25SG Structure of Groups

Qiu Caiyong

August 11, 2025

Preface

Later Version = Better Version.

Contents

Chapter 1

Abelian Groups

Throughout this chapter, we use the additive notation.

$$\text{abelian groups} = \mathbb{Z} \text{ modules}$$

We will pretend that we're doing linear algebra.

1.1 Fundamentals

Proposition 1.1.1 (subgroup generated by a finite subset)
Let G be an abelian group and $X \subseteq G$ be a finite subset, then the intersection of all subgroups containing X is given by

$$\langle X \rangle = \left\{ \sum_{g \in X} n_g g \,\middle|\, n_g \in \mathbb{Z} \right\}$$

We call it the subgroup generated by X. We define $\langle \varnothing \rangle = \{0\}$ to be the trivial subgroup.

Proposition 1.1.2 (subgroup generated by a subset)
Let G be an abelian group and $X \subseteq G$ be a subset, denote the set of all finite subsets of X by $\mathrm{Sub}_{\mathrm{fin}}(X)$, then the intersection of all subgroups containing X is given by

$$\langle X \rangle = \bigcup_{X_0 \in \mathrm{Sub}_{\mathrm{fin}}(X)} \langle X_0 \rangle$$

We call it the subgroup generated by X. (You should verify that this is a subgroup of G, and this definition is an extension of the previous one.)

Definition 1.1.3 (generating subset)
Let G be an abelian group and $X \subseteq G$ be a subset. If $G = \langle X \rangle$, then we say that the subset X is a generating subset of the group G.

For example, G is a generating subset of G.

Definition 1.1.4 (finite independent subset)
Let G be an abelian group and $X \subseteq G$ be a finite subset. If the mapping

$$\mathbb{Z}^{\mathrm{Card}(X)} \xrightarrow{\kappa_X^G} \langle X \rangle, \quad (n_g)_{g \in X} \mapsto \sum_{g \in X} n_g g$$

is injective, then we say that the subset X is an independent subset of G.

Definition 1.1.5 (independent subset)
Let G be an abelian group and $X \subseteq G$ be a subset. If every finite subset X_0 of X is an independent subset of G, then we say that the subset X is an independent subset of G. (You should verify that this definition is an extension of the previous one.)

Remark 1.1.6
The mapping κ_X^G is always surjective by definition.

Example 1.1.7
The empty subset $\varnothing$ is an independent subset.

Example 1.1.8
The subset $\{g\}$ consists of only one element is an independent subset if and only if $\mathrm{ord}(g) = \infty$.

Definition 1.1.9 (basis)
Let G be an abelian group and $X \subseteq G$ be a subset. We say that X is a basis of the group G if X is a generating subset and an independent subset.

1.2 Free Abelian Groups

Definition 1.2.1 (free abelian group)
If G is an abelian group and $X \subseteq G$ is a basis of G, then we say that G is free on X. If G is an abelian group which is free on some subset $X \subseteq G$, then we say that G is a free abelian group.

Example 1.2.2
$(\mathbb{Q}_{>0}, \times)$ is free on the set of primes $\mathbb{P}$, but $\mathbb{Q}$ is not free.

Exercise 1.2.3 (Baer–Specker group)
Show that the group $\mathrm{Map}\,(\mathbb{Z}, \mathbb{Z})$ is not free.

Definition 1.2.4 (free abelian group generated by a set)
Let X be a set, we define $\mathbb{Z}X$ to be the set of all **formal** expressions of the form

$$\sum_{i=1}^{n} a_i x_i, \quad \text{where all } x_i \in X, a_i \in \mathbb{Z}$$

And the set X embed into the group $\mathbb{Z}X$ in a natural way with $\mathbb{Z}X$ free on X.

Proposition 1.2.5 ($\mathbb{Z}X$ as a free object)
For every abelian group G, the restriction

$$\operatorname{Hom}(\mathbb{Z}X, G) \xrightarrow{\bullet|_X} \operatorname{Map}(X, G)$$

is bijective. Given a mapping $f : X \to G$, we will write $f^\sharp : \mathbb{Z}X \to G$ to be the (unique) group homomorphism such that $f^\sharp|_X = f$.

Proof. Suppose $\varphi|_X = \psi|_X$, then $\varphi(x) = \psi(x)$ for all $x \in X$ so φ and ψ agrees on the generating subset X of $\mathbb{Z}X$. Hence $\varphi = \psi$.

To show that $\bullet|_X$ is surjective, we construct $f^\sharp$ explicitly by:

$$f^\sharp\left(\sum_{i=1}^n a_i x_i\right) = \sum_{i=1}^n a_i f(x_i)$$

which can be easily verified to be a group homomorphism. □

Exercise 1.2.6
Let G be an abelian group and $X \subseteq G$ be a subset. Let $j = j_X^G : X \to G$ be the inclusion mapping. Show that:

- X is a generating subset of G if and only if $j^\sharp$ is surjective.
- X is an independent subset of G if and only if $j^\sharp$ is injective.
- X is a basis of G if and only if $j^\sharp$ is bijective.

Corollary 1.2.7 (every object is a quotient of a free object)
Let G be an abelian group and X be a generating subset of G (which always exists since we can take $X = G$), then $(j_X^G)^\sharp : \mathbb{Z}X \to G$ is surjective and G is isomorphic to a quotient group of $\mathbb{Z}X$.

Example 1.2.8
Let X be a finite set with $\operatorname{Card}(X) = n$, then there are $m^n = \operatorname{Card}(\operatorname{Map}(X, \mathbb{Z}/m\mathbb{Z}))$ homomorphisms in total from $\mathbb{Z}X$ to $\mathbb{Z}/m\mathbb{Z}$.

Proposition 1.2.9
If G is an abelian group which is free on $X \subset G$, denote the inclusion $X \to G$ by j, then $j^\sharp : \mathbb{Z}X \to G$ is an isomorphism.

Conversely, if $\varphi : \mathbb{Z}X \to G$ is an isomorphism, then G is free on $\varphi(X)$.

Proof. Everything follows easily from the construction of $j^\sharp$. □

We can speak of the "dimension" of a free abelian group:

Theorem 1.2.10
Let X, Y be two finite set such that $\mathbb{Z}X \simeq \mathbb{Z}Y$, then $\operatorname{Card}(X) = \operatorname{Card}(Y)$.

Proof. Since $\mathbb{Z}X \simeq \mathbb{Z}Y$ we have $\operatorname{Card}(\operatorname{Map}(X, \mathbb{Z}/2\mathbb{Z})) = \operatorname{Card}(\operatorname{Map}(Y, \mathbb{Z}/2\mathbb{Z}))$, which implies $\operatorname{Card}(X) = \operatorname{Card}(Y)$. □

Remark 1.2.11
By Zorn's lemma, $\mathbb{Z}X \simeq \mathbb{Z}Y$ always imply $\operatorname{Card}(X) = \operatorname{Card}(Y)$ as cardinals.

Corollary 1.2.12 (dimension of a free abelian group)
Suppose G an abelian group which is free on some finite subset $X \subseteq G$, then every basis of G has the same cardinality.

Thus for **abelian groups free on some finite subset** (=FF abelian groups), a non-negative integer called the **dimension** is defined. For two FF abelian groups G, H, they are isomorphic if and only if $\dim G = \dim H$.

1.3 Structure of FF Abelian Groups

Recall that an abelian group G is FF if G is free on some finite subset $X \subseteq G$, if and only if G is isomorphic to $\mathbb{Z}Y$ for some finite set Y. And every FF abelian group has a uniquely determined dimension, which is a non-negative integer.

We start by explicitly describe all basis transformations:

Lemma 1.3.1 (base change lemma, version 1)
If $\mathbf{a}_1 = (a_{11}, a_{12}, \ldots, a_{1n}), \ldots, \mathbf{a}_n = (a_{n1}, a_{n2}, \ldots, a_{nn})$ is a basis of the group $\mathbb{Z}^n$, then the matrix $A = (a_{ij})$ has determinant $\det(A) = \pm 1$.

Proof. This is because we can write $\mathbf{e}_i = \sum_{j=1}^n b_{ij}\mathbf{a}_j$. □

Lemma 1.3.2 (base change lemma, version 2)
Let G be a FF abelian group of dimension $\dim G = n$ and $(e_1, \ldots, e_n), (\epsilon_1, \ldots, \epsilon_n)$ be two basis of G. Then there exists a matrix $A = (a_{ij}) \in \mathrm{GL}_n(\mathbb{Z})$ such that

$$e_i = \sum_{j=1}^n a_{ij}\epsilon_j$$

Proof. Left as an exercise. □

The next result explains why $\{2\} \subseteq \mathbb{Z}$ is not a basis:

Proposition 1.3.3 (height lemma)
Let G be a FF abelian group of dimension $\dim G = n$ and $0 \neq g \in G$. Then under every basis $\mathcal{B} = (b_1, \ldots, b_n)$ we can write

$$g = \sum_{i=1}^n \Gamma_i^{\mathcal{B}}(g) b_i, \text{ and we define } \mathrm{ht}_{\mathcal{B}}(g) = \gcd_{1\le i\le n}\left(\Gamma_i^{\mathcal{B}}(g)\right)$$

Then $\mathrm{ht}_{\mathcal{B}}(g) \in \mathbb{N}_+$ is independent of the choice of basis $\mathcal{B}$. We call this number the height of g and denote it by $\mathrm{ht}_G(g)$.

In particular, $\mathrm{ht}_G(b_i) = 1$ for all $b_i \in \mathcal{B}$.

Proof. Left as an exercise. □

Proposition 1.3.4
Let G be a FF abelian group of dimension $\dim G = n$ and $0 \neq g \in G$. Then there exists a basis $(e_1, \ldots, e_n)$ of G such that $g = \mathrm{ht}_G(g)e_1$.

Proof. Consider the following set:

$$\mathrm{B}^+(g) = \left\{\mathcal{B} \text{ is a basis of } G \middle| \Gamma_i^{\mathcal{B}}(g) \geq 0 \text{ for all } i\right\}$$

This set is non-empty since if we have $g = a_1 b_1 + \cdots + a_n b_n$, then

$$g = \sum_{i=1}^{n} |a_i| \left(\mathrm{sgn}(a_i) b_i\right)$$

where $(\mathrm{sgn}(a_1)b_1, \ldots, \mathrm{sgn}(a_n)b_n)$ is still a basis of G. Now for $\mathcal{B} \in \mathrm{B}^+(g)$ define

$$|g|_{\mathcal{B}} = \sum_{i=1}^{n} \Gamma_i^{\mathcal{B}}(g) \in \mathbb{N}_+$$

Then there exists a basis $\mathcal{B}_0 = (e_1, \ldots, e_n) \in \mathrm{B}^+(g)$ such that $|g|_{\mathcal{B}}$ is minimal. We claim that $\Gamma_i^{\mathcal{B}_0}(g) = 0$ for all but one i.

In fact, if for $i \neq j$ we have $\Gamma_i^{\mathcal{B}_0}(g) > 0$ and $\Gamma_j^{\mathcal{B}_0}(g) > 0$. WLOG we assume $\Gamma_i^{\mathcal{B}_0}(g) \leq \Gamma_j^{\mathcal{B}_0}(g)$, then we write

$$g = \left(\sum_{k \neq i, k \neq j} \Gamma_k^{\mathcal{B}_0}(g) e_k\right) + \left(\Gamma_j^{\mathcal{B}_0}(g) - \Gamma_i^{\mathcal{B}_0}(g)\right) e_j + \Gamma_i^{\mathcal{B}_0}(g) \left(e_i + e_j\right)$$

This tells us that after a basis transformation $(\ldots, e_i \mapsto e_i + e_j, \ldots)$, $|g|_{\mathcal{B}}$ decrease by a positive amount $\Gamma_i^{\mathcal{B}_0}(g) > 0$, which is contradictory to our choice of $\mathcal{B}_0$. So only one term of $\Gamma_i^{\mathcal{B}_0}(g)$ is nonzero.

Easy permutation of $\mathcal{B}_0$ makes $g = \mathrm{ht}_G(g) e_1$. □

Recall that an element $g \in G$ is called a torsion element if the order $\mathrm{ord}(g)$ is finite.

Definition 1.3.5 (torsion-free abelian group)
Let G be an abelian group. We say that G is torsion-free if the only torsion element of G is 0. Equivalently, if G has no non-trivial finite subgroup.

Theorem 1.3.6 (finitely generated+torsion free = free on some finite set)
Let G be a finitely generated abelian group, that is, it has at least one generating subset of finite cardinality. If G is torsion-free, then G is free on some finite subset.

Proof. Choose a generating subset $X \subset G$ with minimal cardinality, we now show that $(j_X^G)^\sharp : \mathbb{Z}X \to G$ is injective. Suppose the kernel $K = \ker(j_X^G)^\sharp$ is nontrivial, we choose a non-zero element $k \in K$ with minimal height.

Then under some basis $Y = (e_1, \ldots, e_n)$ of $\mathbb{Z}X$, we can write $k = \mathrm{ht}(k) e_1$. The inclusion $j_Y^{\mathbb{Z}X} : Y \to \mathbb{Z}X$ gives us an isomorphism $\left(j_Y^{\mathbb{Z}X}\right)^\sharp : \mathbb{Z}Y \to \mathbb{Z}X$.

If $\mathrm{ht}(k) = 1$, then $e_1 \in K$, so $\mathbb{Z}(Y \setminus \{e_1\}) \to \mathbb{Z}X \to G$ is surjective, contradictory to our choice of X. If $\mathrm{ht}(k) > 1$, then $e_1 \notin K$ by our choice of k, but then $\left(j_X^G\right)^\sharp (e_1) \in G$ is a non-zero torsion element, another contradiction. □

This theorem tells us that $\mathbb{Q}$ is not finitely generated.

1.4 Subgroups of FF Abelian Groups

We consider the following proposition:
SubFF(n): If G is a FF abelian groups of dimension $\dim G = n$ and $H \leq G$ be a nontrivial subgroup. Then the following set

$$\mathrm{SubInfo}(G,H) = \left\{ \begin{pmatrix} (e_1,\dots,e_n) \\ r \\ (d_1,\dots,d_r) \end{pmatrix} \middle| \begin{array}{c} (e_1,\dots,e_n) \text{ is a basis of } G \\ 1 \leq r \leq n \text{ is an integer} \\ d_i \in \mathbb{N}_+ \text{ with } d_i | d_{i+1}, \text{ and} \\ (d_1 e_1, \dots, d_r e_r) \text{ is a basis of } H \end{array} \right\}$$

is non-empty, and d_1 is the minimum height of all nonzero elements of H.

Proposition 1.4.1 (subgroups of $\mathbb{Z}$)
SubFF(1) is true.

Proof. A FF abelian group of dimension 1 is isomorphic to $\mathbb{Z}$. □

Theorem 1.4.2 (subgroup of FF group)
If **SubFF($n-1$)** is true, then **SubFF(n)** is true.

Proof. Choose $0 \neq h \in H$ with minimal height, and choose a basis $(e_1,\dots,e_n)$ of G such that $h = \mathrm{ht}_G(h)e_1$. We claim that: for any $h' \in H$, if we write $h' = a_1e_1 + \cdots + a_ne_n$, then $\mathrm{ht}_G(h)$ divides a_1: if $a_1 = q\mathrm{ht}(h) + r$ with $0 < r < \mathrm{ht}(h)$, then the element $h' - qh = re_1 + a_2e_2 + \cdots + a_ne_n$ has height strictly less than h, contradict to our choice of h. We claim also that $\mathrm{ht}_G(h)$ divides all a_i, for we can further modify h' to

$$h'' = h' - \frac{a_1}{\mathrm{ht}_G(h)}h + h = \mathrm{ht}_G(h)e_1 + a_2e_2 + \cdots + a_ne_n \in H$$

Then $\mathrm{ht}_G(h'')$ divides $\mathrm{ht}_G(h)$ so they must be equal by our choice of h.

We define $G_0 = \langle e_2,\dots,e_n\rangle$ and $H_0 = H \cap G_0$, then G_0 is free with dimension $\dim(G_0) = n-1$. Only consider the case where H_0 is nontrivial, we show that if $0 \neq h_0 \in H_0$ has minimal height $\mathrm{ht}_{G_0}(h_0)$, then $\mathrm{ht}_G(h)$ divides $\mathrm{ht}_{G_0}(h_0)$. Write $h_0 = a_2e_2 + \cdots + e_ne_n$, then we've already proved that $\mathrm{ht}_G(h)$ divides all a_i, so it also divides $\gcd\{a_i | i = 2,\dots,n\} = \mathrm{ht}_G(h_0) = \mathrm{ht}_{G_0}(h_0)$.

We now apply **SubFF($n-1$)** to $H_0 \leq G_0$, and get a basis $(\epsilon_2,\dots,\epsilon_n)$ of G_0, and some $d_2|d_3|\dots|d_r$ where $d_2 = \mathrm{ht}_{G_0}(h_0)$ and $(d_2\epsilon_2,\dots,d_r\epsilon_r)$ is a basis of H_0. We claim that $(e_1,\epsilon_2,\dots,\epsilon_n)$ is a basis of G and $(d_1e_1, d_2\epsilon_2,\dots,d_n\epsilon_n)$ is a basis of H where $d_1 = \mathrm{ht}_G(h)$ and $d_1|d_2$. The proof of this claim is trivial. □

Remark 1.4.3
The number d_1 divides $\mathrm{ht}_G(h)$ for all $0 \neq h \in H$.

Up to now, we know that the number d_1, D and $r = \dim(H)$ can be read from the inclusion $H \subseteq G$. We will show in next section that all d_i are unique. (A quick dirty proof is by using the Smith normal form of some $r \times n$ matrix.)

Recall that an abelian group G is finitely-generated if it has at least one generating subset with finite cardinality. Obviously every quotient of a finitely-generated (abelian) group is again finitely-generated.

Theorem 1.4.4 (subgroup of finitely-generated abelian group)
Let G be an abelian group and $X \subseteq G$ be a generating subset with n elements. Then every subgroup $H \leq G$ can be generated by at most n elements.

Proof. Consider the kernel K of the following homomorphism

$$\mathbb{Z}X \xrightarrow{j^\sharp} G \xrightarrow{\pi} G/H$$

Then $K \leq \mathbb{Z}X$ is free with dimension $\dim(K) \leq \mathrm{Card}(X)$. And $j^\sharp(K) = H$, as you should verify. $\square$

1.5 Categorical Constructions

We will take the most concrete and the most naïve approach to every categorial constructions.

1.5.1 External Sum of Abelian Groups

Definition 1.5.1 (external sum of **finitely many** abelian groups)
Let $A_1, \ldots, A_n$ be abelian groups, the external direct sum of $A_1, \ldots, A_n$ is

$$\boxplus_{i=1}^{n} A_i = \{(a_1, \ldots, a_n) | a_i \in A_i\}$$

The following canonical homomorphisms will be useful:
• The canonical inclusion homomorphism

$$\iota_i : A_i \to \boxplus_{i=1}^{n} A_i, \quad a \mapsto (0, \ldots, a, \ldots, 0) \text{ placed in the } i\text{-th entry}$$

• The canonical projection homomorphism

$$\pi_i : \boxplus_{i=1}^{n} A_i \to A_i, \quad (a_1, \ldots, a_n) \mapsto a_i$$

Theorem 1.5.2 (universal property of $\boxplus$)
The following mappings

$$\mathrm{Hom}\left(\boxplus_{i=1}^{n} A_i, B\right) \to \boxplus_{i=1}^{n} \mathrm{Hom}\left(A_i, B\right), \quad \varphi \mapsto (A_i \xrightarrow{\iota_i} \boxplus_{i=1}^{n} A_i \xrightarrow{\varphi} B)_{i=1}^{n}$$

$$\mathrm{Hom}\left(B, \boxplus_{i=1}^{n} A_i\right) \to \boxplus_{i=1}^{n} \mathrm{Hom}\left(B, A_i\right), \quad \varphi \mapsto (B \xrightarrow{\varphi} \boxplus_{i=1}^{n} A_i \xrightarrow{\pi_i} A_i)_{i=1}^{n}$$

are isomorphisms of groups.

Proof. Omitted. □

Isomorphisms of the other direction is also easy to write down:

$$\boxplus_{i=1}^{n} \operatorname{Hom}(A_i, B) \xrightarrow{\sqcup} \operatorname{Hom}\left(\boxplus_{i=1}^{n} A_i, B\right), \quad (\varphi_i)_{i=1}^n \mapsto \sum_{i=1}^{n} \left(\boxplus_{i=1}^{n} A_i \xrightarrow{\pi_i} A_i \xrightarrow{\varphi_i} B\right)$$

$$\boxplus_{i=1}^{n} \operatorname{Hom}(B, A_i) \xrightarrow{\sqcap} \operatorname{Hom}\left(B, \boxplus_{i=1}^{n} A_i\right), \quad (\varphi_i)_{i=1}^n \mapsto \sum_{i=1}^{n} \left(B \xrightarrow{\varphi_i} A_i \xrightarrow{\iota_i} \boxplus_{i=1}^{n} A_i\right)$$

1.5.2 Internal Sum of Abelian Groups

Definition 1.5.3 (direct position)
Let G be an abelian group and $H_1, \ldots, H_n$ be **finitely many** subgroups of G. Consider all inclusion mappings $j_i : H_i \to H = \sum_{i=1}^n H_i$ as one element

$$(j_i : H_i \to H)_{i=1}^n \in \boxplus_{i=1}^{n} \operatorname{Hom}(H_i, H)$$

Apply $\sqcup$ to it, we get

$$J = \bigsqcup_{i=1}^{n} \left(H_i \xrightarrow{j_i} H\right) \in \operatorname{Hom}\left(\boxplus_{i=1}^{n} H_i, \sum_{i=1}^{n} H_i\right)$$

If J is a group isomorphism, then we say the family of subgroups $\{H_i\}_{i=1}^n$ is **of direct position**.

Example 1.5.4
Let $H_i \leq G_i$, then the family $(\iota_i(H_i) \leq \boxplus_{i=1}^n G_i)_{i=1}^n$ is of direct position.

Definition 1.5.5 (internal direct sum)
Let G be an abelian group and $H_1, \ldots, H_n$ be **finitely many** subgroups of G. If the family $\{H_i\}_{i=1}^n$ is of direct position, we say that G is the (internal) direct sum of $H_1, \ldots, H_n$. We also write the following as an abbreviation

$$G = H_1 \oplus \cdots \oplus H_n = \bigoplus_{i=1}^{n} H_i$$

By definition, if G is the internal direct sum of finitely many subgroups $H_1, \ldots, H_n$, then G is isomorphic to the external sum of $H_1, \ldots, H_n$.

Theorem 1.5.6 (criterion for internal direct sum)
Let G be an abelian group and $H_1, \ldots, H_n$ be **finitely many** subgroups of G. Then G is the internal direct sum of $H_1, \ldots, H_n$ if and only if:
(1) the union $\bigcup_{i=1}^n H_i$ is a generating subset of G, and
(2) for each i, the intersection of H_i and $\langle \bigcup_{j \neq i} H_i \rangle$ is the trivial group.

Proof. Left as an exercise. □

1.6 Finitely Generated Abelian Groups

Theorem 1.6.1 (structure theorem of finitely generated abelian groups, 1)
Let G be an abelian group which can be generated by n elements, then there exists $m_1|m_2|\cdots|m_n$ with $m_i \in \mathbb{N}_{\geq 0}$ such that

$$G \simeq \boxplus_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z}$$

Proof. Say $X \subset G$ is a generating subset of cardinality n, the inclusion $X \xrightarrow{j} G$ gives us a surjective homomorphism

$$\mathbb{Z}X \xrightarrow{j^\sharp} G$$

Let K be the kernel of $j^\sharp$, and choose a datum from $\mathrm{SubInfo}(\mathbb{Z}X, K)$. Then we have a basis $(e_1, \ldots, e_n)$ of $\mathbb{Z}X$ and a sequence $d_1|d_2|\cdots|d_r$ such that $(d_1e_1, \ldots, d_re_r)$ is a basis of K.

Now we define

$$m_i = \begin{cases} d_i, & i \leq r \\ 0, & i > r \end{cases}$$

Recall that 0 is most elegant number, divisible by everything. We now claim that G is isomorphic to $\boxplus_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z}$. □

We now know that every finitely generated abelian group is isomorphic to a finite direct sum of cyclic groups. In particular, we have:

Corollary 1.6.2 (structure theorem of finite abelian groups, 1)
Every finite abelian group is isomorphic to a direct sum of finite cyclic groups.

As an application, we give the:

Corollary 1.6.3 (inverse Lagrange's theorem for finite abelian groups)
Let G be a finite abelian group and m divides the cardinality of G, then there exists a subgroup $H \leq G$ with cardinality $\mathrm{Card}(H) = m$, and there exists a subgroup $K \leq G$ such that $\mathrm{Card}(G/K) = m$.

Proof. It suffices to prove the theorem for finite cyclic groups. □

1.6.1 Chinese Remainder Theorem

Lemma 1.6.4
Let $m \in \mathbb{N}_{>1}$ be a positive integer with its unique factorization

$$m = \prod_{i=1}^{n} p_i^{v_i}$$

Consider the canonical homomorphism

$$\mathbb{Z} \xrightarrow{\varphi} \boxplus_{i=1}^{n} \mathbb{Z}/p_i^{v_i}\mathbb{Z}, \quad \varphi(x) = (x + p_i^{v_i}\mathbb{Z})_{i=1}^{n} = \left([x]_{p_i^{v_i}\mathbb{Z}}\right)_{i=1}^{n}$$

Then $\ker(\varphi) = m\mathbb{Z}$ and φ is surjective. In particular, we have

$$\mathbb{Z}/m\mathbb{Z} \simeq \boxplus_{i=1}^{n} \mathbb{Z}/p_i^{v_i}\mathbb{Z}$$

Proof. Omitted. This is elementary number theory. □

Corollary 1.6.5 (structure theorem of finitely generated abelian groups, 2)
Every finitely generated abelian group is isomorphic to a finite direct sum of cyclic p-groups $\mathbb{Z}/p^n\mathbb{Z}$ and $\mathbb{Z}$'s.

Proof. Use the Chinese Remainder Theorem to break $\mathbb{Z}/m_i\mathbb{Z}$. □

Corollary 1.6.6 (structure theorem of finite abelian groups, 2)
Every finite abelian group is isomorphic to a direct sum of cyclic p-groups.

1.6.2 Classical Constructions and Uniqueness Theorems

Definition 1.6.7 (torsion subgroup)
Let G be an abelian group, then we define G^{tor} to be the subgroup (Explain why it's a subgroup) consisting of elements of finite order.

Corollary 1.6.8 (rank of a finitely generated abelian group)
Let G be a finitely generated abelian group, then G^{tor} is a finite abelian group, G/G^{tor} is a FF abelian group, and G is isomorphic to $G^{\text{tor}} \boxplus (G/G^{\text{tor}})$.

We define the **rank** of G to be $\text{rank}(G) = \dim(G/G^{\text{tor}})$. This is an invariant of finitely generated abelian groups.

Proof. By the structure theorem, we can assume $G = G_0 \oplus G_1$ where

$$G_0 \simeq \boxplus_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z}, \quad G_1 \simeq \boxplus_{i=1}^{r} \mathbb{Z}$$

So $g \in G$ is of finite order if and only if $g \in G_0$, thus G^{tor} is a finite abelian group. The quotient group G/G^{tor} is obviously finitely generated, we now show that it is torsion-free. Suppose $g + G^{\text{tor}} \in G/G^{\text{tor}}$ is of finite order l, then element $lg \in G^{\text{tor}} \leq G$ is of finite order, so $g \in G^{\text{tor}}$. Being finitely generated and torsion-free, G/G^{tor} is a FF abelian group.

Our decomposition $G = G_0 \oplus G_1$, together with the fact that $G^{\text{tor}} = G_0$ gives us $G/G^{\text{tor}} \simeq G_1$, so G is isomorphic to $G^{\text{tor}} \boxplus (G/G^{\text{tor}})$. □

Corollary 1.6.9 (First uniqueness theorem)
Let G_1, G_2 be finite abelian groups and F_1, F_2 be FF abelian groups, such that $G_1 \boxplus F_1 \simeq G_2 \boxplus F_2$, then $G_1 \simeq G_2$ and $F_1 \simeq F_2$.

For an abelian group G, "Multiply by n" is a group homomorphism for all $n \in \mathbb{Z}$:

$$\times_G^n : G \to G$$

Definition 1.6.10 (classical constructions)
Let G be an abelian group, we define

$$nG = \operatorname{im}(\times_G^n), \quad G[n] = \ker(\times_G^n)$$

These are subgroups of G. We have tautologically the following qualities

$$G = G[0], \quad G^{\text{tor}} = \bigcup_{n \in \mathbb{N}_+} G[n]$$

For prime p, we define the p-primary subgroup $G(p)$ to be

$$G(p) = \bigcup_{n \in \mathbb{N}_+} G[p^n] \leq G^{\text{tor}}$$

If $G = G(p)$, then we say that G is a p-primary abelian group.

We define the support of an abelian group G to be

$$\operatorname{Supp}(G) = \{p \in \mathbb{P} | G(p) \neq 0\}$$

Lemma 1.6.11
Let $x, y \in G$ be two elements commute to each other,then

$$\frac{\operatorname{lcm}(\operatorname{ord}(x), \operatorname{ord}(y))}{\gcd(\operatorname{ord}(x), \operatorname{ord}(y))} \bigg| \operatorname{ord}(xy) \bigg| \operatorname{lcm}(\operatorname{ord}(x), \operatorname{ord}(y))$$

Theorem 1.6.12 (decomposition of the torsion subgroup)
Let G be an abelian group with $\operatorname{Supp}(G)$ begin a finite set, then G^{tor} is the internal direct sum of these non-trivial $G(p)$.

Proof. We need to show that the following homomorphism J is an isomorphism

$$\bigboxplus_{p \in \operatorname{Supp}(G)} G(p) \xrightarrow{J} G^{\text{tor}}, \quad (g_p)_{p \in \operatorname{Supp}(G)} \mapsto \sum_{p \in \operatorname{Supp}(G)} g_p$$

where J is given by the fusion of inclusions $j_p : G(p) \to G^{\text{tor}}$.

First we show that J is injective. By our lemma, we have

$$\operatorname{ord}\left(\sum_{p \in \operatorname{Supp}(G)} g_p\right) = \operatorname{lcm}\left\{\operatorname{ord}(g_p) | p \in \operatorname{Supp}(G)\right\}$$

So if $J\left((g_p)_{p \in \operatorname{Supp}(G)}\right) = 0$, then every element g_p has order 1 and hence trivial.

Next we show that J is surjective. If $g \in G^{\mathrm{tor}}$ with order $\mathrm{ord}(g) = m$. Write the unique factorization of m as

$$m = \prod_{i=1}^{n} p_i^{v_i}$$

The Bezout's theorem gives us some integers $t_1, \ldots, t_n$ with

$$\sum_{i=1}^{n} t_i \frac{m}{p_i^{v_i}} = 1$$

We now define $g_i = \dfrac{m}{p_i^{v_i}} g$, then $g_i \in G(p_i)$ and $g = \sum_{i=1}^{n} g_i$. $\square$

Corollary 1.6.13 (decomposition of finite abelian group)
Let G be a finite abelian group, then $\mathrm{Supp}(G)$ is finite, and

$$G = \bigoplus_{p \in \mathrm{Supp}(G)} G(p)$$

In particular, if G_1, G_2 are two finite abelian groups. Then $G_1 \simeq G_2$ if and only if $G_1(p) \simeq G_2(p)$ for all prime p.

Lemma 1.6.14
Let $G = \mathbb{Z}/m\mathbb{Z}$, and $n \in \mathbb{N}_+$. Let $n_0 = \gcd(n, m)$ and $m_0 = \frac{m}{n_0}$

$$nG \simeq \mathbb{Z}/m_0\mathbb{Z}, \quad G[n] \simeq \mathbb{Z}/n_0\mathbb{Z}$$

Proof. The subgroup nG is the image of

$$\varphi : \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/m\mathbb{Z} \xrightarrow{\times n} \mathbb{Z}/m\mathbb{Z}, \quad \varphi(1) = [n]_m$$

Easy calculation show that $\mathrm{Card}(nG) = m_0$ and hence $\mathrm{Card}(G[n]) = n_0$. $\square$

Theorem 1.6.15 (second uniqueness theorem)
Let $(n_1, \ldots, n_s)$ and $(m_1, \ldots, m_t)$ be two list of positive integers with $n_1, m_1 > 1$ and $n_i | n_{i+1}, m_i | m_{i+1}$ for all i. If

$$G = \boxplus_{i=1}^{s} \mathbb{Z}/n_i\mathbb{Z} \simeq \boxplus_{i=1}^{t} \mathbb{Z}/m_i\mathbb{Z} = H$$

Then we have $s = t$ and $n_i = m_i$ for all i.

Proof. Consider the function

$$f(k) = \mathrm{Card}(G[k]) = \mathrm{Card}(H[k])$$

which can be explicitly calculated by the lemma and gives us

$$\prod_{i=1}^{s} \gcd(k, n_i) = \prod_{i=1}^{t} \gcd(k, m_i)$$

But we have $n_i | n_{i+1}, m_i | m_{i+1}$ for all i, so the equality above is actually

$$\gcd(k, n_1) = \gcd(k, m_1), \quad \text{for all } k$$

which implies $n_1 = m_1$. Now consider $G(n_1)$ and $H(m_1)$, they are also isomorphic, and we have

$$G(n_1) \simeq \boxplus_{i=2}^{s} \mathbb{Z}/n_i\mathbb{Z}, \quad H(m_1) \simeq \boxplus_{i=2}^{t} \mathbb{Z}/m_i\mathbb{Z}$$

Apply the same method to induction. □

Corollary 1.6.16 (structure theorem of finitely generated abelian groups, 3)
Let G be a finitely generated abelian group, then there exists uniquely two non-negative integers r, s and uniquely a list of positive integers $n_1, \ldots, n_s$ with $n_1 > 1$ and $n_i | n_{i+1}$ for all i, such that

$$G \simeq \left(\boxplus_{i=1}^{s} \mathbb{Z}/n_i\mathbb{Z} \right) \boxplus \mathbb{Z}^r$$

These numbers n_i's are called the **invariant factors** of G.

Corollary 1.6.17
Let p be a prime number and $(n_1, \ldots, n_s)$ and $(m_1, \ldots, m_t)$ be two list of positive integers with $n_i \leq n_{i+1}, m_i \leq m_{i+1}$ for all i. If

$$G = \boxplus_{i=1}^{s} \mathbb{Z}/p^{n_i}\mathbb{Z} \simeq \boxplus_{i=1}^{t} \mathbb{Z}/p^{m_i}\mathbb{Z} = H$$

Then we have $s = t$ and $n_i = m_i$ for all i.

Proposition 1.6.18 (p-primary part of a finite abelian group is a p group)
Let G be a finite abelian group and p a prime. Then $G(p)$ is a finite p-group.

Proof. Use the inverse Lagrange theorem. (Suppose $q \neq p$ is a prime such that $q | \mathrm{Card}(G(p))$, then there exists a subgroup of $G(p)$ with cardinality q.) □

Corollary 1.6.19 (third uniqueness theorem)
Let G be a finitely generated abelian group, then there exists **uniquely**:

- a non-negative integer r
- for each prime $p \in \mathrm{Supp}(G)$, a non-negative integer s_p
- a list of positive integers $(n_{p,1}, \ldots, n_{p,s_p})$ with $n_{p,i} \leq n_{p,i+1}$ for all i

such that $G/G^{\mathrm{tor}} \simeq \mathbb{Z}^r$, $G \simeq G^{\mathrm{tor}} \boxplus (G/G^{\mathrm{tor}})$ and

$$G^{\mathrm{tor}} \simeq \boxplus_{p \in \mathrm{Supp}(G)} \boxplus_{i=1}^{s_p} \mathbb{Z}/p^{n_{p,i}}\mathbb{Z}$$

These numbers $n_{p,i}$'s are called the **elementary divisors** of G.

Proof. The torsion subgroup G^{tor} has the same support set as G. And the p-primary part $G^{\mathrm{tor}}(p) = G(p)$ are equal for all $p \in \mathrm{Supp}(G)$. □

We thus complete the classification of all finitely generated abelian groups.

1.7 Splitting Lemma

Definition 1.7.1 (short exact sequence)
A short exact sequence consists of three groups and two group homomorphisms, written as

$$0 \to A \xrightarrow{\alpha} G \xrightarrow{\beta} B \to 0$$

where α is injective, β is surjective, $\mathrm{im}(\alpha) = \ker(\beta)$.

Theorem 1.7.2 (splitting lemma)
Let

$$0 \to A \xrightarrow{\alpha} G \xrightarrow{\beta} B \to 0$$

be a short exact sequence of **abelian** groups. Then the following are equivalent:

1. There exists a homomorphism $\gamma : G \to A$ such that $\gamma\alpha = 1_A$
2. There exists a homomorphism $\delta : B \to G$ such that $\beta\delta = 1_B$
3. There exists an isomorphism $\varphi : G \to A \boxplus B$ such that $\varphi\alpha$ is the canonical inclusion $A \to A \boxplus B$ and $\beta\varphi^{-1}$ is the canonical projection $A \boxplus B \to B$

And we call this sequence a split exact sequence.

Proof. $\square$

1.8 Miscellanea Abelian

Chapter 2

Group Actions

Chapter 3

Small Groups

Chapter 4

Permutation Groups

Chapter 5

Linear Groups