Section II.2. Finitely Generated Abelian Groups

Note. In this section we prove the Fundamental Theorem of Finitely Generated Abelian Groups. Recall that every infinite cyclic group is isomorphic to $\mathbb{Z}$ and every finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$ (Theorem I.3.2).

Theorem II.2.1. Every finitely generated abelian group G is isomorphic to a finite direct sum of cyclic groups in which the finite cyclic summands (if any) are of orders $m_1, m_2, \ldots, m_t$ where $m_1 > 1$ and $m_1 \mid m_2 \mid \cdots \mid m_t$.

Note. We will see that we can further "refine" the values of the m_i's of Theorem II.2.1 and express the orders of the cyclic groups in terms of powers of primes. First we need a preliminary result.

Lemma II.2.3. If m is a positive integer and $m = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$ ($p_1, p_2, \ldots, p_t$ distinct primes and each $n_i \in \mathbb{N}$), then

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1{}^{n_1}} \oplus \mathbb{Z}_{p_2{}^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_t{}^{n_t}}.$$

Note. Notice that in the proof of Lemma II.2.3, it is shown that $\mathbb{Z}_{rn} \cong \mathbb{Z}_r \oplus \mathbb{Z}_n$ if $\gcd(r, n) = 1$. In fact, the converse of Lemma II.2.3 also holds as follows.

Lemma II.2.A. If m is a positive integer and $m = nk$ where n and k are not relatively prime, then $\mathbb{Z}_m \not\cong \mathbb{Z}_n \oplus \mathbb{Z}_k$.

Theorem II.2.2. Every finitely generated abelian group G is isomorphic to a finite direct sum of cyclic groups, each of which is either infinite or of order a power of a prime.

Note. The following result shows that the converse of Lagrange's Theorem (Corollary I.4.6) holds for finite abelian groups.

Corollary II.2.4. If G is a finite abelian group of order n, then G has a subgroup of order m for every positive integer m that divides n.

Note. We still have not completed the fundamental theorem—we still need to establish uniqueness of the decompositions into direct sums of cyclic groups. We need a preliminary result.

Lemma II.2.5. Let G be an abelian group, m an integer, and p a prime integer. Then each of the following is a subgroup of G:

(i) $mG = \{mu \mid u \in G\}$;

(ii) $G[m] = \{u \in G \mid mu = 0\}$;

(iii) $G(p) = \{u \in G \mid |u| = p^n \text{ for some } n \geq 0\}$;

(iv) $G_t = \{u \in G \mid |u| \text{ is finite}\}$;

In particular there are the following isomorphism relationships

(v) $\mathbb{Z}_{p^n}[p] \cong \mathbb{Z}_p$ and $p^m\mathbb{Z}_{p^n} \cong \mathbb{Z}_{p^{n-m}}$ $(m < n)$.

Let H and G_i $(I \in I)$ be abelian groups.

(vi) If $g : G \to \sum_{i \in I} G_i$ is an isomorphism, then the restrictions of g to mG and $G[m]$ respectively are isomorphisms giving

$$mG \cong \sum_{i \in I} mG_i \text{ and } G[m] \cong \sum_{i \in I} G_i[m].$$

(vii) If $f : G \to H$ is an isomorphism then the restrictions of f to G_t and $G(p)$ respectively are isomorphisms giving

$$G_t \cong H_t \text{ and } G(p) \cong H(p).$$

Definition. Let G be an abelian group with subgroup (a subgroup by Lemma II.2.5)

$$G_t = \{u \in G \mid \text{ the order } |u| \text{ is finite}\}.$$

G_t is the *torsion subgroup* of G. If $G = G_t$ then G is a *torsion group*. If $G_t = \{0\}$ then G is *torsion free*.

Theorem II.2.6. Fundamental Theorem of Finitely Generated Abelian Groups.

Let G be a finitely generated abelian group.

(i) There is a unique nonnegative integer s such that the number of infinite cyclic summands in any decomposition of G as a direct sum of cyclic groups is precisely s;

(ii) either G is free abelian or there is a unique list of (not necessarily distinct) positive integers $m_1, m_2, \ldots, m_t$ such that $m_1 > 1$, $m_1 \mid m_2 \mid \cdots \mid m_t$ and

$$G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_t} \oplus F$$

with F free abelian;

(iii) either G is free abelian or there is a list of positive integers $p_1^{s_1}, p_2^{s_2}, \ldots, p_k^{s_k}$ which is unique except for the order of its members, such that $p_1, p_2, \ldots, p_k$ are (not necessarily distinct) primes, $s_1, s_2, \ldots, s_k$ are (not necessarily distinct) positive integers and

$$G \cong \mathbb{Z}_{p_1{}^{s_1}} \oplus \mathbb{Z}_{p_2{}^{s_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k{}^{s_k}} \oplus F$$

with F free abelian.

Note. We know by Theorem II.1.1(iii) that a free abelian group is a direct sum of copies of the additive groups $\mathbb{Z}$. Since group G is finitely generated, then the number of copies of $\mathbb{Z}$ in the direct sum must be finite. So group F in Theorem II.2.6 is of the form $F \cong \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$. So Theorem II.2.6 implies that a finitely generated abelian group G is of the form

$$G \cong (\mathbb{Z}_{p_1{}^{s_1}} \oplus \mathbb{Z}_{p_2{}^{s_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k{}^{s_k}}) \oplus (\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z})$$

where the p_i are (not necessarily distinct) primes and the s_i are positive integers. This version of the fundamental theorem is the version stated by Fraleigh; see my class notes for Introduction to Modern Algebra 1 and 2 (MATH 4127/5127, 4137/5137) on Section II.11. Direct Products and Finitely Generated Abelian Groups and Section VII.38. Free Abelian Groups . The parameter s of Theorem II.2.6 is the *Betti number* of group G.

Definition. Let G be a finitely generated abelian group with

$$G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_t} \oplus F$$

where F is free abelian and $m_1 \mid m_2 \mid \cdots \mid m_t$. The $m_1, m_2, \ldots, m_t$ are the *invariant factors* of G. With

$$G \cong \mathbb{Z}_{{p_1}^{s_1}} \oplus \mathbb{Z}_{{p_2}^{s_2}} \oplus \cdots \oplus \mathbb{Z}_{{p_k}^{s_k}} \oplus F$$

where F is free abelian, each p_i is prime, and each s_i is a positive integer, then the powers of prime $p_1^{s_1}, p_2^{s_2}, \ldots, p_k^{s_k}$ are the *elementary divisors* of G.

Corollary II.2.7. Two finitely generated abelian groups G and H are isomorphic if and only if G/G_t and H/H_t have the same rank and G and H have the same invariant factors (or elementary divisors).

Note. As you know from senior level modern algebra, the fundamental theorem can be used to find the distinct abelian groups of a given order.

Example. Find all abelian groups (up to isomorphism) of order 720. First, we need to factor 720: $720 = 2^4 \cdot 3^2 \cdot 5$. For the factor 2^4 we get the following non-isomorphic groups:

$$\mathbb{Z}_{16}, \mathbb{Z}_2 \oplus \mathbb{Z}_8, \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4, \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \text{ and } \mathbb{Z}_4 \oplus \mathbb{Z}_4.$$

The factor 3^2 yields: $\mathbb{Z}_9$ and $\mathbb{Z}_3 \oplus \mathbb{Z}_3$. Factor 5 yields: $\mathbb{Z}_5$. So we get a total of 10 possible groups of order 720:

$\mathbb{Z}_{16} \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$	$\mathbb{Z}_{16} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$
$\mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$	$\mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$
$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$
$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$
$\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$	$\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$

Note. Hungerford explains how to find the m_i's of Theorem II.2.6(ii) from the $p_i^{s_i}$'s of Theorem II.2.6(iii). We illustrate this with an example.

Example. Consider $G = \mathbb{Z}_5 \oplus \mathbb{Z}_{15} \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_{36} \oplus \mathbb{Z}_{54}$. Then by Lemma II.2.3 we can decompose these constituent groups as

$$G \cong \mathbb{Z}_5 \oplus (\mathbb{Z}_3 \oplus \mathbb{Z}_5) \oplus \mathbb{Z}_{25} \oplus (\mathbb{Z}_4 \oplus \mathbb{Z}_9) \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_{27}).$$

So the elementary divisors of G are $2, 2^2, 3, 3^2, 3^3, 5, 5, 5^2$ which we arrange as

$$\begin{array}{lll} 2^0, & 3, & 5 \\ 2, & 3^2, & 5 \\ 2^2, & 3^3, & 5^2. \end{array}$$

Then we take products across rows to get $m_1 = 1 \cdot 3 \cdot 5 = 15$, $m_2 = 2 \cdot 3^2 \cdot 5 = 90$, and $m_3 = 2^2 \cdot 3^3 \cdot 5^2 = 2700$. So the invariant factors are 15, 90, 2700 and so by Theorem II.2.6(ii), $G \cong \mathbb{Z}_{15} \oplus \mathbb{Z}_{90} \oplus \mathbb{Z}_{2700}$.

Revised: 12/7/2023