition of a finite abelian group \( G \) are called the elementary divisors of \( G \). Further, the representation of \( G \), as the direct product of cyclic p-subgroups is called the elementary divisor decomposition of \( G \).
For example, if \( G \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \), then 2, 3 and 9 are the elementary divisors of \( G \). Also, \( G' \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \) has the same order as \( G \), but different elementary divisors, namely 2, 3, 3, 3.

We shall come back to these divisors a little later in this section. For now, try some related exercises.

**E1)** Let \( G_1 \) and \( G_2 \) be abelian groups of order \( p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k} \), where \( p_i \neq p_j \) for \( i \neq j \). Prove that \( G_1 \cong G_2 \) if and only if \( G_1(p_i) \cong G_2(p_i) \) for all \( i = 1, 2, \ldots, k \).

**E2)** Let \( G \) be an abelian group such that \( |G| = p^r \), where \( p \) is a prime. If \( G \cong H_1 \times H_2 \times \ldots \times H_m \) and \( G \cong K_1 \times K_2 \times \ldots \times K_n \), where the \( H_i \)'s and \( K_j \)'s are non-trivial cyclic subgroups of \( G \), with \( |H_1| \geq |H_2| \geq \ldots \geq |H_m| \) and \( |K_1| \geq |K_2| \geq \ldots \geq |K_n| \), then \( m = n \) and \( |H_i| = |K_i| \) for all \( i = 1, \ldots, m \).

**E3)** Obtain the elementary divisors of \( \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \). Are these the same as the elementary divisors of \( \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \)? Why, or why not?

Now, you may wonder how the Structure Theorem can be applied to specific groups in practice. To answer this, consider \( G \), a finite abelian group of order \( n = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k} \), where the \( p_i \)'s are distinct primes, \( n_i \geq 1 \) for all \( i = 1, \ldots, k \). Now, you know that the first step is to decompose \( G \) as a product of its Sylow subgroups, \( G(p_i), 1 \leq i \leq k \). Each of these Sylow subgroups have order \( p_i^{n_i} \), \( p_i^{n_2} \), \ldots, \( p_i^{n_k} \), respectively. You also know that each of these subgroups can be decomposed into a direct product of cyclic groups of prime power orders. Let us consider \( G(p_i) \). Suppose we have the following decomposition:

\[
G(p_i) \cong \mathbb{Z}_{p_i^{e_1}} \times \mathbb{Z}_{p_i^{e_2}} \times \ldots \times \mathbb{Z}_{p_i^{e_t}}.
\]

Here, we may assume \( e_1 \geq e_2 \geq \ldots \geq e_t \geq 1 \) (this is because for direct products, \( H \times K \cong K \times H \)). Now,

\[
p_i^{n_i} = o(G(p_i)) = o(\mathbb{Z}_{p_i^{e_1}} \times \mathbb{Z}_{p_i^{e_2}} \times \ldots \times \mathbb{Z}_{p_i^{e_t}})
= l_{p_i^{e_1}} \cdot l_{p_i^{e_2}} \cdot \ldots \cdot l_{p_i^{e_t}}
= p_i^{e_1 \cdot e_2 \cdot \ldots \cdot e_t}.
\]

So \( n_i = e_1 + e_2 + \ldots + e_t \). Hence the possibilities for the cyclic decomposition of each Sylow \( p_i \)-subgroup comes from **looking at all possible partitions** \( e_1 + e_2 + \ldots + e_t \) of \( n_i \), with \( e_1 \geq e_2 \geq \ldots \geq e_t \geq 1 \).

This gives us a method to apply the Structure Theorem of Finite Abelian Groups to find all the abelian groups, up to isomorphism, of a given order. You can see how the procedure works through an example of a \( p \)-group. Then we will move on to examples in which there is more than one prime involved.
Example 1: Determine all the possible abelian groups, up to isomorphism, of order 16.

Solution: As \( \sigma(G) = 16 = 2^4 \), we need to consider all the ways of partitioning 4. These are
\[
4 = 4 \\
4 = 3 + 1 \\
4 = 2 + 2 \\
4 = 2 + 1 + 1 \\
4 = 1 + 1 + 1 + 1.
\]
Therefore, \( G \) must be isomorphic to one of the following groups:
\[
\mathbb{Z}_{16} \\
\mathbb{Z}_4 \times \mathbb{Z}_4 = \mathbb{Z}_8 \times \mathbb{Z}_2 \\
\mathbb{Z}_4 \times \mathbb{Z}_2 = \mathbb{Z}_4 \times \mathbb{Z}_4 \\
\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 = \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \\
\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.
\]
Conversely, all five groups listed above are abelian groups of order 16, and no two of them are isomorphic. (For instance, \( \mathbb{Z}_8 \times \mathbb{Z}_2 \neq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \), since \( \mathbb{Z}_8 \times \mathbb{Z}_2 \) has an element of order 8, while all the non-zero elements of \( \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \) have order 2.)

Example 2: Determine all the possible abelian groups, up to isomorphism, of order 56.

Solution: \( \sigma(G) = 56 = 2^3 \times 7 \). We know that \( G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \), where \( |G(2)| = 2^3 \) and \( |G(7)| = 7 \). To obtain the possible exponents for elementary divisors of \( G(2) \) and \( G(7) \), we look at all possible ways of partitioning 3 (the exponent of \( 2^3 \)) and 1 (the exponent of \( 7^1 \))
\[
\begin{array}{c|c}
G(2) & G(7) \\
3 & 1 \\
2 + 1 & \\
1 + 1 + 1 & \\
\end{array}
\]
Thus, \( G \) must be isomorphic to one of the following groups:
\[
\mathbb{Z}_{2^3} \times \mathbb{Z}_7 = \mathbb{Z}_8 \times \mathbb{Z}_7 \\
\mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_7 = \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_7 \\
\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_7 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_7
\]
Conversely, all three groups listed above are abelian groups of order 56, and no two of them are isomorphic.

Example 3: Determine all the possible abelian groups, up to isomorphism, of order \( 2^3 \times 3^4 \).

Solution: \( G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \), where \( |G(2)| = 2^3 \), \( |G(3)| = 3^4 \) and
**Special Groups and Semigroups**

\[ |G(5)| = 5^3. \] The possible exponents for the elementary divisors of G(2), G(3) and G(5) are as follows:

<table>
<thead>
<tr>
<th>G(2)</th>
<th>G(3)</th>
<th>G(5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>1+1</td>
<td>3+1</td>
<td>2+1</td>
</tr>
<tr>
<td>2+2</td>
<td>1+1+1</td>
<td></td>
</tr>
<tr>
<td>1+1+1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Hence, the following is the list of all non-isomorphic abelian groups of order \(2^3 \cdot 3 \cdot 5^3\):

- \(\mathbb{Z}_4 \times \mathbb{Z}_{61} \times \mathbb{Z}_{125}\)
- \(\mathbb{Z}_4 \times \mathbb{Z}_{61} \times \mathbb{Z}_{25} \times \mathbb{Z}_5\)
- \(\mathbb{Z}_4 \times \mathbb{Z}_{61} \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5\)
- \(\mathbb{Z}_4 \times \mathbb{Z}_{27} \times \mathbb{Z}_3 \times \mathbb{Z}_{125}\)
- \(\mathbb{Z}_4 \times \mathbb{Z}_{27} \times \mathbb{Z}_3 \times \mathbb{Z}_{25} \times \mathbb{Z}_5\)
- \(\mathbb{Z}_4 \times \mathbb{Z}_{3} \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5\)
- \(\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{125}\)
- \(\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_{25} \times \mathbb{Z}_5\)
- \(\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5\)
- \(\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{125}\)
- \(\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25} \times \mathbb{Z}_5\)
- \(\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5\)
- \(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{61} \times \mathbb{Z}_{125}\)
- \(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{61} \times \mathbb{Z}_{25} \times \mathbb{Z}_5\)
- \(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{61} \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5\)
- \(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27} \times \mathbb{Z}_3 \times \mathbb{Z}_{125}\)
- \(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27} \times \mathbb{Z}_3 \times \mathbb{Z}_{25} \times \mathbb{Z}_5\)
- \(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5\)
- \(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_9 \times \mathbb{Z}_{125}\)
- \(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_9 \times \mathbb{Z}_{25} \times \mathbb{Z}_5\)
- \(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5\)
- \(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_{125}\)
- \(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_{25} \times \mathbb{Z}_5\)
- \(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5\)
Abelian Groups

\[
\begin{align*}
Z_4 \times Z_4 \times Z_3 \times Z_3 \times Z_3 \times Z_2 \times Z_2 \\
Z_2 \times Z_2 \times Z_3 \times Z_3 \times Z_3 \times Z_3 \times Z_5 \\
Z_2 \times Z_2 \times Z_3 \times Z_3 \times Z_3 \times Z_3 \times Z_3 \times Z_5
\end{align*}
\]

Also note that all the groups listed above are abelian, of order \(2^3 \cdot 3^4 \cdot 5^3\), and non-isomorphic.

***

Example 4: Let \(G\) be an abelian group of order 200, with exactly four elements of order 5. What are the possible isomorphism classes of \(G\)?

Solution: \(o(G) = 200 = 5^2 \cdot 2^3\).

So \(G \cong G(5) \times G(2)\), with \(o(G(5)) = 5^2\) and \(o(G(2)) = 2^3\).

Now, considering the partitions of 2 and 3, we have

\[
\begin{align*}
1+1 & \quad 2+1 \\
1+1+1 &
\end{align*}
\]

so, there are 6 possible isomorphism groups.

Any element of order 5 can only be from the direct summands of \(G(5)\), that is, \(Z_{25}\) or \(Z_4 \times Z_5\), since \(5 \nmid 2^3\). Further, 3 groups are of the form \(Z_{25} \times H\), up to isomorphism. (Here \(H\) is \(Z_8\), or \(Z_4 \times Z_2\), or \(Z_2 \times Z_2 \times Z_2\).)

Each of these has exactly 4 elements of order 5, namely, \((5,0),(10,0),(15,0),(20,0)\), where 0 is the zero element of \(H\). Note that if \((x,y) = (\overline{0},0)\), then \(5x = \overline{0}\) and \(5y = 0\), where \(x \in Z_{25}\), \(y \in H\).

The other 3 groups are of the form \(Z_4 \times Z_5 \times H\), which has 24 elements of order 5, of the form \((x,y,0), \forall x, y \in Z_5, x \neq (\overline{0},0), y \neq (\overline{0},0)\).

Thus, the required isomorphism classes are only three, namely, \(Z_{25} \times Z_4, Z_{25} \times Z_4 \times Z_2, Z_{25} \times Z_2 \times Z_2 \times Z_2\).

***

From the examples above, you may have gauged the following algorithm for finding all the possible non-isomorphic types of abelian groups of order \(n\):

Step 1: Factor \(n\) into distinct primes: \(n = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}\).

Step 2: Find the number \(p(n_i)\) of all the partitions of \(n_i\), i.e., \(p(n_i)\) is the number of ways \(n_i\) can be written as a sum of positive integers \(n_i = e_1 + e_2 + \ldots + e_t\), with \(e_1 \geq e_2 \geq \ldots \geq e_t (\geq 1), t \geq 1\) (in other words, \(p(n_i)\) is the number of ways to write \(n_i\) as a sum of positive integers, in descending order).

Step 3: Find all the abelian groups of order \(p_i^{n_i}\) (there will be \(p(n_i)\) of them).

Step 4: Repeat Steps 2 and 3 for primes \(n_2, \ldots, n_k\) and \(p_2, \ldots, p_k\).

Step 5: Build direct products of these \(p_i\)-groups in all the ways possible, to end up with \(p(n_1)p(n_2)\ldots p(n_k)\) non-isomorphic abelian groups of order \(n\).
It’s now time for you to check your understanding of what you have studied so far.

E4) Find all the possible abelian groups, up to isomorphism, of order
   i) 105,  ii) 270,  iii) 9801.

E5) What is the smallest positive integer \( n \) such that
   i) there are exactly two non-isomorphic abelian groups of order \( n \)?
   ii) there are exactly three non-isomorphic abelian groups of order \( n \)?

E6) How many abelian groups, up to isomorphism, are there
   i) of order \( pq \), where \( p \) and \( q \) are distinct primes?
   ii) of order \( pqr \), where \( p \), \( q \) and \( r \) are distinct primes?

E7) Suppose \( G \) is an abelian group of order 120 with exactly three elements of order 2. Determine all possible isomorphism classes of \( G \).

Now, let us consider another useful consequence of the fundamental structure theorem you have studied. This is a theorem you have proved earlier in Section 3.3, Unit 3.

**Theorem 5 (Converse of Lagrange’s theorem for abelian groups):** Let \( G \) be an abelian group of order \( n \) and let \( m \) be any positive divisor of \( n \). Then there exists a subgroup of \( G \) of order \( m \).

Before getting to its proof, consider an illustration of this result. You can think of this as a model for giving another proof of this theorem.

So, let \( G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_7 \), a group of order 1120210560.

Let us take a divisor of \( \text{order } G \), say 6048. How do we produce a subgroup of \( G \) of order 6048? For this, let us first look at the factorisation of 6048, i.e., \( 6048 = 2^5 \cdot 3^2 \cdot 7 \). Then let us find the prime powers of the cyclic group factors of \( G \) which just exceed or equal \( 2^5, 3^2 \) and \( 7 \), respectively.

Firstly, the exponent 5 of 2 is greater than all the exponents of 2 in \( \text{order } G \). So, we rewrite 5 as \( 3 + 2 \). Similarly, the exponent of 3 is rewritten as \( 2 + 1 \). Then we match them to whatever extent possible, as below.

\[
\begin{array}{cccccccc}
2^1 & 2^3 & 2 & 3^2 & 3^3 & 5 & 7^1 & 7 \\
\mid & \mid & \mid & \mid & \mid & \mid & \mid & \mid \\
2^3 & 2^2 & 3^2 & 3 & 7 \\
\end{array}
\]

\( \text{Elementary divisors of } G \)

Now, take a subgroup of the cyclic group in order to match the total exponent that we need for each prime. In this way, we can see that \( \mathbb{Z}_{2^3} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_{3} \times \mathbb{Z}_{7} \) is a subgroup of the desired order.

Note that we have used the fact that every cyclic group has a subgroup of order any number that divides its order.
Now you can try proving Theorem 5 (see E8 below).

E8) Prove Theorem 5, using Theorem 4. Also recall that the converse of Lagrange’s theorem is true for cyclic groups.

E9) There are six types of abelian groups, up to isomorphism, of order 108. Prove that

i) two of them have exactly one subgroup of order 3;

ii) two of them have exactly four subgroups of order 3; and

iii) two of them have exactly 13 subgroups of order 3.

Now, do you think that the elementary divisor decomposition is the only way of representing an abelian group as a direct product of its subgroups? Think about this, while considering the following procedure.

Take \( G = \mathbb{Z}_{2^4} \times \mathbb{Z}_{3^3} \times \mathbb{Z}_5 \times \mathbb{Z}_7 \)

Let us write out these prime powers in the following format, one row for each prime base, and ordered from the largest exponent to the smallest, from left to right. So we get,

\[
\begin{array}{cccc}
2^4 & 2^2 & 2 & 1 \\
3^3 & 3 & 1 & 1 \\
5^5 & 5^5 & 5 & 5 \\
7 & 1 & 1 & 1
\end{array}
\]...

Now, the row of powers of 5 in (I) is the longest. To make all the rows of the same length, put 1 in the blank positions. So we now get the following arrangement:

\[
\begin{array}{cccc}
2^4 & 2^2 & 2 & 1 \\
3^3 & 3 & 1 & 1 \\
5^5 & 5^5 & 5 & 5 \\
7 & 1 & 1 & 1
\end{array}
\]...

Using the fact that the direct product is associative and commutative, we can rewrite \( G \) as:

\[
G = \mathbb{Z}_5 \times (\mathbb{Z}_2 \times \mathbb{Z}_3) \times (\mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_5) \times (\mathbb{Z}_{2^3} \times \mathbb{Z}_3 \times \mathbb{Z}_5) \times (\mathbb{Z}_{2^4} \times \mathbb{Z}_3 \times \mathbb{Z}_5) \times (\mathbb{Z}_{2^4} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7) \quad \text{(columnwise, from right to left in Arrangement I above)}
\]

\[
= \mathbb{Z}_5 \times \mathbb{Z}_{10} \times \mathbb{Z}_{1500} \times \mathbb{Z}_{42000} \quad \left( \prod_{i} \mathbb{Z}_{m_i}, \; m_i = \text{product of integers in the } i\text{th column in Arrangement II above} \right)
\]

Now, the orders 5, 10, 1500, 42000 of the successive cyclic groups satisfy 42000 | 1500, 1500 | 42000. So each number divides the succeeding number.

Thus, \( G \) is written in two ways as a direct product, one as per the elementary divisor decomposition, and the other as an alternative form.

Keep this example in mind while considering the following result that gives an alternative way of presenting the structure of an abelian group.

**Theorem 6 (Alternative Structure Theorem)**: Every finite abelian group \( G(\neq \{e\}) \) is isomorphic to a direct product of the form \( \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_t} \), for
some integers \(m_1, m_2, \ldots, m_t\) satisfying \(m_i \geq 2\) for all \(i = 1, \ldots, t\) and \(m_i \mid m_{i+1}\) for \(1 \leq i \leq t - 1\).

Moreover, the integers \(m_1, m_2, \ldots, m_t\) are uniquely determined by \(G\).

**Proof:** Suppose \(G\) is abelian of order \(n = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}\), where the \(p_i\)'s are distinct primes. We can assume that \(G\) is already in the form mentioned in Theorem 4. To express \(G\) in the form we now need, we will undertake the following steps:

**Step 1:** First we group together all the elementary divisors which are powers of the same prime. In this way, we obtain \(k\) lists of integers (one for each \(p_i\)).

**Step 2:** In each of these \(k\) lists, we arrange the integers row-wise in non-increasing order, as done in Arrangement (I) in the example above.

**Step 3:** Among these \(k\) rows, suppose the longest consists of \(t\) integers. Make each of these \(k\) rows of length \(t\) by appending 1 in as many places as required at the end of each list, as in Arrangement (II) in the example above.

**Step 4:** Let \(m_i\) be the product of the integers in the \(i^{th}\) column of this arrangement, \(m_j\) be the product of the integers in the \((t-1)^{th}\) column in each of these lists, and so on.

The ordering of lists in this way ensures that \(m_i \mid m_{i+1}\) for \(1 \leq i \leq t - 1\). Thus, \(G \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_t}\), which is in the form required.

Now, to complete the proof, we need to prove the uniqueness of \(m_1, m_2, \ldots, m_t\). First, note that once \(G\) is represented in the form given in the statement, the elementary divisors of \(G\) are the prime power factors of \(m_1, m_2, \ldots, m_t\). The divisibility relations on the \(m_i\)'s imply that \(m_1\) is the product of the largest of the prime powers among the elementary divisors, \(m_{t-1}\) is the product of the largest of the prime powers among the elementary divisors once the factors of \(m_1\) have been removed, and so on. If \(m_1', m_2', \ldots, m_t'\) are another set of integers that satisfy the statement of the theorem, then we take the prime power factors of these elements and similarly obtain the elementary divisors of \(G\). But from Theorem 4, you know that the elementary divisors of \(G\) are unique. Therefore, the uniqueness of the \(m_i\) in this theorem follows.

The unique representation in Theorem 6 allows us to define the following terms.

**Definition:** Let \(G\) be a finite abelian group, and \(G \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_t}\), with \(m_i \geq 2\) \(\forall i\) and \(m_i \mid m_{i+1}\) \(\forall i = 1, \ldots, t - 1\). The integers \(m_1, m_2, \ldots, m_t\) are called the invariant factors of \(G\). The representation of \(G\) in this form is called the invariant factor decomposition of \(G\).

Thus, in the detailed example before Theorem 6, you have seen that the group
with invariant factors $5, 10, 1500, 42000$, has elementary divisors $2^4, 2^2, 2, 3, 3, 5^3, 5^3, 5, 5, 7$.

Let us consider another example.

**Example 5:** Obtain 3 distinct possible invariant factor decompositions of a group of order $2^2 3^4 5^3$.

**Solution:** In Example 3, you have seen all the possible non-isomorphic abelian groups of order $2^2 3^4 5^3$. Take any 3 of these non-isomorphic decompositions. Let us take the first, fifth and the twelfth listed there.

Consider the elementary divisors in the first one, namely, $2^2, 3^4, 5^3$. Arranging the distinct prime powers, we get only one column since each row here is of length 1:

\[
\begin{align*}
2^2 \\
3^4 \\
5^3
\end{align*}
\]

So $m = 2^2 \times 3^4 \times 5^3 = 40500$ is the only invariant factor, and $\mathbb{Z}_m$ is the corresponding invariant factor decomposition.

Now let us consider the fifth decomposition given in Example 3, namely, $\mathbb{Z}_4 \times \mathbb{Z}_{25} \times \mathbb{Z}_3 \times \mathbb{Z}_{25} \times \mathbb{Z}_5$.

We arrange the distinct prime powers among the elementary divisors as below:

\[
\begin{align*}
2^2 \\
3^3 \\
5^2 \\
5
\end{align*}
\]

We re-present this as

\[
\begin{align*}
2^2 \\
3^3 \\
5^2 \\
5
\end{align*}
\]

Then $m_1 = 1 \times 3 \times 5 = 15$, $m_2 = 2^2 \times 3^3 \times 5^2 = 2700$. So the invariant factor decomposition is $\mathbb{Z}_{15} \times \mathbb{Z}_{2700}$.

Similarly, you can see that $\mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$ has invariant decomposition $\mathbb{Z}_{15} \times \mathbb{Z}_{15} \times \mathbb{Z}_{130}$.

***

If you have followed the discussion so far, then you should be able to solve the following problems.

---

E10) Give the possible elementary divisor decompositions and invariant factor decompositions of an abelian group of order 56.

E11) Find the elementary divisors, and the invariant factor decomposition, of the following groups:

i) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
We have proved the structure theorem of finite abelian groups in two equivalent forms, as stated in Theorem 4 and Theorem 6. Both these theorems are a particular case of what you shall study in the next section.

5.3 FINITELY GENERATED ABELIAN GROUPS

In this section we shall consider a more general class of abelian groups than the one you studied in Sec. 5.2. Towards this end, we shall first discuss what a finitely generated abelian group is and what a free abelian group is. However, before focussing on abelian groups, we will consider what any group which is finitely generated looks like.

5.3.1 Finitely Generated Groups

To start with, recall that for an integer \( n \geq 1 \), \( \mathbb{Z}^n \) denotes the direct product \( \mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z} \). By \( \mathbb{Z}^0 \), we will mean the identity group \{0\}.

Also, recall what a cyclic subgroup of a group is. For instance, consider \( S_5 \), and \( X = \{(1, 2)\} \subseteq S_5 \). Now, look at the intersection of all subgroups of \( S_5 \) that contain \( X \). This is the smallest subgroup of \( S_5 \) that contains \( X \), and you should check that this is \( \{e, (1, 2)\} \), the subgroup generated by \( \{(1, 2)\} \), denoted by \( \langle (1, 2) \rangle \).

More generally, let \( G \) be a group (not necessarily abelian), and \( X \subseteq G, X \neq \emptyset \). Then there is at least one subgroup of \( G \) containing \( X \), namely, \( G \) itself. Consider all the subgroups of \( G \) containing \( X \) and take their intersection. This will be the smallest subgroup of \( G \) that contains \( X \), and is denoted by \( \langle X \rangle \).

**Proposition 1:** Let \( G \) be a group (not necessarily abelian) and \( X \) be a non-empty subset of \( G \). Then
\[
\langle X \rangle = \{a_1^{n_1}a_2^{n_2} \ldots a_k^{n_k} \mid a_i \in X, n_i \in \mathbb{Z} \text{ for all } i = 1, \ldots, k, k \geq 1\},
\]
where the \( a_i \)s are not necessarily distinct.

**Proof:** First of all, you should check that
\[
K = \{a_1^{n_1}a_2^{n_2} \ldots a_k^{n_k} \mid a_i \in X, n_i \in \mathbb{Z} \text{ for all } i, \ldots, k, k \geq 1\}
\]
is a subgroup of \( G \) containing \( X \). Therefore, by definition, \( \langle X \rangle \subseteq K \).

Now, let \( H \) be a subgroup of \( G \) containing \( X \). Then for any \( a_1, \ldots, a_k \in X \), and \( n_1, \ldots, n_k \in \mathbb{Z} \), \( a_1^{n_1}a_2^{n_2} \ldots a_k^{n_k} \in H \). Therefore, \( K \subseteq H \). Hence, by the definition of \( \langle X \rangle \), \( K \subseteq \langle X \rangle \).

Thus, \( K = \langle X \rangle \). \( \blacksquare \)

Note that in the proposition above, \( G \) is any group (not necessarily an abelian group). Also, note that if \( G \) is abelian, then we can take the \( a_i \)s to be distinct.
The proposition above leads us to the following definition.

**Definition:** A subset $X$ of $G$ is said to **generate** $G$ if $G = \langle X \rangle$. In addition, if $X$ is finite, then we say that $G$ is **finitely generated** (f.g., in brief).

So, for example, every cyclic group is finitely generated, as it is generated by a singleton.

Consider some more examples.

**Example 6:** Show that every finite group $G$ is finitely generated, but the converse need not be true.

**Solution:** For any group $G$, $G = \langle G \rangle$ certainly. So, if $G$ is finite, then $G$ will be finitely generated.

For the converse, consider $\mathbb{Z}$. It is finitely generated, as $\mathbb{Z} = \langle 1 \rangle$.

However, $\mathbb{Z}$ is certainly not finite!

***

**Example 7:** Show that $\mathbb{Z} \times \mathbb{Z}$ is finitely generated, and in fact, $\mathbb{Z}^n$ is f.g. for $n \geq 1$.

**Solution:** For any $(n, m) \in \mathbb{Z} \times \mathbb{Z}$, $(n, m) = n(1, 0) + m(0, 1)$, assuming the operation as addition. Thus, $\{(1, 0), (0, 1)\}$ is a generating set for $\mathbb{Z} \times \mathbb{Z}$.

In the same way, $\mathbb{Z}^n$ is finitely generated, as it can be generated by the set of $n$-tuples, $\{(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, 0, \ldots, 1)\}$.

***

**Example 8:** Check whether $\{2\}$ generates $\mathbb{Z}_6$ or not.

**Solution:** Since $1 \neq n \cdot 2$ for any $n \in \mathbb{Z}$, $\mathbb{Z}_6$ is not generated by $\{2\}$.

***

Try the following exercises now.

---

**E12)** Find the subgroup of $\mathbb{Z}_{12}$ generated by

- i) $\{2, 3\}$,
- ii) $\{4, 6\}$,
- iii) $\{8, 10\}$.

**E13)** Is $\mathbb{Z}_8$ generated by $\{4, 5\}$? Give reasons for your answer.

**E14)** If a group $G$ is f.g., is the generating set unique? Why, or why not?

**E15)** If $G_1$ and $G_2$ are f.g. groups, show that $G_1 \times G_2$ is also f.g.

**E16)** Show that $(\mathbb{Q}, +)$ is not finitely generated.

---

In the next-subsection we focus on particular abelian groups that are generated ‘freely’.
5.3.2 Free Abelian Groups

In this sub-section, we will work only with abelian groups, and we shall denote the binary operation in an abelian group $G$ by $+$ instead of the multiplicative notation. So, we will write $na$ instead of $a^n$, if $a \in G$ and $n \in \mathbb{Z}$.

Thus, if $G = \langle X \rangle$. Then, by Proposition 1, given any $g \in G$, there exist $k \geq 1, a_1, a_2, \cdots, a_k \in X, n_1, n_2, \cdots, n_k \in \mathbb{Z}$ such that $g = n_1a_1 + n_2a_2 + \cdots + n_ka_k$. 

...\(8\)

In other words, each $g \in G$ can be written as a $\mathbb{Z}$-linear combination of finitely many elements of $X$, as you just saw in Example 7. In case $X$ has the additional property that the expression of writing any $g \in G$, as a finite $\mathbb{Z}$-linear combination of the elements of $X$ (as given in Equation 8) is unique, then we say that $X$ generates $G$ freely. Let’s understand this concept with some examples.

Example 9: Check whether or not $\mathbb{Z}$ is freely generated by $\{1\}$.

Solution: You already know that $\mathbb{Z} = \langle \{1\} \rangle$. Now, $\{1\}$ has the property that each element $n \in \mathbb{Z}$ can be uniquely written as $n\cdot 1$, i.e., if $n\cdot 1 = m\cdot 1$, then $n = m$. So, $\mathbb{Z}$ is freely generated by $\{1\}$.

***

Here we give an important comment related to this example.

Remark 2: Note that the freely generating set need not be unique. e.g., $\{-1\}$ also generates $\mathbb{Z}$ freely. Thus, $\mathbb{Z}$ has two distinct freely generating sets.

Example 10: Show that $\mathbb{Z} \times \mathbb{Z}$ is freely generated by $\{(1, 0), (0, 1)\}$.

Solution: Suppose $(n, m)$ is any element of $\mathbb{Z} \times \mathbb{Z}$. Then $(n, m) = n(1, 0) + m(0, 1)$. Suppose $(n, m) = n'(1, 0) + m'(0, 1)$ also for $n', m' \in \mathbb{Z}$. Then $(n, m) = (n', m')$. Hence $n = n', m = m'$.

Thus, each $(n, m)$ in $\mathbb{Z} \times \mathbb{Z}$ can be uniquely written as $(n, m) = n(1, 0) + m(0, 1)$, i.e., the coefficients $n$ and $m$ in this $\mathbb{Z}$-linear combination are unique. Hence, $\mathbb{Z}^2$ is freely generated by $\{(1, 0), (0, 1)\}$.

***

Example 11: $\mathbb{Z}/3\mathbb{Z}$ is generated by $\{\bar{1}\}$, but it is not freely generated by $\{\bar{1}\}$.

Solution: Since the elements of $\mathbb{Z}/3\mathbb{Z}$ are $\{0, \bar{1}, 2\bar{1}\}, \{\bar{1}\}$ generates $\mathbb{Z}/3\mathbb{Z}$. Also, as $\bar{2} = 2\bar{1} = 5\bar{1}$ and $2 \neq 5$, $\{\bar{1}\}$ does not generate it freely.

***

These examples lead us to the following definition.

Definition: An abelian group $G$ is called free abelian if there is a non-empty subset $X$ of $G$ such that $G$ is freely generated by $X$. In such a situation, $X$ is called a basis for $G$. 
As you have seen in Example 10, \( \mathbb{Z} \times \mathbb{Z} \) is a free abelian group and \{(1, 0), (0, 1)\} is a basis. Similarly, \( \mathbb{Z}^n \) is a free abelian group with a basis \{(1, 0, ..., 0), (0, 1, ..., 0), ..., (0, 0, ..., 1)\}. Also, note that a free abelian group can have several different bases. For example, \( \mathbb{Z} \) is free abelian with basis \{1\}, or with basis \{-1\}.

Why don’t you solve the following exercises now, to help you develop your understanding of a free abelian group?

E17) Show that if \( G \) and \( G' \) are free abelian groups, then \( G \times G' \) is a free abelian group.

E18) If \( G \) is a free abelian group with a basis consisting of \( n \) elements, then show that \( G \) is isomorphic to \( \mathbb{Z}^n \).

Let’s try and probe free abelian groups some more. To start with, consider the following result that you have actually applied in some of the examples above.

**Theorem 7:** Let \( X \) be a subset of an abelian group \( G \). Then the following are equivalent:

(i) \( X \) generates \( G \) freely.

(ii) \( X \) generates \( G \), and \( n_1 x_1 + n_2 x_2 + \cdots + n_k x_k = 0 \) if and only if \( n_1 = n_2 = \cdots = n_k = 0 \), where \( x_i \in X \), \( n_i \in \mathbb{Z} \) for \( i = 1, \ldots, k \).

**Proof:** To prove this, we need to prove \((i) \Rightarrow (ii)\) and \((ii) \Rightarrow (i)\).

\((i) \Rightarrow (ii)\) From (i), we know that \( X \) generates \( G \). Now, suppose \( n_1 x_1 + n_2 x_2 + \cdots + n_k x_k = 0 \) for some \( x_i \in X \) and \( n_i \in \mathbb{Z} \). Then we have two ways to write 0 as a \( \mathbb{Z} \)-linear combination of elements of \( X \), namely,

\[ 0 = n_1 x_1 + n_2 x_2 + \cdots + n_k x_k \quad \text{and} \quad 0 = 0 x_1 + 0 x_2 + \cdots + 0 x_k. \]

But, as \( X \) generates \( G \) freely, any \( g \in G \) must be uniquely written as a \( \mathbb{Z} \)-linear combination of elements of \( X \). Thus, \( n_i = 0 \) for all \( i \), and hence (i) implies (ii).

\((ii) \Rightarrow (i)\) Let \( g \in G \). Since \( X \) generates \( G \), we see that \( g \) can be written in the form \( g = n_1 x_1 + n_2 x_2 + \cdots + n_k x_k \) for \( n_i \in \mathbb{Z} \). Now, suppose \( g \) has another such expression in terms of a \( \mathbb{Z} \)-linear combination of elements of \( X \), say \( g = m_1 x'_1 + m_2 x'_2 + \cdots + m_s x'_s \), with \( m_i \in \mathbb{Z} \), \( x'_i \in X \forall i = 1, \ldots, s \), and the \( x'_i \)'s may or may not be distinct from the \( x_i \)'s. Let us consider the set \( \{x'_1, \ldots, x'_s, x'_r, \ldots, x'_r\} \). After re-ordering the \( x_i \)'s and \( x'_i \)'s, if necessary, assume that \( x_i = x'_1, x_2 = x'_2, \ldots, x_r = x'_r \) and the rest of the \( x_i \)'s and \( x'_i \)'s are distinct.

Then \( g = n_1 x_1 + \cdots + n_r x_r = m_1 x'_1 + m_2 x'_2 + \cdots + m_r x'_r \)

\[ \Rightarrow (n_1 - m_1)x_1 + \cdots + (n_r - m_r)x_r + \cdots + n_j x_j - m_j x'_j + \cdots - m_r x'_r = 0. \]

\[ \Rightarrow n_i = m_i \forall i = 1, \ldots, r \quad \text{and} \quad n_j = 0 = m_k \forall j = \ell + 1, \ldots, r; k = \ell + 1, \ldots, s \quad (\text{by our hypothesis (ii)}). \]

\[ \Rightarrow g = n_1 x_1 + \cdots + n_r x_r = m_1 x'_1 + \cdots + m_r x'_r \quad \text{and} \quad n_i = m_i \forall i = 1, \ldots, \ell. \]

Thus, the coefficients are unique, and (i) follows.
This theorem helps us check whether a given set is a basis of a given abelian group or not. Consider an example.

**Example 12:** Check whether or not \( \mathbb{Z}/n\mathbb{Z} \) is free abelian, \( n \geq 2 \).

**Solution:** You know that \( \{1\} \) generates \( \mathbb{Z}/n\mathbb{Z} \). You also know that \( n \cdot 1 = 0 \), with \( n \neq 0 \). Hence, by Theorem 7, \( \{1\} \) does not generate \( \mathbb{Z}/n\mathbb{Z} \) freely. Along the same lines you can check that no generating set will generate \( \mathbb{Z}/n\mathbb{Z} \) freely.

***

You should do the following exercises now.

---

E19) Show that a non-trivial finite abelian group cannot be free abelian.

E20) Can a singleton be a basis of \( \mathbb{Z} \times \mathbb{Z} \)? Justify your answer.

---

As you have seen earlier, a free abelian group can have many bases. For example, \{\( (1, 0)\), \( (0, 1) \)\} is a basis of \( \mathbb{Z} \times \mathbb{Z} \).

Another basis is \{\( (1,1)\), \( (1,2) \)\} because each \( (n,m) \in \mathbb{Z} \times \mathbb{Z} \) can be uniquely written as \( (n,m) = (2n-m)(1,1) + (m-n)(1,2) \).

Note that both these bases have the same number of elements. In fact, any two bases of a free abelian group must have the same number of elements. We will now prove this result only in the case that \( G \) has a finite basis.

**Theorem 8:** Let \( G \) be a non-trivial free abelian group with a finite basis \( B \). Then every basis of \( G \) is finite, with cardinality \( |B| \).

**Proof:** Let \( B = \{x_1, x_2, \ldots, x_r\} \) be a basis of \( G \). Then \( G \) is isomorphic to \( \mathbb{Z}^r \), as you have shown in E18.

Let \( 2G = \{2g \mid g \in G \} \). Then \( 2G \) is a subgroup of \( G \), and \( G/2G = \mathbb{Z}^r/2\mathbb{Z}^r = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2 \) ( \( r \) copies). Thus, \( o(G/2G) = 2^r \).

So, \( r = \log_2[o(G/2G)] \).

Similarly, if \( B' = \{x'_1, \ldots, x'_s\} \) is another basis of \( G \), then \( s = \log_2[o(G/2G)] = r \).

Hence, **any finite basis** must have the same number of elements.

Now the question arises: can \( G \) have an infinite basis? Suppose it can. Let \( Y \) be an infinite basis for \( G \). Consider a subset of \( Y \) consisting of \( s \) elements, say \( \{y_1, y_2, \ldots, y_s\} \), where \( s > r \). Let \( H \) be the subgroup of \( G \) generated by \( \{y_1, y_2, \ldots, y_s\} \), and let \( K \) be the subgroup of \( G \) generated by the remaining elements of \( Y \). Then \( G = \langle Y \rangle \simeq H \times K \) and \( G/2G = H \times K/(2H \times 2K) = (H/2H) \times (K/2K) \).

Since \( o(H/2H) = 2^r \), we see that \( o(G/2G) \geq 2^r \). But \( o(G/2G) = 2^r \). This is a contradiction as \( s > r \). Hence our assumption is wrong, and \( G \) cannot have an infinite basis. 

\[ \square \]
You have seen why all bases of a free abelian group with a finite basis must have the same cardinality. (In fact, this is true even if the group has an infinite basis, but we shall not be proving this case here.) In view of this, the following definition makes sense.

**Definition:** The rank of a finitely generated free abelian group $G$ is defined to be the number of elements in a basis of $G$.

For example, $\mathbb{Z}$ is of rank one. More generally, $\mathbb{Z}^r$ is of rank $r$ for $r \geq 1$. So, e.g., the solution of E20 follows immediately from Theorem 8.

Now, consider a subgroup of a free abelian group $G$. Must it be free abelian? If so, will its rank have any relationship to the rank of $G$? These questions are addressed in the following theorem.

**Theorem 9:** Let $G$ be a free abelian group of rank $n \geq 1$ and let $H$ be a non-trivial subgroup of $G$. Then $H$ is free abelian of rank $\leq n$. Furthermore, there exists a basis $\{x_1, x_2, \ldots, x_n\}$ of $G$, and $s$ positive integers $d_1, d_2, \ldots, d_s$, such that $d_i|d_{i+1}$ for $i = 1, 2, \ldots, s - 1$ and $\{d_1x_1, d_2x_2, \ldots, d_sx_s\}$ is a basis of $H$.

**Proof:** We will show that $H$ has a basis of the described form. This will, of course, show that $H$ is free abelian of rank at most $n$.

Suppose $Y = \{y_1, y_2, \ldots, y_n\}$ is a basis for $G$. Then any element $h \in H$ can be expressed in the form $k_1y_1 + k_2y_2 + \cdots + k_ny_n$, where $k_1, \ldots, k_n \in \mathbb{Z}$. Moreover, if $h \neq 0$, then some $k_i \neq 0$. Among all the bases of $G$, select a basis $Y_1$ that yields the non-zero coefficient of least magnitude $|k_i|$ over all the non-zero elements of $H$ written as $\mathbb{Z}$-linear combinations of elements of $Y_1$. By re-numbering the elements of $Y_1$, if necessary, we can assume that there is $w_1 \in H$ such that $w_1 = d_1y_1 + d_2y_2 + \cdots + d_ny_n$, where $d_1 > 0$, and $d_1$ is the minimal attainable coefficient as just described.

Using the division algorithm, write $k_j = d_1q_j + r_j$, where $q_j \in \mathbb{Z}$ and $0 \leq r_j < d_1$ for $j = 2, \ldots, n$.

Then $w_1 = d_1(y_1 + q_2y_2 + \cdots + q_ny_n) + r_2y_2 + \cdots + r_ny_n$. \hfill \ldots(9)

Now let $x_1 = y_1 + q_2y_2 + \cdots + q_ny_n$. Then $\{x_1, y_2, \ldots, y_n\}$ is also a basis for $G$. From Equation (9) and our choice of $Y_1$ for minimal coefficient $d_1$, we see that $r_1 = r_2 = \cdots = r_n = 0$, otherwise we get a coefficient of lesser value than $d_1$, a contradiction. Thus, $w_1 = d_1x_1$, and hence $d_1x_1 \in H$.

Now consider the basis $\{x_1, y_2, \ldots, y_n\}$ of $G$. You have seen that any element of $H$ can be expressed in the form $h_1x_1 + k_2y_2 + \cdots + k_ny_n$, $h_1, k_2, \ldots, k_n \in \mathbb{Z}$. Since $d_1x_1 \in H$, we can subtract a suitable multiple of $d_1x_1$ and then use the minimality of $d_1$ to see that $h_1$ is a multiple of $d_1$, along the lines we followed to reach Equation 9.

Moreover, it follows that $k_2y_2 + \cdots + k_ny_n \in H$.

Among all such bases $\{x_1, y_2, \ldots, y_n\}$, we choose $Y_2 = \{y_2, \ldots, y_n\}$ that leads to some $k_i \neq 0$ of minimal magnitude.
It is possible that all \( k_i \) are zero for all bases, in which case, \( H \) is generated by \( d_1x_1 \) and we are done.

Otherwise, re-numbering the elements of \( Y_2 \), we can assume that there is \( w_2 \in H \) such that
\[
 w_2 = d_2y_2 + k_3y_3 + \cdots + k_ny_n,
\]
where \( d_2 > 0 \) and \( d_2 \) is minimal as described above.

Exactly as in the procedure done earlier, we can modify our basis from \( Y_2 = \{x_1, y_2, \ldots, y_n\} \) to a basis \( \{x_1, x_2, y_3, \ldots, y_n\} \) for \( G \), where \( d_1x_1, d_2x_2 \in H \). Writing \( d_2 = dq + r \) for \( 0 \leq r < d_1 \) and \( q \in \mathbb{Z} \), we see that
\[
\{x_1 + qx_2, x_2, y_3, \ldots, y_n\}
\]
is a basis for \( G \) and \( d_1x_1 + d_2x_2 = d_1(x_1 + qx_2) + rx_2 \) is in \( H \). By our minimal choice of \( d_1 \), we have \( r = 0 \), so \( d_1 \) divides \( d_2 \).

We now consider all bases of the form \( \{x_1, x_2, y_3, \ldots, y_n\} \) for \( G \) and examine elements of \( H \) of the form \( k_3y_3 + \cdots + k_ny_n \). You must have realised the pattern by now. The process continues until we obtain a basis \( \{x_1, x_2, \ldots, x_s, y_{s+1}, \ldots, y_n\} \), till the only element of \( H \) of the form \( k_{s+1}y_{s+1} + \cdots + k_ny_n \) is zero, i.e., all \( k_i \) are zero. We then let
\[
x_{s+1} = y_{s+1}, \ldots, x_n = y_n
\]
and obtain a basis for \( G \) of the form described in the statement of the theorem.

What the theorem above says is that every subgroup of a free abelian group of rank \( n \) looks structurally like \( \mathbb{Z}^r \) for some \( r \leq n \). Let us consider an example.

**Example 13:** Show, by example, that it is possible for a proper subgroup of a free abelian group of finite rank \( r \) also to have rank \( r \).

**Solution:** Consider \( \mathbb{Z} \). This is free abelian of rank one. Now consider \( 3\mathbb{Z} \). This is also free abelian, generated by \( \{3\} \), and hence of rank one.

***

**Example 14:** Show that \( P_n = \{a_0 + a_1 + a_2x^2 + \cdots + a_nx^n | a_i \in \mathbb{Z}\} \) is a f.g. free abelian group of rank \( n+1 \).

**Solution:** Consider \( X = \{1, x, \ldots, x^n\} \). You know that \( X \) generates \( P_n \). Also, if \( \sum_{i=0}^{n} a_ix^i = \sum_{i=0}^{n} b_ix^i \), then \( a_i = b_i \forall i \neq 1, \ldots, n \). Hence the result.

***

Let us now look at the order of the elements of an abelian group. You know that if \( G \) is a free abelian group with a basis \( X \), then \( nx = 0 \Rightarrow n = 0 \forall x \in X \). However, the abelian group \( \mathbb{Z}_2 \times \mathbb{Z} \) has an element \( (1, 0) \) of order 2 and an element \( (0, 1) \) of no finite order. This leads us to the following definition.

**Definitions:**
1) Let \( G \) be a group. An element of \( G \) with finite order is called a **torsion element** of \( G \).
2) The set of torsion elements of an **abelian group** \( G \) is a subgroup of \( G \), called the **torsion subgroup** of \( G \). This is denoted by \( \text{Tor}(G) \).
3) An abelian group \( G \) is called a **torsion group** if \( \text{Tor}(G) = G \), and \( G \) is called a **torsion-free group** if \( \text{Tor}(G) = \{0\} \).
For example, $\text{Tor}(\mathbb{Z}_2 \times \mathbb{Z}) = \mathbb{Z}_2 \times \{0\} \cong \mathbb{Z}_2$ and $\text{Tor}(\mathbb{Z}) = \{0\}$.

Thus, $\mathbb{Z}$ is torsion-free.

**Example 15:** If $G$ is a finite group, find $\text{Tor}(G)$.

**Solution:** Since every element of $G$ is of finite order, $\text{Tor}(G) = G$. Hence $G$ is a torsion group.

***

Again, it is time for you to check your understanding of what you have studied so far.

---

**E21)** Mark each of the following true or false. Give reasons for your choices.

i) These exists a free abelian group of every positive integer rank.

ii) If $X$ is a basis for a free abelian group $G$ and $X \subseteq Y \subseteq G$, then $Y$ is a basis for $G$.

iii) If $K$ is a non-trivial subgroup of a finitely generated free abelian group, then $K$ is free abelian.

iv) If $K$ is a non-trivial subgroup of a finitely generated free abelian group, then $G/K$ is free abelian.

v) Any two free abelian groups of the same finite rank are isomorphic.

**E22)** i) Show that $\text{Tor}(G)$ is a subgroup of $G$, if $G$ is abelian.

ii) If $G$ is not abelian, will $\text{Tor}(G)$ still be a subgroup of $G$? Why, or why not?

**E23)** Show that the torsion subgroup of a finitely generated free abelian group is $\{0\}$.

**E24)** Show that $\text{Tor}(G_1 \times G_2) = \text{Tor}(G_1) \times \text{Tor}(G_2)$, where $G_1$ and $G_2$ are two abelian groups.

**E25)** Suppose $G$ is a finite abelian group and $F$ is a finitely generated free abelian group. Show that $G \times F$ is a finitely generated abelian group, and its torsion subgroup is isomorphic to $G$.

**E26)** Find the orders of the torsion subgroups of $\mathbb{Z}_4 \times \mathbb{Z} \times \mathbb{Z}_3$ and $\mathbb{Z}_{12} \times \mathbb{Z} \times \mathbb{Z}_{12}$.

---

We now have all the tools in hand to understand what a f.g. abelian group looks like, in general.

### 5.4 STRUCTURE THEOREMS

In Sec.5.2 you studied the structure of finite abelian groups. In this section, you will study the proof and applications of the following structure theorem for finitely generated abelian groups, which is a generalisation of the invariant factor decomposition of finite abelian groups.
Theorem 10 (Structure Theorem for Finitely Generated Abelian Groups):
Let $G$ be a finitely generated abelian group. Then

(i) $G \simeq \mathbb{Z}^{t} \times \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_t}$, for some integers $r$, $m_1,m_2,...,m_t$ satisfying $r \geq 0$, $m_i \geq 2$ for all $i$, and $m_i | m_{i+1}$ for $1 \leq i \leq t-1$.

(ii) The integers $r$, $m_1,m_2,...,m_t$, satisfying the expression in (i) above, are uniquely determined by $G$.

Proof: Let $G$ be generated by the set $\{g_1,g_2,\ldots,g_n\}$. Let $F = \mathbb{Z}^n$. Consider the map $\psi : F \to G$ given by $\psi(a_1,a_2,\ldots,a_n) = a_1g_1 + a_2g_2 + \cdots + a_ng_n$. You can check that $\psi$ is a well-defined homomorphism and is surjective. Let $H = \ker \psi$. By Theorem 9, there is a basis $\{x_1,x_2,\ldots,x_n\}$ of $F$ such that $\{d_1x_1,\ldots,d_nx_n\}$ is a basis for $H$, where $d_i$ divides $d_{i+1}$ for $1 \leq i \leq n-1, s \leq n$. Consequently, $G \simeq F/H = (\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z})/(d_1\mathbb{Z} \times d_2\mathbb{Z} \times \cdots \times d_l\mathbb{Z}) \times \{0\} \times \cdots \times \{0\}$

It is possible that $d_s = 1$, in which case $Z_{d_i} = \{0\}$ and can be dropped (upto isomorphism) from this product. Similarly, $d_i$ may be dropped if it is 1, and so on. If $m_i$ is the first $d_i > 1$, $m_{i+1}$ is the next, and so on, then $G$ is isomorphic to a direct product of cyclic groups of the form given in the theorem, with $r = n - s$. Hence (i) is proved. (Note that if $n = s$, $r = 0$.)

For showing the uniqueness, suppose $G'$ is in the form given in (i) and $G' \simeq \mathbb{Z}^{r'} \times \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_t}$ also, for some integers $r',m_1',m_2',\ldots,m_t'$ satisfying $r' \geq 0$, $m'_{i} \geq 2$ for all $i$ and $m'_{i} | m'_{i+1}$ for all $i = 1, \ldots, b$.

Consider the subgroup $\text{Tor}(G)$ of $G$. By E25, you know that $\text{Tor}(G) \simeq \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_t}$ and $\text{Tor}(G') \simeq \mathbb{Z}_{m_1'} \times \mathbb{Z}_{m_2'} \times \cdots \times \mathbb{Z}_{m_t'}$.

Since $\text{Tor}(G)$ is finite abelian, by the uniqueness of its invariant factors we see that $t = b$, and $m_i = m_{i}'$ for all $i = 1, \ldots, t$.

Furthermore, as $G/\text{Tor}(G) \simeq \mathbb{Z}^{r'}$ and $G'/\text{Tor}(G) \simeq \mathbb{Z}^{r'}$, it follows by Theorem 8 that $r = r'$. This proves the assertion (ii) and completes the proof of Theorem 10.

In view of the uniqueness in Theorem 10, the following definitions make sense.

Definitions: For a finitely generated abelian group $G$,

1) the integer $r$ in this decomposition is called the **free rank**, or **Betti number**, of $G$.

2) the integers $m_1,m_2,\ldots,m_t$ are called the **invariant factors** of $G$.

3) the description of $G$ in the form given is called the **invariant factor decomposition** of $G$.
For instance, the free rank of a free abelian group is the same as its rank. If it is of rank \( n \), then its invariant factor decomposition is \( \mathbb{Z}^n \).

The following theorem is an alternative form in which the structure of a f.g. abelian group can be given, and it is a generalisation of Theorem 4.

**Theorem 11 (Elementary Divisor Decomposition of a Finitely Generated Abelian Group):** Let \( G \) be a finitely generated abelian group. Then

\[
G = \mathbb{Z}^r \times \mathbb{Z}_{q_1^{e_1}} \times \mathbb{Z}_{q_2^{e_2}} \times \cdots \times \mathbb{Z}_{q_s^{e_s}},
\]

where \( r \geq 0 \) is an integer and \( q_1^{e_1}, q_2^{e_2}, \ldots, q_s^{e_s} \) are positive powers of primes which may not be distinct. Moreover, \( r, q_1^{e_1}, q_2^{e_2}, \ldots, q_s^{e_s} \) are uniquely determined by \( G \).

**Proof:** Let the invariant factor decomposition of \( G \) be

\[
G = \mathbb{Z}^r \times \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t}, \quad r \in \mathbb{N}, \quad m_1, \ldots, m_t \in \mathbb{Z}.
\]

Now, we can decompose each cyclic group \( \mathbb{Z}_{m_i} \) into a direct product of cyclic groups of prime power order. This way, we can express \( G \) in the form required in the statement.

The uniqueness of \( r \) and the prime powers can be proved by proceeding as in the proof of part (ii) of Theorem 10. This completes the proof.

Consider an example.

**Example 16:** Find the Betti number, and the invariant factors of,

\[
G = \mathbb{Z}_6 \times \mathbb{Z}_{14} \times \mathbb{Z}_{15} \times \mathbb{Z}_7.
\]

**Solution:** Here the Betti number is 7.

Since \( G = (\mathbb{Z}_2 \times \mathbb{Z}_3) \times (\mathbb{Z}_2 \times \mathbb{Z}_7) \times (\mathbb{Z}_3 \times \mathbb{Z}_5) \times \mathbb{Z}_7 \), by arranging the powers of the primes we get \( G = \mathbb{Z}_6 \times \mathbb{Z}_{210} \times \mathbb{Z}_7 \). Thus, the invariant factors of \( G \) are 6, 210.

***

Try some exercises now.

---

E27) Find the Betti number, and invariant factors, of the group

\[
\mathbb{Z} \times \mathbb{Z}_6 \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_{12} \times \mathbb{Z}_{10}.
\]

Also write the elementary divisor decomposition of this group.

E28) What is the Betti number of a finite abelian group?

E29) Is it true that any two finitely generated abelian groups with the same Betti number are isomorphic? If yes, prove this. If not, write the necessary and sufficient conditions for two finitely generated abelian groups to be isomorphic.

E30) Let \( G \) be a finitely generated abelian group and \( H \) be a subgroup of \( G 

i) Is \( G/H \) a finitely generated abelian group?

ii) If we assume that \( G \) is a free abelian group, is \( G/H \) free abelian? Justify your answers.
With this we come to the end of our discussion on the structure of abelian groups. Let us take a brief look at what you have studied in this unit.

5.5 SUMMARY

In this unit, we have discussed the following points.

1. The direct product of groups, or of subgroups, and their properties.

2. The proof of the Structure Theorem for Finite Abelian Groups, namely, a finite abelian group \( G \) can be written in the form \( \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \cdots \times \mathbb{Z}_{p_r^{e_r}} \) (elementary divisor decomposition), or as \( \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_i} \) with \( m_i \geq 2 \) and \( m_i | m_{i+1}, \forall i \) (invariant factor decomposition).

3. Applying the structure theorem for finite abelian groups to obtain all possible abelian groups, up to isomorphism, of a given order.

4. The proof of the converse of Lagrange’s theorem for finite abelian groups.

5. The definition, and examples, of finitely generated groups.

6. What a free abelian group is, its rank and its properties.

7. i) The proof of the Structure Theorem for Finitely Generated Abelian Groups, namely, any finitely generated abelian group \( G \) can be written in the form \( \mathbb{Z}^r \times \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_i} \) with \( m_i \geq 2, \forall i \) and \( r \geq 0 \). \( r \) is the rank, or Betti number, of \( G \), and the \( m_i \) are the invariant factors of \( G \).

ii) The proof of the Alternate Structure Theorem, i.e., the Elementary Divisor Decomposition of a Finitely Generated Abelian Group. This states that any finitely generated abelian group \( G \) can be written in the form \( \mathbb{Z}^r \times \mathbb{Z}_{q_1^{e_1}} \times \cdots \times \mathbb{Z}_{q_s^{e_s}} \), where \( r \geq 0 \) is an integer, \( q_1, q_2, \ldots, q_s \) are primes which may not be distinct. Moreover, \( r, q_1^{e_1}, q_2^{e_2}, \ldots, q_s^{e_s} \) are uniquely determined by \( G \).

8. Obtaining the rank, invariant factors and elementary divisors of any given finitely generated abelian group.

5.6 SOLUTIONS / ANSWERS

E1) Let \( G_1 \) and \( G_2 \) be abelian groups of order \( p_1^{n_1}p_2^{n_2} \cdots p_k^{n_k} \) and \( \theta : G_1 \to G_2 \) be the isomorphism. For \( 1 \leq i \leq r \), let \( \theta_i \) be the restriction of \( \theta \) to \( G_1(p_i) \). You should check that \( \theta_i \) is a 1-1 homomorphism, and \( \theta_i(G_1(p_i)) \) is a subgroup of \( G_2 \). Also, \( \theta \) being 1-1, \( |\theta_i(G_1(p_i))| = |G_1(p_i)| = p_i^{n_i} \), and hence \( G_2(p_i) = \theta_i(G_1(p_i)) \) as the Sylow \( p_i \) subgroup of \( G_2 \) is unique. Thus, \( \theta_i \) is a 1-1 onto mapping from \( G_1(p_i) \) to \( G_2(p_i) \), and hence an isomorphism from \( G_1(p_i) \) to \( G_2(p_i) \).
Conversely, if \( G_1(p_i) = G_2(p_i) \) \( \forall i = 1, \ldots, k \), then
\[
G_1 \cong \prod_i G_1(p_i) \cong \prod_i G_2(p_i) \cong G_2.
\]

E2) We proceed by induction on \( r \). When \( r = 1 \), \(|G| = p \). Then \( G \cong H_1 \) and \( G \cong K_1 \), so \( m = n = 1 \) and \(|H_i| = |K_i|\).

Now suppose that the statement is true for all abelian groups of order less than \( p^s \), for some \( s \in \mathbb{N} \). For any abelian group \( L \), \( L^p = \{ x^p | x \in L \} \) is a subgroup of \( L \). Further, if \( L \) is finite then \(|L/L^p| = p \). Also \( G \cong H_1 \times H_2 \times \cdots \times H_m \) implies that \( G^p \cong H_1^p \times H_2^p \times \cdots \times H_m^p \), where \( m' \) is the largest integer \( i \) such that \(|H_i| > p \). Similarly, \( G \cong K_1 \times K_2 \times \cdots \times K_n \) implies that \( G^p \cong K_1^p \times K_2^p \times \cdots \times K_n^p \), where \( n' \) is the largest integer \( j \) such that \(|K_j| > p \). Since \(|G^p| < |G|\), by induction we have \( m' = n' \) and 
\[
|H_i^p| = |K_i^p| \text{ for } i = 1, 2, \ldots, m'.
\]

All that remains to be proved is that the number of \( H_i \)'s of order \( p \) equals the number of \( K_i \)'s of order \( p \); that is, we must prove that \( n - n' = m - m' \). This follows from the fact that
\[
|H_1| |H_2| \cdots |H_m| p^{m-m'} = |G| = |K_1||K_2| \cdots |K_n| p^{n-n'}, m' = n' \text{ and } |H_i| = |K_i| \text{ for } 1 \leq i \leq m'.
\]

E3) The elementary divisors of \( G \cong \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_{11} \) are \( 5, 5, 11^1 \).

Since \( \mathbb{Z}_{55} \cong \mathbb{Z}_5 \times \mathbb{Z}_{11}, \mathbb{Z}_{55} \times \mathbb{Z}_{55} \cong \mathbb{Z}_5 \times \mathbb{Z}_{11} \times \mathbb{Z}_5 \times \mathbb{Z}_{11} \times \mathbb{Z}_5 \times \mathbb{Z}_{11} \times \mathbb{Z}_5 \).

Its elementary divisors are \( 5, 5, 5, 11, 11 \). These are not the same as those of \( G \).

E4) i) \( 105 = 3 \cdot 5 \cdot 7 \). Therefore, looking at the algorithm given before the exercise, \( \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \) is the only abelian group of order 105. Note that \( \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_{105} \).

ii) \( 270 = 2^1 \cdot 3^3 \cdot 5^1 \). Therefore, looking at the partitions of 1, 3, 1, it follows that the non-isomorphic abelian groups of order 270 are \( \mathbb{Z}_2 \times \mathbb{Z}_{27} \times \mathbb{Z}_5, \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_5, \) and \( \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \).

iii) \( 9801 = 3^4 \cdot 11^2 \). Now, the partitions of the exponents are
\[
\begin{align*}
&1 + 3 \quad 1 + 1 \\
&1 + 1 + 2 \\
&2 + 2 \\
&1 + 1 + 1 + 1
\end{align*}
\]

Therefore, the required non-isomorphic abelian groups are \( \mathbb{Z}_{63} \times \mathbb{Z}_{21}, \mathbb{Z}_3 \times \mathbb{Z}_{27} \times \mathbb{Z}_{121} \).
Special Groups and Semigroups

\[ Z_3 \times Z_3 \times Z_3 \times Z_{121}, \]
\[ Z_9 \times Z_9 \times Z_{121}, \]
\[ Z_3 \times Z_3 \times Z_3 \times Z_3 \times Z_{121}, \]
\[ Z_6 \times Z_{11}, \]
\[ Z_3 \times Z_{27} \times Z_{11} \times Z_{11}, \]
\[ Z_3 \times Z_3 \times Z_3 \times Z_4 \times Z_{11} \times Z_{11}, \]
\[ Z_9 \times Z_9 \times Z_{11} \times Z_{11}, \]
\[ Z_3 \times Z_3 \times Z_3 \times Z_3 \times Z_{11} \times Z_{11}. \]

E5) i) The smallest positive integer \( n \) such that there are exactly two non-isomorphic abelian groups of order \( n \) is \( n = 4 \). This is because for \( n = 2, 3 \), the groups of order \( n \) are cyclic, and hence, unique up to isomorphism. For \( n = 4 \), there are two non-abelian groups of order \( n \), namely \( Z_4 \) and \( Z_2 \times Z_2 \).

ii) The smallest positive integer \( n \) such that there are exactly three non-abelian abelian groups of order \( n \) is \( n = 8 \). This is because for \( n = 2, 3, 5, 7 \), the groups of order \( n \) are cyclic, and hence, unique up to isomorphism. For \( n = 4 \), there are two non-abelian groups of order \( n \), as shown in (i) above. For \( n = 6 \), there is a unique abelian group of order \( n \), i.e., \( Z_2 \times Z_3 \times Z_2 \times Z_3 \). For \( n = 8 \), there are three non-isomorphic abelian groups, namely, \( Z_8, Z_4 \times Z_2, Z_2 \times Z_2 \times Z_2 \).

E6) In both the cases, there is a unique group since the exponents of the primes are 1.

E7) \( 120 = 2^3 \times 3 \times 5 \). Therefore, the groups of order 120 are \( Z_8 \times Z_3 \times Z_5, Z_2 \times Z_4 \times Z_3 \times Z_5, Z_2 \times Z_4 \times Z_3 \times Z_5 \) and \( Z_2 \times Z_4 \times Z_3 \times Z_5 \). The first group has only one element of order 2, namely, \((4,0,0)\). The second group has precisely three elements of order 2, namely, \((1,0,0,0), (1,2,0,0), (0,2,0,0)\). The third group has 7 elements of order 2, namely, \((x,y,z,0,0)\), where \((x,y,z) \in Z_2 \times Z_3 \times Z_5 \setminus \{(0,0,0)\}\). Therefore, the required group is \( Z_2 \times Z_4 \times Z_3 \times Z_5 \). Therefore, along the same lines as in Example 4, you can check that if \( G \) has precisely 3 elements of order 2, then \( G \cong Z_2 \times Z_4 \times Z_3 \times Z_5 \).

E8) By Theorem 4, you can assume that \( G = Z_{q_1^{e_1}} \times Z_{q_2^{e_2}} \times \ldots \times Z_{q_s^{e_s}} \), where \( q_1, q_2, \ldots, q_s \) are primes (not necessarily distinct) and \( e_i \geq 1 \) for all \( i \). Since \( |G| = q_1^{f_1} q_2^{f_2} \ldots q_s^{f_s} \), and \( m \) divides \( |G| \), we must have \( m = q_1^{f_1} q_2^{f_2} \ldots q_s^{f_s} \), where \( 0 \leq f_i \leq e_i \) for all \( i \). Now if \( \langle a_i \rangle \) is a subgroup of \( Z_{q_i^{e_i}} \) of order \( q_i^{f_i} \) (this is possible since the
converse of Lagrange’s theorem is true for cyclic groups), then \( \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_n \rangle \) is a subgroup of \( G \) of order \( m \).

E9) There are 6 types of abelian groups of order \( 108 = 2^3 \cdot 3^3 \), namely,

i) \( \mathbb{Z}_4 \times \mathbb{Z}_{27} \)

ii) \( \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27} \)

iii) \( \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \)

iv) \( \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_y \)

v) \( \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \)

vi) \( \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \)

So, the number of elements of order 3 in the groups (i)–(vi) is given as in the following table:

<table>
<thead>
<tr>
<th>Group</th>
<th>Number of elements of order 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>(i)</td>
<td>2 ([\text{i.e.,} (\bar{0}, \bar{9}), (\bar{0}, 18)])</td>
</tr>
<tr>
<td>(ii)</td>
<td>2 ([\text{i.e.,} (\bar{0}, \bar{0}, \bar{9}), (\bar{0}, \bar{0}, 18)])</td>
</tr>
<tr>
<td>(iii)</td>
<td>8 ([\text{i.e.,} (\bar{0}, \bar{x}, \bar{y}), \bar{x} \in \mathbb{Z}_3, \bar{y} \in 3\mathbb{Z}_9, \text{both } \bar{x} \text{ and } \bar{y} \text{ not zero simultaneously.}])</td>
</tr>
<tr>
<td>(iv)</td>
<td>8</td>
</tr>
<tr>
<td>(v)</td>
<td>26 ([\text{i.e.,} (\bar{0}, \bar{x}, \bar{y}, \bar{z}), \bar{x}, \bar{y}, \bar{z} \in \mathbb{Z}_3, \text{not all zero simultaneously.}])</td>
</tr>
<tr>
<td>(vi)</td>
<td>26</td>
</tr>
</tbody>
</table>

Now recall that if \( H \) is a subgroup of order 3 in a group \( G \), then \( H \) is cyclic and is generated by an element of order 3. Furthermore, \( H \) has precisely 2 elements of order 3 and both of them generate it. Consequently, groups (i) and (ii) have unique subgroups of order 3; groups (iii) and (iv) have four subgroups of order 3; and the groups (v) and (vi) have 13 subgroups of order 3.

E10) Abelian groups of order 56 have been constructed in Example 2.

<table>
<thead>
<tr>
<th>Elementary Divisor Decomposition</th>
<th>Invariant Factor Decomposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathbb{Z}_6 \times \mathbb{Z}_7 )</td>
<td>( \mathbb{Z}_{56} )</td>
</tr>
<tr>
<td>( \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_7 )</td>
<td>( \mathbb{Z}<em>2 \times \mathbb{Z}</em>{28} )</td>
</tr>
<tr>
<td>( \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_7 )</td>
<td>( \mathbb{Z}_2 \times \mathbb{Z}<em>2 \times \mathbb{Z}</em>{14} )</td>
</tr>
</tbody>
</table>

E11) We have the following:

<table>
<thead>
<tr>
<th>G</th>
<th>Elementary divisor form</th>
<th>Invariant factor form</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5 )</td>
<td>already in this form</td>
<td>( \mathbb{Z}<em>{40} \times \mathbb{Z}</em>{10} )</td>
</tr>
<tr>
<td>( \mathbb{Z}<em>9 \times \mathbb{Z}</em>{25} \times \mathbb{Z}_{35} \times \mathbb{Z}_4 )</td>
<td>( \mathbb{Z}<em>9 \times \mathbb{Z}</em>{25} \times \mathbb{Z}_7 \times \mathbb{Z}_5 \times \mathbb{Z}_4 )</td>
<td>( \mathbb{Z}_{60} \times \mathbb{Z}_5 )</td>
</tr>
<tr>
<td>( \mathbb{Z}<em>5 \times \mathbb{Z}</em>{10} \times \mathbb{Z}_{50} )</td>
<td>( \mathbb{Z}_5 \times \mathbb{Z}<em>5 \times \mathbb{Z}</em>{25} \times \mathbb{Z}_2 \times \mathbb{Z}_2 )</td>
<td>already in this form</td>
</tr>
</tbody>
</table>
Special Groups and Semigroups

E12) i) Let $H$ be the subgroup of $\mathbb{Z}_{12}$ generated by $\{2, 3\}$. Then $T = 3 - 2 \in H$. Therefore, $\langle T \rangle \subseteq H$. But $\langle T \rangle = \mathbb{Z}_{12}$. Therefore, $H = \mathbb{Z}_{12}$.

ii) $2 = 6 - 4 \in <4, 6> \subseteq <2>$. Therefore, $H \subseteq <2>$.

iii) Let $K$ be the subgroup of $\mathbb{Z}_{12}$ generated by $\{6, 8, 10\}$. Then $2 = 8 - 6 \in K$. Therefore, $<2> \subseteq K$. But $\{6, 8, 10\} \subseteq <2>$. Therefore, $K = <2> = \{0, 2, 4, 6, 8, 10\}$.

E13) No. Because if $H$ is the subgroup of $\mathbb{Z}_8$ generated by $\{4, 6\}$, then it can be shown, as in E12, that $H = <4> = \{0, 2, 4, 6\}$, and so $H \neq \mathbb{Z}_8$.

E14) The generating set need not be unique. For example, both $\{4, 6\}$ and $\{6, 8, 10\}$ generate $<2>$ in $\mathbb{Z}_{12}$.

Similarly, both $\{1\}$ and $\{-1\}$ generate $\mathbb{Z}$.

E15) Let $\{a_1, \ldots, a_n\}$ and $\{b_1, \ldots, b_n\}$ generate $G_1$ and $G_2$, respectively.

Any element of $G_1 \times G_2$ is of the form $(g_1, g_2)$, where $g_1 \in G_1, g_2 \in G_2$.

Since $g_1 \in G_1$, $g_1 = a_1^{n_1} \cdots a_n^{n_n}$, $n_i \geq 0$. Similarly, $g_2 = b_1^{m_1} \cdots b_n^{m_n}$, $m_j \geq 0$.

Therefore, $(g_1, g_2) = \prod\{a_i^{n_i}, b_j^{m_j}\}$.

Also, $(a_i^{n_i}, b_j^{m_j}) = \prod\{(a_i, e_j)^{n_i}(e_i, b_j)^{m_j}\}$, where $e_1, e_2$ are the identities of $G_1$ and $G_2$, respectively.

Thus, $G_1 \times G_2$ has a finite set generating it, viz.,

$\{(a_i, e_2), (e_i, b_j)\}_{i=1, \ldots, r, j=1, \ldots, s}$.

E16) Suppose $(\mathbb{Q}, +)$ is finitely generated, say generated by $\frac{a_1}{b_1}, \frac{a_2}{b_2}, \ldots, \frac{a_n}{b_n}$.

Then any rational number is expressed as $k_1 \frac{a_1}{b_1} + k_2 \frac{a_2}{b_2} + \cdots + k_n \frac{a_n}{b_n}$ for some integers $k_1, k_2, \ldots, k_n$. Let $\ell = \text{l.c.m.} (b_1, b_2, \ldots, b_n)$.

Consider $\frac{1}{\ell + 1} \in \mathbb{Q}$. Suppose $\frac{1}{\ell + 1} = k_1 \frac{a_1}{b_1} + \cdots + k_n \frac{a_n}{b_n}$.

Then $b_1 \cdots b_n = (\ell + 1)(k_1 a_1 + \cdots + k_n a_n)$, which is not possible. Hence our assumption that $(\mathbb{Q}, +)$ is finitely generated is wrong.

E17) If $G$ is free abelian with basis $X$ and $G'$ is free abelian with basis $X'$, then you can show that $G \times G'$ is free abelian with basis $\{(x, 0), (0, x') | x \in X, x' \in X'\}$.

E18) Suppose that $G$ is free abelian with basis $\{x_1, \ldots, x_n\}$. Define $\theta : \mathbb{Z}^n \to G : \theta(a_1, \ldots, a_n) = a_1 x_1 + \cdots + a_n x_n$. You should check that $\theta$ is a well-defined group homomorphism, which is 1-1 and onto.
E19) Let $G$ be an abelian group of order $n, n \geq 2$. Suppose $G$ is free abelian and let $X$ be a basis of $G$. Consider $x \in X$. Since $x \in G$, $nx = 0$. This is not possible if $X$ is a basis, unless $n = 0$. We reach a contradiction. Hence $G$ is not free abelian.

E20) Suppose $\{(a, b)\}$ generates $\mathbb{Z} \times \mathbb{Z}$. Then each element of $\mathbb{Z} \times \mathbb{Z}$ is of the form $(na, nb)$, where $n \in \mathbb{Z}$. Now consider $(a+1, b) \in \mathbb{Z} \times \mathbb{Z}$. Then $na = a+1, nb = b$. Thus, $n = 1$ and $a = a+1$, which is absurd. Hence, we reach a contradiction. Thus, a singleton cannot generate $\mathbb{Z} \times \mathbb{Z}$.

E21) i) True. For any $n \geq 1$, $\mathbb{Z}^n$ is free abelian of rank $n$.
ii) False. $\{1\}$ is a basis of $\mathbb{Z}$. Also $\{1\} \subseteq \{1, 2\} \subseteq \mathbb{Z}$, but $\{1, 2\}$ is not a basis because, for example, $0 = 0.1 + 0.2 = 2.1 + (-1).2$ are two different ways of writing 0 as a $\mathbb{Z}$-linear combination of 1 and 2.
iii) True. Follows from Theorem 9.
iv) False. $2\mathbb{Z}$ is a subgroup of the free abelian group $\mathbb{Z}$, but $\mathbb{Z}/2\mathbb{Z}$, being finite, is not free abelian.
v) True. If $G$ and $G'$ are free abelian of rank $r$, then both are isomorphic to $\mathbb{Z}^r$, and hence isomorphic to each other.

E22) i) Firstly, $\text{Tor}(G) \neq \emptyset$ since $0 \in \text{Tor}(G)$. Next, for $g, h \in \text{Tor}(G)$, let the order of $g$ and $h$ be $n$ and $m$, respectively. Then $nm(g - h) = 0$ implies that $g - h \in \text{Tor}(G)$ (we have written the binary operation in $G$ additively). Hence $\text{Tor}(G) \leq G$.
ii) It need not be a subgroup. For example, let $G = \text{GL}_2(\mathbb{R})$.
Take $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$.
Then $A^3 = I, B^3 = I$, so that $A, B \in \text{Tor}(G)$.
However, $AB = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$.
You can check that $(AB)^n = \begin{bmatrix} 1^n & 2^n \\ 0 & 1^n \end{bmatrix}$, so that $AB \notin \text{Tor}(G)$.
Hence, $\text{Tor}(G) \not\leq G$.

E23) Let $F$ be a free abelian group. Suppose $a \in F$ is an element of finite order. By Theorem 9, $\langle a \rangle$ is free abelian. Also, since $a \in \text{Tor}(F), \langle a \rangle$ is finite. By E19, this is possible only if $\langle a \rangle$ is trivial, i.e., $a = \{0\}$.

E24) $(x, y) \in \text{Tor}(G_1 \times G_2)$
\[\iff (x, y)^n = (e_1, e_2) \text{ for some } n \in \mathbb{N}\]
\[\iff x^n = e_1, y^n = e_2 \text{ for some } n \in \mathbb{N}\]
\[\iff x \in \text{Tor}(G_1), y \in \text{Tor}(G_2).\]
Hence the two sets are equal.
Special Groups and Semigroups

E25) \( G \times F \) is abelian because
\[(a, b) \cdot (a', b') = (a, a', b, b') = (a, a', b, b') = (a, b) \cdot (a', b') \text{ for all } (a, b), (a', b') \in G \times F.\]
Also, if \( F \) is generated by the finite set \( X \), then \( G \times F \) is generated by \( G \times X \), which is a finite set. Hence, \( G \times F \) is also finitely generated.
Next, \( \text{Tor}(G \times F) = \text{Tor}(G) \times \text{Tor}(F) = G \times \{e\} \), by E23 and E24.

E26) By E25, the torsion subgroup of \( \mathbb{Z}_4 \times \mathbb{Z} \times \mathbb{Z}_3 \) is isomorphic to \( \mathbb{Z}_4 \times \mathbb{Z}_3 \), which has order 12.
The torsion subgroup of \( \mathbb{Z}_{12} \times \mathbb{Z} \times \mathbb{Z}_{12} \) has order 144.

E27) We have
\[
\mathbb{Z} \times \mathbb{Z}_6 \times \mathbb{Z} \times \mathbb{Z}_{12} \times \mathbb{Z}_{10} \cong \mathbb{Z}_3 \times \mathbb{Z}_6 \times \mathbb{Z}_{12} \times \mathbb{Z}_{10}
\]
\[
\cong \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_2
\]
\[
\cong \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5
\]
This is the elementary divisor decomposition of the given group.
Using the method explained in the Structure Theorem, \( \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \) is isomorphic to \( \mathbb{Z}_3 \times \mathbb{Z}_6 \times \mathbb{Z}_{10} \), so that the invariant factors of the given group are 2, 6, 60. Furthermore, its Betti number is 3.

E28) The Betti number of a finite abelian group is 0.

E29) No. For example, \( \mathbb{Z} \times \mathbb{Z}_2 \) and \( \mathbb{Z} \times \mathbb{Z}_3 \) have the same Betti number but are not isomorphic. This is because, for example, \( \mathbb{Z} \times \mathbb{Z}_2 \) has an element of order 2 but no element of order 3; similarly, \( \mathbb{Z} \times \mathbb{Z}_3 \) has an element of order 3 but no element of order 2.
The necessary and sufficient condition for two finitely generated abelian groups to be isomorphic is that the two groups should have the same Betti number and the same invariant factors; or, equivalently, the two groups should have the same Betti number and the same elementary divisors. This has been proved in the two Structure Theorems in this section.

E30) i) The group \( G/H \) is finitely generated. In fact, if \( e_1, e_2, \ldots, e_n \) generate \( G \), then \( \overline{e_1}, \overline{e_2}, \ldots, \overline{e_n} \) generate \( G/H \) over \( \mathbb{Z} \).
ii) No, the group \( G/H \) need not be free. For example, \( \mathbb{Z} \) is a free group over \( \mathbb{Z} \) generated by 1. But, the quotient \( \mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z} \) is not a free abelian group.