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:*

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

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 an 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 $\operatorname{Ker}\psi$ of $F(X)$ has a basis $\{d_1x_1, \cdots, d_rx_r\}$ for some $r \leq n$ and $d_1 \mid d_2 \mid \cdots \mid d_r$. Then

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

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

$$\mathbb{Z}_m \;\simeq\; \mathbb{Z}_{p_1^{n_1}\cdots p_{t-1}^{n-1}} \oplus \mathbb{Z}_{p_t^{n_t}} \;\simeq\; \cdots \;\simeq\; \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{n_t}}.$$

□

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_τ is either trivial or it can be decomposed as follow:*

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

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

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

2. *There is a list of prime powers $p_1^{s_1}, \cdots, p_k^{s_k}$, unique up to the order of its members, such that $p_1, \cdots, p_k$ are (not necessarily distinct) primes, $s_1, \cdots, s_k$ 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 $p_1^{s_1}, \cdots, p_k^{s_k}$ are called the **elementary divisors** *of G.*

Proof. The existence of s, $m_1, m_2, \cdots, m_t$ and $p_1^{s_1}, \cdots, p_k^{s_k}$ 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

$$\begin{aligned} G &\simeq (\mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_t}) \oplus \mathbb{Z}^s, && m_i > 1, \quad m_1 \mid m_2 \mid \cdots \mid m_t, \quad \text{and } s \geq 0, \\ G &\simeq (\mathbb{Z}_{m'_1} \oplus \cdots \oplus \mathbb{Z}_{m'_{t'}}) \oplus \mathbb{Z}^{s'}, && m'_i > 1, \quad m'_1 \mid m'_2 \mid \cdots \mid m'_{t'}, \quad \text{and } s' \geq 0. \end{aligned}$$

Let $m := m_t m'_{t'}$. Then the abelian group

$$\begin{aligned} mG := \{mu \mid u \in G\} &\simeq m(\mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_t}) \oplus (m\mathbb{Z})^s \simeq \mathbb{Z}^s \\ &\simeq m(\mathbb{Z}_{m'_1} \oplus \cdots \oplus \mathbb{Z}_{m'_{t'}}) \oplus (m\mathbb{Z})^{s'} \simeq \mathbb{Z}^{s'}. \end{aligned}$$

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

Next consider G_τ. Let $\mathcal{I}$ denote the set of multisets of invariant factors $\{m_1, \cdots, m_t\}$ of G so that $m_i > 1$, $m_1 \mid m_2 \mid \cdots \mid m_t$, and $G_\tau \simeq \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_t}$. Let $\mathcal{E}$ denote the set of multisets of elementary divisors $\{p_1^{s_1}, p_2^{s_2}, \cdots, p_k^{s_k}\}$ of G such that $G_\tau \simeq \mathbb{Z}_{p_1^{s_1}} \oplus \cdots \mathbb{Z}_{p_k^{s_k}}$. We define a bijective map from $\mathcal{I}$ to $\mathcal{E}$ as follow.

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

$$G_\tau \simeq \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_t}, \qquad m_i > 1, \quad m_1 \mid m_2 \mid \cdots \mid m_t.$$

and that m_t has the prime decomposition $m_t = q_1^{n_1} \cdots q_r^{n_r}$ where $q_1, \cdots, q_r$ are distinct primes and $n_1, \cdots, n_r \in \mathbb{Z}^+$, then every m_i has the decomposition $m_i = q_1^{n_{i1}} \cdots q_r^{n_{ir}}$ such that

$$0 \le n_{1j} \le n_{2j} \le \cdots \le n_{tj} = n_j \quad \text{for} \quad j = 1, \cdots, r.$$

Then there is the decomposition

$$G_\tau \simeq \bigoplus_{j=1}^{r} \bigoplus_{i=1}^{t} \mathbb{Z}_{q_j^{n_{ij}}}$$

Removing 1's from those prime powers $q_j^{n_{ij}}$ and reindexing the prime powers, we get a multiset of elementary divisors $\{p_1^{s_1}, \cdots, p_k^{s_k}\} \in \mathcal{E}$. One can check that this builds up a bijection from $\mathcal{I}$ to $\mathcal{E}$.

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

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

$$G_\tau \simeq \bigoplus_{j=1}^{r} \bigoplus_{i=1}^{t_j} \mathbb{Z}_{q_j^{n_{ij}}}. \tag{2.1}$$

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

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_ℓ $(1 \le \ell \le r)$,

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

There are $q_\ell^{t_\ell} - 1$ elements of order q_ℓ in $G[q_\ell]$. So q_ℓ and t_ℓ are unique for all multisets of elementary divisors of G.

For any $b \in \mathbb{Z}^+$,

$$q_\ell^b G_\tau \simeq \bigoplus_{j=1}^{r} \bigoplus_{i=1}^{t_j} (q_\ell^b \mathbb{Z}_{q_j^{n_{ij}}}) \simeq \left(\bigoplus_{\substack{j=1 \\ j\neq\ell}}^{r} \bigoplus_{i=1}^{t_j} \mathbb{Z}_{q_j^{n_{ij}}} \right) \oplus \left(\bigoplus_{\substack{i=1 \\ n_{i\ell}>b}}^{t_\ell} \mathbb{Z}_{q_\ell^{n_{i\ell}-b}} \right)$$

Then

$$(q_\ell^b G_\tau)[q_\ell] \simeq \left(\bigoplus_{\substack{i=1 \\ n_{i\ell}>b}}^{t_\ell} \mathbb{Z}_{q_\ell^{n_{i\ell}-b}} \right) [q_\ell] \simeq (\mathbb{Z}_{q_\ell})^{w(q_\ell,b)},$$

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

Hence there is only one multiset of elementary divisors and one multiset of invariant factors for G. This completes the proof. □

Cor 2.12. *Two finitely generated abelian groups G and H are isomorphic if and only if G/G_τ and H/H_τ 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 $\mathbb{Z}_5 \oplus \mathbb{Z}_{15} \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_{36} \oplus \mathbb{Z}_{54}$.*