2.2 Finitely Generated Abelian Groups

We classify the structures of finitely generated abelian groups in this section. All results are special cases of finitely generated modules over a principal ideal domain (to be discussed in Section IV.6).

**Lem 2.7.** Every finitely generated abelian group \( G \) is (isomorphic to) a direct sum of cyclic groups:

\[
\bigoplus_{i=1}^{t} \mathbb{Z}_{m_i} \oplus \mathbb{Z}^s, \quad m_1 \mid m_2 \mid \cdots \mid m_t.
\]

**Proof.** Let \( X \subseteq G \) be a finite set that generates \( G \). Let \( F(X) \) be the free group on \( X \). By the proof of Theorem 2.4, there is a group epimorphism \( \psi : F(X) \to G \). By Theorem 2.5, there exists a basis \( \{x_1, \cdots, x_n\} \) of \( F(X) \) such that the subgroup \( \ker \psi \) of \( F(X) \) has a basis \( \{d_1 x_1, \cdots, d_r x_r\} \) for some \( r \leq n \) and \( d_1 \mid d_2 \mid \cdots \mid d_r \). Then

\[
G \simeq F(X)/\ker \psi = \bigoplus_{i=1}^{r} (\mathbb{Z}/d_i \mathbb{Z}) \oplus \mathbb{Z}^{n-r}.
\]

Note that if \( d_i = 1 \), then \( \mathbb{Z}/d_i \mathbb{Z} \) is trivial. Remove 1’s from the sequence \( (d_1, \cdots, d_r) \) and denote the resulting sequence \( (m_1, \cdots, m_t) \). Then \( m_1 \mid \cdots \mid m_t \) and \( G \simeq \bigoplus_{i=1}^{t} \mathbb{Z}_{m_i} \oplus \mathbb{Z}^{n-r} \).

**Lem 2.8.** If \( m \in \mathbb{N} \) has the prime decomposition \( m = p_1^{n_1} \cdots p_t^{n_t} \), where \( p_1, \cdots, p_t \) are distinct primes and \( n_i \geq 1 \), then

\[
\mathbb{Z}_m \simeq \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{n_t}}.
\]

**Proof.** Let \( 1_r \) denote the identity of \( \mathbb{Z}_r \). If \( (r, k) = 1 \), then \( \mathbb{Z}_{rk} \to \mathbb{Z}_r \oplus \mathbb{Z}_k \) defined by \( a \cdot 1_{rk} \mapsto a \cdot (1_r, 1_k) \) is a group isomorphism. Then

\[
\mathbb{Z}_m \simeq \mathbb{Z}_{p_1^{n_1}} \cdots \mathbb{Z}_{p_{r-1}^{n_{r-1}}} \oplus \mathbb{Z}_{p_t^{n_t}} \simeq \cdots \simeq \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{n_t}}.
\]

**Lem 2.9.** Every finitely generated abelian group \( G \) is (isomorphic to) a direct sum of cyclic groups:

\[
\bigoplus_{i=1}^{k} \mathbb{Z}_{p_i^{n_i}} \oplus \mathbb{Z}^s,
\]

where \( p_1, \cdots, p_t \) are (not necessarily distinct) primes, \( s \geq 0 \), and \( n_i \geq 1 \) for every \( i \).

**Proof.** Use Lemma 2.7 and Lemma 2.8.
**Cor 2.10.** If $G$ is a finite abelian group of order $n$, then $G$ has a subgroup of order $m$ for every positive factor $m$ of $n$.

**Proof.** The statement is true for $G = \mathbb{Z}_{p^m}$ where $p$ is a prime. Then apply Lemma 2.8.

For an abelian group $G$, the set

$$G_\tau := \{ u \in G \mid |u| \text{ is finite} \}$$

forms a subgroup, called the **torsion subgroup** of $G$. If $G = G_\tau$, then $G$ is said to be a **torsion group**. If $G_\tau = 0$, then $G$ is said to be **torsion-free**.

Here is the structure theorem of finitely generated abelian groups.

**Thm 2.11.** Let $G$ be a finitely generated abelian group. Then $G = G_\tau \oplus F$, where $F \simeq \mathbb{Z}^s$ is a finitely generated free abelian subgroup of $G$. The integer $s \geq 0$ is unique in any such decompositions of $G$. The torsion group $G_\tau$ is either trivial or it can be decomposed as follow:

1. There is a unique list of (not necessarily distinct) positive integers $m_1, m_2, \ldots, m_t$ such that $m_i > 1$, $m_1 | m_2 | \cdots | m_t$, and

   $$G_\tau \simeq \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_t}.$$  

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

2. There is a list of prime powers $p_1^{s_1}, \ldots, p_k^{s_k}$, unique up to the order of its members, such that $p_1, \ldots, p_k$ are (not necessarily distinct) primes, $s_1, \ldots, s_k$ are (not necessarily distinct) positive integers and

   $$G_\tau \simeq \mathbb{Z}_{p_1^{s_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{s_k}}.$$  

The prime powers $p_1^{s_1}, \ldots, p_k^{s_k}$ are called the **elementary divisors** of $G$.

**Proof.** The existence of $s, m_1, m_2, \ldots, m_t$ and $p_1^{s_1}, \ldots, p_k^{s_k}$ are shown by Lemmas 2.7 and 2.9.

It remains to prove that they are unique in any corresponding decompositions of $G$.

Suppose that $G$ is isomorphic to two decompositions

$$G \simeq (\mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_t}) \oplus \mathbb{Z}^s, \quad m_i > 1, \ m_1 | m_2 | \cdots | m_t, \text{ and } s \geq 0,$$

$$G \simeq (\mathbb{Z}_{m_1'} \oplus \cdots \oplus \mathbb{Z}_{m_t'}) \oplus \mathbb{Z}^{s'}, \quad m_i' > 1, \ m_1' | m_2' | \cdots | m_t', \text{ and } s' \geq 0.$$  

Let $m := m_t m_t'$. Then the abelian group

$$mG := \{ mu \mid u \in G \} \simeq m(\mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_t}) \oplus (m\mathbb{Z})^s \simeq \mathbb{Z}^s,$$

$$\simeq m(\mathbb{Z}_{m_1'} \oplus \cdots \oplus \mathbb{Z}_{m_t'}) \oplus (m\mathbb{Z})^{s'} \simeq \mathbb{Z}^{s'}.$$
2.2. FINITELY GENERATED ABELIAN GROUPS

So $mG$ is a free abelian group and $s = s'$ by Proposition 2.3. This proves the uniqueness of $s$.

Next consider $G_r$. Let $I$ denote the set of multisets of invariant factors $\{m_1, \ldots, m_t\}$ of $G$ so that $m_i > 1$, $m_1 | m_2 | \cdots | m_t$, and $G_r \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_t}$. Let $E$ denote the set of multisets of elementary divisors $\{p_1^{n_1}, p_2^{n_2}, \ldots, p_k^{n_k}\}$ of $G$ such that $G_r \cong \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \mathbb{Z}_{p_k^{n_k}}$. We define a bijective map from $I$ to $E$ as follow.

Suppose that $\{m_1, \ldots, m_t\} \in E$ so that

$$G_r \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_t}, \quad m_i > 1, \quad m_1 | m_2 | \cdots | m_t.$$ 

and that $m_i$ has the prime decomposition $m_i = q_1^{n_1} \cdots q_r^{n_r}$ where $q_1, \ldots, q_r$ are distinct primes and $n_1, \ldots, n_r \in \mathbb{Z}^+$, then every $m_i$ has the decomposition $m_i = q_1^{n_i} \cdots q_r^{n_r}$ such that

$$0 \leq n_{1j} \leq n_{2j} \leq \cdots \leq n_{ij} = n_j \quad \text{for} \quad j = 1, \ldots, r.$$ 

Then there is the decomposition

$$G_r \cong \bigoplus_{j=1}^{r} \bigoplus_{i=1}^{t} \mathbb{Z}_{q_j^{n_{ij}}}$$

Removing 1’s from those prime powers $q_j^{n_{ij}}$ and reindexing the prime powers, we get a multiset of elementary divisors $\{p_1^{n_1}, \ldots, p_k^{n_k}\} \in E$. One can check that this builds up a bijection from $I$ to $E$.

Finally, we show that $|E| = 1$. This implies that $|I| = 1$, and thus there exists exactly one multiset of invariant factors and one multiset of elementary divisors of $G$.

Let $\{q_j^{n_{ij}} \mid j = 1, \ldots, r, \; i = 1, \ldots, t_j\}$ be a multiset of elementary divisors of $G$, where $q_1, \ldots, q_r$ are distinct primes and $n_{ij} \geq 1$. Then

$$G_r \cong \bigoplus_{j=1}^{r} \bigoplus_{i=1}^{t_j} \mathbb{Z}_{q_j^{n_{ij}}}.$$  \hspace{1cm} (2.1)

We may assume that $n_{1\ell} \leq n_{2\ell} \leq \cdots \leq n_{t_\ell \ell}$ for $\ell = 1, \ldots, r$.

For $m \in \mathbb{Z}^+$, define $G[m] := \{u \in G \mid mu = 0\}$. Then $G[m]$ is a subgroup of $G$, and $(G_1 \oplus G_2)[m] = G_1[m] \oplus G_2[m]$ for groups $G_1, G_2$. For each prime $q_\ell$ ($1 \leq \ell \leq r$),

$$G[q_\ell] \cong G_r[q_\ell] \cong \bigoplus_{j=1}^{r} \bigoplus_{i=1}^{t_j} \mathbb{Z}_{q_j^{n_{ij}}} [q_\ell] \cong \bigoplus_{i=1}^{t_\ell} \left(q_\ell^{n_{i\ell}} \mathbb{Z}_{q_\ell^{n_{i\ell}}} \right) \cong (\mathbb{Z}_{q_\ell})^{t_\ell}.$$ 

There are $q_\ell^{t_\ell} - 1$ elements of order $q_\ell$ in $G[q_\ell]$. So $q_\ell$ and $t_\ell$ are unique for all multisets of elementary divisors of $G$. 
For any \( b \in \mathbb{Z}^+ \),

\[
q^b_\ell G_\tau \cong \bigoplus_{j=1}^r \bigoplus_{i=1}^{t_j} (q^b_\ell \mathbb{Z}_{q^j_n}) \cong \left( \bigoplus_{j=1}^r \bigoplus_{i=1}^{t_j} \mathbb{Z}_{q^j_n} \right) \oplus \left( \bigoplus_{i=1}^{t_\ell} \mathbb{Z}_{n_\ell > b} \right)
\]

Then

\[
(q^b_\ell G_\tau)[q_\ell] \cong \left( \bigoplus_{i=1}^{t_\ell} \mathbb{Z}_{n_\ell > b} \right)[q_\ell] \cong (\mathbb{Z}_{q^\ell})^{w(q_\ell, b)},
\]

where \( w(q_\ell, b) \) denotes the number of integers \( n_1, \ldots, n_{t_\ell} \) that are greater than \( b \). The abelian group \((q^b_\ell G_\tau)[q_\ell]\) is independent of the choice of elementary divisors of \( G \). So \( w(q_\ell, b) \) for all \( b \in \mathbb{N} \) are unique. Thus \( n_1, \ldots, n_{t_\ell} \) are unique for every \( \ell = 1, \ldots, r \).

Hence there is only one multiset of elementary divisors and one multiset of invariant factors for \( G \). This completes the proof. \( \square \)

**Cor 2.12.** Two finitely generated abelian groups \( G \) and \( H \) are isomorphic if and only if \( G/G_\tau \) and \( H/H_\tau \) have the same rank and \( G \) and \( H \) have the same invariant factors [resp. elementary divisors].

**Ex.** How many Abelian groups of order 360 up to equivalence?

**Ex.** Find the invariant factors and elementary divisors of \( \mathbb{Z}_5 \oplus \mathbb{Z}_{15} \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_{36} \oplus \mathbb{Z}_{54} \).