CHAPTER 3

FINITE ABELIAN GROUPS

3.1 Basis of an abelian group

Definition 3.1.1. Let G be an abelian group, and let $S = \{x_1, x_2, \ldots, x_n\}$ be a finite subset of G. We say that S *generates* G if for all $x \in G$, there exist $\alpha_i \in \mathbb{Z}$, for $1 \leq i \leq n$ such that

$$x = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n.$$

If so, we denote $G = \langle x_1, x_2, \ldots, x_n \rangle$.

Definition 3.1.2. Let G be an abelian group, and let $S = \{x_1, x_2, \ldots, x_n\}$ be a finite subset of G. We say that S is a *basis* for G if:

- S generates G, and
- for all $m_i \in \mathbb{Z}$, $1 \leq i \leq n$,

$$m_1 x_1 + m_2 x_2 + \cdots + m_n x_n = 0 \implies m_i x_i = 0 \; \forall \; 1 \leq i \leq n.$$

Proposition 3.1.3. *Let G be an abelian group, and let $S = \{x_1, x_2, \ldots, x_n\}$ be a basis for G. Then,*

$$G \cong \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_n \rangle.$$

Proof. Define the map $\varphi \colon \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_n \rangle \to G$ by

$$\varphi(\alpha_1 x_1, \alpha_2 x_2, \ldots, \alpha_n x_n) = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n.$$

Since G is abelian, the map is a homomorphism. Moreover, since S generates G, the map is surjective. Now, let $(\alpha_1 x_1, \alpha_2 x_2, \ldots, \alpha_n x_n) \in \ker \varphi$. In that case,

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = 0.$$

Since S is a basis, we find that $\alpha_i x_i = 0$ for all $1 \leq i \leq n$. Hence,

$$(\alpha_1 x_1, \alpha_2 x_2, \ldots, \alpha_n x_n) = (0, 0, \ldots, 0).$$

This implies that the kernel is trivial. So,

$$G \cong \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_n \rangle.$$

□

Lemma 3.1.4. *Let G be an abelian group, and let $S = \{x_1, x_2, \ldots, x_n\}$ generate G, and let $c_1, c_2, \ldots, c_n \in \mathbb{Z}_{\geq 0}$ with $\gcd(c_1, c_2, \ldots, c_n) = 1$. Then, there exists $y_2, y_3, \ldots, y_n \in G$ such that $G = \langle y_1, y_2, \ldots, y_n \rangle$, where $y_1 = c_1 x_1 + c_2 x_2 + \cdots + c_n x_n$.*

Proof. We will show this by induction on $s = c_1 + c_2 + \cdots + c_n \geq 1$. If $s = 1$, then we know that $c_i = 1$ for some $1 \leq i \leq n$, and $c_j = 0$ for all $1 \leq j \leq n$ with $i \neq j$. Hence, $y_1 = x_i$. In that case, we can set $y_2, y_3, \ldots, y_n$ to be the remaining elements in $x_1, x_2, \ldots, x_n$, and the statement holds.

Now, assume that $s \geq 2$. Since $\gcd(c_1, c_2, \ldots, c_n) = 1$, we find that there exist two elements $c_i, c_j \neq 0$. Without loss of generality, assume that $c_1 \geq c_2 > 0$. We claim that $M = \langle x_1, x_1 + x_2, x_3, \ldots, x_n \rangle$. For $x \in M$, we know that there exist $\alpha_i \in \mathbb{Z}$ for $1 \leq i \leq n$ such that

$$x = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n.$$

Hence,

$$x = (\alpha_1 - \alpha_2)x_1 + \alpha_2(x_1 + x_2) + \cdots + \alpha_n x_n \in \langle x_1, x_1 + x_2, \ldots, x_n \rangle.$$

Hence, $M = \langle x_1, x_1 + x_2, \ldots, x_n \rangle$. Moreover, since $\gcd(c_1, c_2, \ldots, c_n) = 1$, we can find $a_1, a_2, \ldots, a_n$ such that

$$c_1 a_1 + c_2 a_2 + \cdots + c_n a_n = 1.$$

Hence,

$$(c_1 - c_2)a_1 + c_2(a_1 + a_2) + \cdots + c_n a_n = 1.$$

This implies that $\gcd(c_1 - c_2, c_2, \ldots, c_n) = 1$. Further, we have $(c_1 - c_2) + c_2 + \cdots + c_n < s$. So, the induction hypothesis tells us that there exist $y_2, \ldots, y_n \in G$ with

$$y_1 = (c_1 - c_2)x_1 + c_2(x_1 + x_2) + \cdots + c_n x_n = c_1 x_1 + c_2 x_2 + \cdots + c_n x_n$$

such that $M = \langle y_1, y_2, \ldots, y_n \rangle$. So, the result follows from induction. □

Definition 3.1.5. Let G be an abelian group. We say that G is *finitely generated* if there exist $x_1, x_2, \ldots, x_n$ such that $G = \langle x_1, x_2, \ldots, x_n \rangle$.

Theorem 3.1.6. *Let G be a finitely generated abelian group. Then, G has a basis. In particular, G is a direct product of cyclic groups.*

Proof. We will use induction on the length of the shortest generating set. If the length is 1, then $G = \langle x_1 \rangle$, for some $x_1 \in G$. Hence, $\{x_1\}$ is a basis for G. Now, assume that the shortest generating set of G has length is n. So, fix $G = \langle x_1, x_2, \ldots, x_n \rangle$, where for any other $y_1, y_2, \ldots, y_n \in G \setminus \{0\}$ with $G = \langle y_1, y_2, \ldots, y_n \rangle$, we have $1 < |x_1| \leq |y_1|$.[1] We show that $G \cong \langle x_1 \rangle \times \langle x_2, \ldots, x_n \rangle$. So, assume, for a contradiction, that $G \ncong \langle x_1 \rangle \times \langle x_2, \ldots, x_n \rangle$. Define the map $\varphi : \langle x_1 \rangle \times \langle x_2, \ldots, x_n \rangle \to G$ by $\varphi(\alpha_1 x_1, w) = \alpha_1 x_1 + w$. This is a surjective homomorphism, so it cannot be injective. So, let $(\alpha_1 x_1, w) \in \ker \varphi$ be a non-trivial element. If $\alpha_1 = 0$, then $\alpha_1 x_1 = 0$ and $w = -\alpha_1 x_1 = 0$ as well, so we must have $\alpha_1 \neq 0$. Denote

$$w = \alpha_2 x_2 + \cdots + \alpha_n x_n.$$

By changing x_i to $-x_i$ if needed, we can assume that $\alpha_i \geq 0$ for all $1 \leq i \leq n$. We can further assume that $\alpha_1 < |x_1|$. We have $d = \gcd(\alpha_1, \alpha_2, \ldots, \alpha_n) > 0$. So, define $c_i = \alpha_i / d$. Then, the lemma tells us that there exist $y_2, \ldots, y_n$ with

$$y_1 = c_1 x_1 + \cdots + c_n x_n$$

[1] We can get rid of x_1 if $|x_1| = 1$, which contradicts the minimality of n.

such that $M = \langle y_1, \ldots, y_n \rangle$. We know that

$$dy_1 = \alpha_1 x_1 + \cdots + \alpha_n x_n = 0.$$

In that case,

$$|y_1| \leq d \leq \alpha_1 < |x_1|.$$

This is a contradiction. Hence,

$$G \cong \langle x_1 \rangle \times \langle x_2, \ldots, x_n \rangle.$$

By induction, we know that $\langle x_2, \ldots, x_n \rangle$ has a basis $\{z_1, z_2, \ldots, z_k\}$. Then, G has basis $\{x_1, z_1, z_2, \ldots, z_k\}$. □

Corollary 3.1.7. *Let G be a finite abelian group such that for any $k \geq 0$, G has at most k elements of order dividing k. Then, G is cyclic.*

Proof. By the previous result, we find that

$$G \cong \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_n \rangle.$$

Since G is finite, x_i has finite order for all $1 \leq i \leq n$. Now, let $1 \leq i, j \leq n$ with $i \neq j$. If $k \mid |x_i|$ and $k \mid |x_j|$, then both $\langle x_i \rangle$ and $\langle x_j \rangle$ have distinct subgroups of order k. Hence, G has more than k elements of order dividing k. So, we must find that $\gcd(|x_i|, |x_j|) = 1$. In that case,

$$|(x_1, x_2, \ldots, x_n)| = |x_1||x_2| \ldots |x_n|.$$

Hence, G is cyclic. □

Corollary 3.1.8. *Let F be a field and let $G \leq F^\times$ be finite. Then, G is cyclic.*

Proof. Let $n \in \mathbb{Z}_{\geq 1}$. We know that the equation $x^n - 1 \in F[x]$ has at most n roots. This implies that there are at most n elements of order dividing n. Using the result above, it follows that G is cyclic. □

3.2 The Fundamental Theorem

Lemma 3.2.1. *Let G be an abelian group such that*

$$G \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_n^{\alpha_n}},$$

where $\alpha_i \geq 2$ and p_i prime for $1 \leq i \leq k$ and $r \geq 0$, let p be a prime and let $k \in \mathbb{Z}_{\geq 1}$. Then, p^k divides an element in $\{p_1, \ldots, p_n\}$ if and only if G has an element of order p^k.

Proof. Assume that p^k divides an element in $\{p_1^{\alpha_1}, \ldots, p_n^{\alpha_n}\}$. Without loss of generality, assume further that $p^k \mid p_1$. In that case, consider the element $x = (p_1^{\alpha_1 - k}, 0, \ldots, 0)$. We find that $x \neq 0$ with

$$p^k x = (p_1^{\alpha_1}, 0, \ldots, 0) = 0.$$

Hence, $x \in G$ has order p^k.

Now, assume that G has an element x of order p^k. Let $x = (a_1, \ldots, a_n)$. We know that $p^{k-1}x \neq 0$, so without loss of generality, assume that $p^{k-1}a_1 \neq 0$. Moreover, since x has order p^k, we find that

$$p^k x = (p^k a_1, \ldots, p^k a_n) = 0.$$

So, $p^k a_1 = 0$. Hence, $|a_1| = p^k$. By Lagrange, we find that $p^k \mid p_1^{\alpha_1}$. □

Lemma 3.2.2. *Let G be an abelian group such that*

$$G \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_n^{\alpha_n}},$$

where $\alpha_i \geq 2$ and p_i prime for $1 \leq i \leq k$ and $r \geq 0$, let p be a prime. Then, for all $k \in \mathbb{Z}_{\geq 1}$, p^k divides a_k values in the collection $p_1^{\alpha_1}, \ldots, p_n^{\alpha_n}$ if and only if G has

$$(p^k)^{a_k} \cdot (p^{k-1})^{a_{k-1} - a_k} \ldots (p)^{a_2 - a_1} = p^{a_1 + a_2 + \cdots + a_k}$$

elements of order dividing p^k.

Proof. First, assume that p^k divides a_k elements in the collection $p_1^{\alpha_1}, \ldots, p_n^{\alpha_n}$ for all $k \in \mathbb{Z}_{\geq 1}$. In a cyclic group, there is at most one subgroup of some order. Since there are a_k elements in the collection $p_1^{\alpha_1}, \ldots, p_n^{\alpha_n}$ that p^k divides, it follows that G has a_k subgroups of order p^k. In general, G has a_i subgroups of order p^i for $0 \leq i \leq k$. Since a subgroup of order p^i has a single subgroup of order p^{i-1}, and it is maximal, it follows that G has

$$(p^k)^{a_k} \cdot (p^{k-1})^{a_{k-1} - a_k} \ldots (p)^{a_2 - a_1}$$

elements of order dividing p^k.

Now, assume that G has

$$(p^k)^{a_k} \cdot (p^{k-1})^{a_{k-1} - a_k} \ldots (p)^{a_2 - a_1}$$

elements of order dividing p^k. We know that a cyclic group of order dividing p^k has p^k elements of order p^k. Moreover, these are counted twice for a cyclic group of order p^{k-1}, so we need to remove them. Hence, it follows that p^k divides a_k values in the collection $p_1^{\alpha_1}, \ldots, p_n^{\alpha_n}$.

□

Theorem 3.2.3 (Fundamental Theorem of Finitely Generated Abelian Groups)**.** *Let G be a non-trivial finitely generated abelian group. Then,*

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k},$$

where $n_i \geq 2$ for $1 \leq i \leq k$ and $r \geq 0$. Moreover,

- *r (called the* rank*) is uniquely determined by G;*
- *the values n_i can be chosen such that $n_1 \mid n_2 \mid \cdots \mid n_k$- these are uniquely determined by G (called the* invariant factors*);*
- *the values n_i can be chosen to be prime powers- these are uniquely determined by G, up to permutation (called the* elementary divisors*).*

Proof. We have shown that

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$$

since these are precisely the cyclic groups. We first show that the rank is uniquely determined by G. So, let p be a prime such that $p \nmid n_i$ for all $1 \leq i \leq k$. Then,

$$G/pG \cong (\mathbb{Z}_p)^r$$

since $\mathbb{Z}_{n_i} = p\mathbb{Z}_{n_i}$ for all $1 \leq i \leq k$- we have $(p, n_i) = 1$. The space $(\mathbb{Z}_p)^r$ is a vector space over the field $\mathbb{F}_p$. We have

$$r = \dim_{\mathbb{F}_p}(G/pG)^r,$$

so it is uniquely determined by G.

We will now show the existence of elementary divisors. We know that for $n_1, n_2 \in \mathbb{Z}_{\geq 1}$, if $(n_1, n_2) = 1$, then

$$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \cong \mathbb{Z}_{n_1 n_2}.$$

So, if the prime factorisation of n_i is $n_i = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, then

$$\mathbb{Z}_{n_i} \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}.$$

Hence, we have the existence of elementary divisors. Using this, we can construct invariant factors- assume that the following is the elementary divisor representation of G:

$$G \cong \mathbb{Z}_{p_1^{\alpha_{1,1}}} \times \cdots \times \mathbb{Z}_{p_1^{\alpha_{1,n}}} \times \mathbb{Z}_{p_2^{\alpha_{2,1}}} \cdots \times \mathbb{Z}_{p_k^{\alpha_{k,n}}},$$

where $p_i^{\alpha_{i,n}} \geq 1$ and $0 \leq \alpha_{i,j-1} \leq \alpha_{i,j}$ for $1 \leq i \leq k$ and $1 \leq j \leq n$. Then,

$$G \cong \mathbb{Z}_{x_1} \times \mathbb{Z}_{x_2} \times \cdots \times \mathbb{Z}_{x_n}$$

is the invariant factor representation for G, where

$$x_j = \prod_{i=1}^{k} p_i^{\alpha_{i,j}}.$$

By construction, we have $x_1 \mid x_2 \mid \cdots \mid x_n$. Hence, we can find an invariant factor representation for G.

We next show the uniqueness of elementary divisors and invariant factors. Since there is an algorithm that produces invariant factors from elementary divisors, it suffices to show that the elementary divisors are unique. Assume that

$$G \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}.$$

Let p be a prime. By Cauchy's Theorem, $p \in \{p_1, p_2, \ldots, p_k\}$ if and only if G has an element of order p. □

Example 3.2.4. Let

$$G = \mathbb{Z}_{16} \times \mathbb{Z}_{18} \times \mathbb{Z}_{27} \times \mathbb{Z}_{52}.$$

This is a finitely generated abelian group, but is not in elementary divisor form or invariant factor form. To convert it to elementary divisor, we break each factor into its prime factors.

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{16} \times \mathbb{Z}_9 \times \mathbb{Z}_{27} \times \mathbb{Z}_{13}.$$

Now, to convert it to invariant factors, we write all the factors as follows:

$$\begin{array}{ccc} 2 & 4 & 16 \\ 1 & 9 & 27 \\ 1 & 1 & 13 \end{array}$$

We combine each column to construct the invariant factors. In this case, we have

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_{36} \times \mathbb{Z}_{5616}.$$