25SG Structure of Groups

Qiu Caiyong

August 20, 2025

Preface

Later Version = Better Version.

This is the course note for the course **Group Theory II**, lectured by the author in Shenzhen Middle School, 2025. It is based on Hungerford's *Algebra*.

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

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

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 $\mathrm{Card}(X) = n$, then there are $m^n = \mathrm{Card}(\mathrm{Map}\,(X, \mathbb{Z}/m\mathbb{Z}))$ 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 $\mathrm{Card}(X) = \mathrm{Card}(Y)$.

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

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

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

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

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

where $(\operatorname{sgn}(a_1)b_1, \ldots, \operatorname{sgn}(a_n)b_n)$ 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 $\operatorname{ord}(g)$ 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

$$\mathrm{SubInfo}(G,H) = \left\{ \begin{pmatrix} (e_1,\dots,e_n) \\ r \\ (d_1,\dots,d_r) \end{pmatrix} \middle| \begin{array}{c} (e_1,\dots,e_n) \text{ is a basis of } G \\ 1 \leq r \leq n \text{ is an integer} \\ d_i \in \mathbb{N}_+ \text{ with } d_i | d_{i+1}, \text{ and} \\ (d_1e_1,\dots,d_re_r) \text{ is a basis of } H \end{array} \right\}$$

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. □

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:

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

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

1.5.2 Internal Sum of Abelian Groups

Definition 1.5.3 (direct position)
Let G be an abelian group and $H_1, \dots, H_n$ 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

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

Apply $\sqcup$ to it, we get

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

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 $H_1, \dots, H_n$ 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 $H_1, \dots, H_n$. 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 $H_1, \dots, H_n$, then G is isomorphic to the external sum of $H_1, \dots, H_n$.

Theorem 1.5.6 (criterion for internal direct sum)
Let G be an abelian group and $H_1, \dots, H_n$ be **finitely many** subgroups of G. Then G is the internal direct sum of $H_1, \dots, H_n$ 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$\frac{\mathrm{lcm}(\mathrm{ord}(x), \mathrm{ord}(y))}{\gcd(\mathrm{ord}(x), \mathrm{ord}(y))} \Bigg| \mathrm{ord}(xy) \Bigg| \mathrm{lcm}(\mathrm{ord}(x), \mathrm{ord}(y))$$

Theorem 1.6.12 (decomposition of the torsion subgroup)
Let G be an abelian group with $\mathrm{Supp}(G)$ 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

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

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

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

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

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

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

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

The Bezout's theorem gives us some integers $t_1, \dots, t_n$ 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 $g = \sum_{i=1}^{n} g_i$. □

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

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

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 $\operatorname{Card}(nG) = m_0$ and hence $\operatorname{Card}(G[n]) = n_0$. □

Theorem 1.6.15 (second uniqueness theorem)
Let $(n_1, \dots, n_s)$ and $(m_1, \dots, m_t)$ 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

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

which can be explicitly calculated by the lemma and gives us

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

Choose $k = n_1$ gives us $n_1^s = (\gcd(n_1, m_1))^t \leq n_1^t$, so $s \leq t$ and similarly $t \leq s$. So $s = t$. The equality now gives us $n_1^s = (\gcd(n_1, m_1))^s$ and hence $m_1 | n_1$ and similarly $n_1 | m_1$, 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, $\operatorname{im}(\alpha) = \ker(\beta)$.

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. □

1.8 Miscellanea Abelian

Theorem 1.8.1
Every finitely generated subgroup of $\mathbb{Q}/\mathbb{Z}$ is cyclic.

Proof. WLOG, we can assume the subgroup H is generated by

$$\frac{a_1}{N} + \mathbb{Z}, \ldots, \frac{a_n}{N} + \mathbb{Z}$$

Then H is a subgroup of the finite cyclic group $\frac{1}{N}\mathbb{Z}/\mathbb{Z}$. □

Chapter 2

Group Actions

2.1 Definitions of Group Actions

Recall that for a set X, the set of all bijections from X to X is a group

$$\mathrm{Perm}(X) = \{\pi : X \to X | \pi \text{ is bijective}\}$$

The multiplication on $\mathrm{Perm}(X)$ is given by

$$(\pi_1\pi_2)(x) = \pi_1(\pi_2(x))$$

We also introduce another group $\mathrm{Perm}^{\mathrm{op}}(X)$ whose underlying set is $\mathrm{Perm}(X)$ but the multiplication $*$ is given by

$$(\pi_1 * \pi_2)(x) = \pi_2(\pi_1(x))$$

This will be very confusing, so if $\pi \in \mathrm{Perm}^{\mathrm{op}}(X)$, we will never write $\pi(x)$ for the image of $x \in X$ under $\pi \in \mathrm{Perm}^{\mathrm{op}}(X)$. Instead, we will write x^{π}. Notice that the multiplication $*$ on $\mathrm{Perm}^{\mathrm{op}}(X)$ is now given by

$$x^{\pi_1 * \pi_2} = (x^{\pi_1})^{\pi_2}$$

So we can safely write $x^{\pi_1\pi_2}$.

Definition 2.1.1 (left action)
Let G be a group and X be a set. A left action of G on X is a group homomorphism $\alpha : G \to \mathrm{Perm}(X)$. Instead of $\alpha(g) \in \mathrm{Perm}(X)$, we simply write α_g. And instead of $\alpha_g(x)$, we simply write gx, although this may be dangerous.

The simplified notation is natural in the following sense:

$$(g_1g_2)x = \alpha_{g_1g_2}(x) = (\alpha_{g_1}\alpha_{g_2})(x) = \alpha_{g_1}(\alpha_{g_2}(x)) = g_1(g_2x)$$

If G acts on X on the left side, we also say that X is a left G-set. You should imagine X as some sort of vector space over G.

Definition 2.1.2 (right action)
Let G be a group and X be a set. A right action of G on X is a group homomorphism $\alpha : G \to \mathrm{Perm}^{\mathrm{op}}(X)$. Instead of $\alpha(g) \in \mathrm{Perm}(X)$, we simply write α_g. And instead of x^{α_g}, we simply write x^g, although this may be dangerous.

The simplified notation is natural in the following sense:

$$x^{g_1 g_2} = \alpha_{g_1 g_2}(x) = (\alpha_{g_1} * \alpha_{g_2})(x) = \alpha_{g_2}(\alpha_{g_1}(x)) = (x^{g_1})^{g_2}$$

If G acts on X on the right side, we also say that X is a right G-set. The theory of right actions is essentially the same as the theory of left actions, so we will focus mainly on the theory of left actions only. But let's introduce some important examples:

Example 2.1.3 (tautological left action)
Let $G \leq \mathrm{Perm}(X)$ be a subgroup, then the canonical injection $G \to \mathrm{Perm}(X)$ gives us a left action of G on X. And the action is given explicitly by

$$gx = g(x)$$

Example 2.1.4 (tautological right action)
Let $G \leq \mathrm{Perm}^{\mathrm{op}}(X)$ be a subgroup, then the canonical injection $G \to \mathrm{Perm}^{\mathrm{op}}(X)$ gives us a right action of G on X. And the action is given explicitly by

$$x^g = g(x)$$

Example 2.1.5 (left translation action)
Let $H \leq G$ be a subgroup, then H acts on G on the left side given by $hg = hg$.

Example 2.1.6 (right translation action)
Let $H \leq G$ be a subgroup, then H acts on G on the right side given by $gh = gh$.

Example 2.1.7 (left translation action on left coset space)
Let $H \leq G$ be a subgroup, then G (and hence all its subgroups) acts on the left cosets space on the left side given by $g(xH) = (gx)H$.

Example 2.1.8 (right translation action on right coset space)
Let $H \leq G$ be a subgroup, then G (and hence all its subgroups) acts on the right cosets space on the right side given by $(Hx)g = H(xg)$.

Example 2.1.9 (left conjugation action)
Let $H \leq G$ be a subgroup, then H acts on G on the left side given by

$$\mathrm{con}_h^{\mathrm{L}}(g) = hgh^{-1}$$

Example 2.1.10 (right conjugation action)
Let $H \leq G$ be a subgroup, then H acts on G on the right side given by

$$\mathrm{con}_h^{\mathrm{R}}(g) = h^{-1}gh$$

The left and right conjugation actions are somehow more interesting than translation actions in the sense of $\mathrm{con}_h^{\mathrm{L}}, \mathrm{con}_h^{\mathrm{R}}$ are not only a permutation of G (as a set) but actually a **group automorphism** of G.

Recall that the subset of all subgroups of a group G is denoted by $\mathrm{Sub}(G)$.

Example 2.1.11 (left conjugation action on subgroups)
Let $H \leq G$ be a subgroup, then H acts on $\mathrm{Sub}(G)$ on the left side given by

$$\mathrm{con}_h^{\mathrm{L}}(A) = hAh^{-1}$$

Example 2.1.12 (right conjugation action on subgroups)
Let $H \leq G$ be a subgroup, then H acts on $\mathrm{Sub}(G)$ on the right side given by

$$\mathrm{con}_h^{\mathrm{R}}(A) = h^{-1}Ah$$

Finally, we give three useful methods to obtain more actions

Definition 2.1.13 (product action)
Let $\alpha : G \to \mathrm{Perm}(X)$ and $\beta : G \to \mathrm{Perm}(Y)$ be two left actions, then G acts on the Cartesian product $X \times Y$ by

$$g(x, y) = (gx, gy)$$

Definition 2.1.14 (induced action)
Let $\alpha : G \to \mathrm{Perm}(X)$ be a left action, and $\varphi : H \to G$ be a group homomorphism. Then the composition $H \xrightarrow{\varphi} G \xrightarrow{\alpha} \mathrm{Perm}(X)$ is again a left action.

Definition 2.1.15 (power action)
If X is a left G-set, then the power set 2^X is also a left G-set where the action is given by

$$gX_0 = \{gx | x \in X_0\}, \quad \text{for all } X_0 \in 2^X$$

Denote the set of all n-element subsets of X by $X[n]$, then G acts on $X[n]$ by

$$gX_0 = \{gx | x \in X_0\}, \quad \text{for all } X_0 \in X[n]$$

2.2 G-Maps and G-Subsets

Recall that a left G-set X is a set X together with a left action of G on X.

Definition 2.2.1 (G-map, isomorphism of actions)
Let X, Y be two left G-sets. A map $\varphi : X \to Y$ is called a G-map if

$$f(gx) = gf(x), \text{ for all } x \in X, g \in G$$

The set of all G-maps from X to Y is denoted by $\mathrm{Map}_G(X, Y)$.

If φ is bijective, we call it a G-isomorphism. If there exists at least one G-isomorphism from X to Y, we say that X and Y are G-isomorphic.

Definition 2.2.2 (G-subset)
Let X be a left G-set and $Y \subseteq X$ be a subset. If $gy \in y$ for all $y \in Y$ and $g \in G$, we call Y a G-subset of X.

2.3 The Orbit-Stabilizer Theorem

Definition 2.3.1 (orbit)
Let X be a left G-set and $x \in X$, we define the orbit of x under G to be

$$Gx = \{gx | g \in G\}$$

This is a G-subset of X, actually the smallest G-subset containing x.

Orbits are similar to cosets in the following sense:

Theorem 2.3.2 (orbits form a partition of the G-set)
Let X be a left G-set and $x_1, x_2 \in X$. If $Gx_1 \cap Gx_2$ is non-empty, then these two orbits are equal: $Gx_1 = Gx_2$.

Definition 2.3.3 (transitive action)
Let X be a left G-set. If there exists $x \in X$ such that $Gx = X$, we say the action is transitive.

Definition 2.3.4 (stabilizer subgroup)
Let X be a left G-set and $x \in G$, we define the stabilizer of x under the action G by

$$G_x = \{g \in G | gx = x\}$$

This is a subgroup of G. We also write $\mathrm{Stab}_X(x)$ for G_x.

Definition 2.3.5 (free action, faithful action)
Let X be a G-set, we call the action a free action if $G_x = 1$ for all $x \in X$.

The homomorphism $\alpha : G \to \mathrm{Perm}(X)$ given by the action is injective if and only if

$$\bigcap_{x \in X} G_x = 1$$

And in this case, we will call the action a faithful action. By definition, any free action is faithful. (Actually, free is much stronger than faithful.)

The stabilizer subgroup construction gives us many (I'll say it's too many) important subgroups to play with

Definition 2.3.6 (centralizer)
Consider the left conjugation action of H on G. Then the stabilizer of $g \in G$ under this action is called the centralizer of g in H

$$\mathrm{C}_H(g) = \left\{h \in H \middle| \mathrm{con}_h^{\mathrm{L}}(g) = g\right\} = \{h \in H | hg = gh\}$$

For a subset $S \subseteq G$, we define the centralizer of S in H to be

$$\mathrm{C}_H(S) = \bigcap_{g \in S} \mathrm{C}_H(g) = \{h \in H | hs = sh \text{ for all } s \in S\}$$

The subgroup $\mathrm{C}_G(G)$ is called the centre of G and denoted by $\mathrm{Z}(G)$. It is always a normal subgroup of G.

Definition 2.3.7 (normalizer)
Consider the left conjugation action of H on 2^G. Then the stabilizer of the subset $S \leq G$ under this action is called the normalizer of S in H

$$\mathrm{N}_H(S) = \left\{h \in H \middle| \mathrm{con}^{\mathrm{L}}_h(S) = S\right\} = \{h \in H | hS = Sh\}$$

By definition we have $\mathrm{C}_H(S) \leq \mathrm{N}_H(S)$.

A subgroup $K \leq G$ is a normal subgroup of G if and only if $\mathrm{N}_G(K) = G$.

Let G be a group and $H \leq G$ be a subgroup, then H is normal in every subgroup contained by $\mathrm{N}_G(H)$ and containing H.

Theorem 2.3.8 (orbit-stabilizer theorem)
Let X be a G-set and $x \in X$. Then the cardinality of Gx is equal to the index $[G : G_x]$ of G_x in G, and hence divides $\mathrm{Card}(G)$.

Proof. The mapping $gG_x \mapsto gx$ is a well-defined (Explain why!) G-isomorphism between the coset space G/G_x and the orbit Gx. □

The above proof tells us that the “building blocks” of G-sets are coset spaces.

Corollary 2.3.9 (cardinality of conjugacy classes)
Consider the left conjugation action of G on G, the stabilizer of $x \in G$ is the centralizer $\mathrm{C}_G(x)$, the conjugacy class containing x, given by

$$\mathrm{Cl}_G(x) = \left\{gxg^{-1} \middle| g \in G\right\}$$

is the orbit of x under this action, and has cardinality $[G : \mathrm{C}_G(x)]$. In particular, $\mathrm{Card}(\mathrm{Cl}_G(x))$ divides $\mathrm{Card}(G)$.

Similarly, for a subgroup $H \leq G$, the set of subgroups conjugate to H

$$\mathrm{Cl}_G(H) = \left\{gHg^{-1} \middle| g \in G\right\}$$

has cardinality $[G : \mathrm{N}_G(H)]$, which again divides $\mathrm{Card}(G)$.

As a result, the cardinality of G can be written as the sum of all cardinalities of conjugacy classes of elements of G. This equality is called the **class equation** of G. The number of 1's appearing in the class equation is equal to $\mathrm{Card}(\mathrm{Z}(G))$.

Definition 2.3.10 (finite p-group)
Let p be a prime. A finite group G is called a p-group if the cardinality $\mathrm{Card}(G)$ is a power of p.

Corollary 2.3.11 (p-group has non-trivial centre)
Let G be a finite p-group, then $\mathrm{Z}(G)$ is a non-trivial subgroup of G. In particular, a finite p-group cannot be a simple group unless it is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Proof. The class equation of G must have a multiple of p number of 1. □

Remark 2.3.12
The Tarski monster group is an infinite simple p-group.

Theorem 2.3.13 (the comparison philosophy)
Let X be a left G-set and $x \in X, \gamma \in G$. Then

$$G_{\gamma x} = \mathrm{con}^{\mathrm{L}}_{\gamma}(G_x)$$

Proof. This is obvious to me. You better quit math if you never feel it. □

Theorem 2.3.14 (orbit-counting theorem)
Let X be a left G-set. The number of orbits is given by

$$\mathrm{Card}\left(\{Gx | x \in X\}\right) = \frac{1}{\mathrm{Card}(G)} \sum_{g \in G} \mathrm{Card}(\mathrm{Fix}(g))$$

where $\mathrm{Fix}(g) = \{x \in X | gx = x\}$ is the fixed points of g.

Proof. This is proved by some clever double counting. Consider the set

$$\mathrm{F} = \{(g, x) | gx = x\}$$

double counting F tells us

$$\sum_{g \in G} \mathrm{Card}(\mathrm{Fix}(g)) = \sum_{x \in X} \mathrm{Card}(G_x) = \mathrm{Card}(G) \sum_{x \in X} \frac{1}{\mathrm{Card}(Gx)}$$

Now let's look the summation

$$\sum_{x \in X} \frac{1}{\mathrm{Card}(Gx)}$$

If we sum this orbit by orbit, then for each orbit the summation is 1. □

2.4 Coset-Spaces as G-Sets

Recall that if $H \leq G$ is a subgroup, then the space of left cosets G/H is naturally a G-set. In this section, G/H will always be understood as a G-set.

Let $A, B \leq G$ be two subgroups. Suppose $\varphi : G/A \to G/B$ is a G-map, we consider the image of A under φ, denoted by $\varphi(A) = \gamma B$. Since φ is a G-map, we know that

$$\varphi(gA) = g\varphi(A) = (g\gamma)B, \quad \text{for all } g \in G$$

So all the information of φ is encoded in the coset $\gamma B \in G/B$.

But the coset γB can not be arbitrarily chosen: If $g_1 A = g_2 A$, we must have

$$g_1 \gamma B = g_2 \gamma B \iff g_1^{-1} g_2 \in \mathrm{con}^{\mathrm{L}}_{\gamma}(B)$$

That is, we should have $A \subseteq \mathrm{con}^{\mathrm{L}}_{\gamma}(B)$. Actually, this requirement is easy to understand if we rewrite it as

$$A = \mathrm{Stab}_{G/A}(A) \subseteq \mathrm{Stab}_{G/B}(\varphi(A)) = \mathrm{con}^{\mathrm{L}}_{\gamma}(\mathrm{Stab}_{G/B}(B)) = \mathrm{con}^{\mathrm{L}}_{\gamma}(B)$$

Proposition 2.4.1 (G-maps between coset-spaces)
Let $A \leq G$ be a subgroup and X be a left G-set. Then we have a bijection from

$$X^A = \{x \in X | ax = x, \text{ for all } a \in A\}$$

to the set of all G-maps $\mathrm{Map}_G(G/A, X)$, given by the following

$$\Psi_A^X : X^A \to \mathrm{Map}_G(G/A, X), \quad \Psi_A^B(x) : gA \mapsto gx$$

Proof. If $x \in X^A$, then $\Psi_A^X(x)$ is a **well-defined** map from G/A to X since whenever $g_1 A = g_2 A$, we have $g_1^{-1} g_2 \in A \Rightarrow g_1^{-1} g_2 x = x \Rightarrow g_2 x = g_1 x$. It's easy to verify that $\Psi_A^X(x)$ is a G-map.

The fact that Ψ_A^X is bijective is easy and left as an exercise. □

Corollary 2.4.2
Let G be a finite group and A, B be two subgroups.

- If A is conjugate to B, then $\mathrm{Card}\left((G/B)^A\right) = \mathrm{Card}\left((G/A)^B\right) > 0$
- If $\mathrm{Card}\left((G/B)^A\right) > 0, \mathrm{Card}\left((G/A)^B\right) > 0$, then A is conjugate to B.

Proof. If A is conjugate to B, say $A = \gamma B \gamma^{-1}$ and $B = \gamma^{-1} A \gamma$. Then

$$\Psi_A^B(\gamma B) : G/A \to G/B, \quad xA \mapsto x\gamma B$$

$$\Psi_B^A(\gamma^{-1} A) : G/B \to G/A, \quad yB \mapsto y\gamma^{-1} A$$

are G-maps, inverse to each other. Hence G/A and G/B are isomorphic, and

$$\mathrm{Card}\left((G/B)^A\right) = |\mathrm{Map}_G(G/A, G/B)| = |\mathrm{Map}_G(G/B, G/A)| = \mathrm{Card}\left((G/A)^B\right)$$

Now suppose $\mathrm{Card}\left((G/B)^A\right) > 0, \mathrm{Card}\left((G/A)^B\right) > 0$, then there exists γ_1, γ_2 such that $A \leq \mathrm{con}_{\gamma_1}^{\mathrm{L}}(B), B \leq \mathrm{con}_{\gamma_2}^{\mathrm{L}}(A)$. These are actually equalities since G is a finite group. □

Denote $\mathrm{Card}\left(\mathrm{Map}_G(A, B)\right)$ as $n([A], [B])$ where $[H] = \left\{gHg^{-1} \middle| g \in G\right\}$ is the conjugacy class containing H. Write $[A] \leq [B]$ if $n([A], [B]) > 0$, then the conjugacy classes of subgroups of G is a partially ordered set.

Consider the case G is finite and X is a left G-set which is also finite. The orbit decomposition of X gives us a function f_X

$$X \simeq \coprod_{[A]} \coprod_{i=1}^{f_X([A])} G/A$$

And if we calculate the number of G-maps from G/K to X, we have

$$X([K]) := \mathrm{Card}\mathrm{Map}_G(G/K, X) = \sum_{[A] \geq [K]} f_X([A]) n([K], [A])$$

Theorem 2.4.3 (Burnside)
Let G be a finite group. Two finite left G-sets X and Y are G-isomorphic if and only if $X([K]) = Y([K])$ for all conjugacy classes $[K]$.

Proof. This is called the Möbius inversion. (I'm not sure about this.) □

2.5 More on Automorphisms

Definition 2.5.1 (inner automorphism)
An automorphism $\varphi \in \mathrm{Aut}(G)$ is called inner, if there exists $g \in G$ such that $\varphi = \mathrm{con}^{\mathrm{L}}_g$. The set $\mathrm{Inn}(G)$ of all inner automorphisms is precisely the image of

$$G \xrightarrow{\mathrm{con}^{\mathrm{L}}} \mathrm{Aut}(G), \quad g \mapsto \mathrm{con}^{\mathrm{L}}_g$$

So $\mathrm{Inn}(G) \le \mathrm{Aut}(G)$ is a subgroup.

Since $\ker(\mathrm{con}^{\mathrm{L}} : G \to \mathrm{Aut}(G)) = \mathrm{Z}(G)$, we have $\mathrm{Inn}(G) \simeq G/\mathrm{Z}(G)$.

Remark 2.5.2
If $H \le G$ is a subgroup and $h \in H$. Then $\mathrm{con}^{\mathrm{L}}_h$ can be viewed as an element both in $\mathrm{Aut}(H)$ and $\mathrm{Aut}(G)$.

Actually, an equivalent definition of inner automorphisms is "extensible automorphisms": An automorphism $\varphi \in \mathrm{Aut}(G)$ is inner if and only if for every group extension $\widetilde{G} \ge G$, there exists $\widetilde{\varphi} \in \mathrm{Aut}(\widetilde{G})$ extending φ.

Remark 2.5.3
Let $H \le G$ be a subgroup. Even if $g \notin H$, the conjugation $\mathrm{con}^{\mathrm{L}}_h$ still acts on H if $h \in \mathrm{N}_G(H)$. In this case $\mathrm{con}^{\mathrm{L}}_h : H \to H$ may not be an inner automorphism of H, but we have the following:

Theorem 2.5.4 (NC theorem)
Let $H \le G$ be a subgroup. Then the normalizer $\mathrm{N}_G(H)$ of H in G acts on the subgroup H by conjugation. The kernel of this action

$$\mathrm{con}^{\mathrm{L}}_{H \le G} : \mathrm{N}_G(H) \to \mathrm{Aut}(H)$$

is precisely the centralizer $\mathrm{C}_G(H)$. In particular, the quotient group $\mathrm{N}_G(H)/\mathrm{C}_G(H)$ is isomorphic to some subgroup of $\mathrm{Aut}(H)$.

Proof. Trivial. □

Theorem 2.5.5 (Inn as a normal subgroup)
The group of inner automorphisms $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.

Proof. Choose $\mathrm{con}^{\mathrm{L}}_\gamma \in \mathrm{Inn}(G)$, we calculate its conjugation (by $\varphi \in \mathrm{Aut}(G)$):

$$(\varphi \circ \mathrm{con}^{\mathrm{L}}_\gamma \circ \varphi^{-1})(g) = \varphi\left(\gamma\varphi^{-1}(g)\gamma^{-1}\right) = \varphi(\gamma)g\varphi(\gamma)^{-1} = \mathrm{con}^{\mathrm{L}}_{\varphi(\gamma)}(g)$$

Which means $\mathrm{con}^{\mathrm{L}}_\varphi(\mathrm{con}^{\mathrm{L}}_\gamma) = \mathrm{con}^{\mathrm{L}}_{\varphi(\gamma)} \in \mathrm{Inn}(G)$. □

The quotient group $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the outer automorphism group $\mathrm{Out}(G)$ of G. If G is abelian, then $\mathrm{Aut}(G)$ is isomorphic to $\mathrm{Out}(G)$.

Proposition 2.5.6 (automorphisms of cyclic groups)
Every automorphism of $\mathbb{Z}/n\mathbb{Z}$ is of the form

$$[k]_n \xrightarrow{\times a} [ak]_n$$

where $\gcd(a, n) = 1$. And we have $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq \mathrm{Out}(\mathbb{Z}/n\mathbb{Z}) \simeq ((\mathbb{Z}/n\mathbb{Z})^\times, \times)$.

Theorem 2.5.7 (almost every group has an automorphism)
If $\mathrm{Aut}(G)$ is trivial, then $\mathrm{Card}(G) \leq 2$.

Proof. If G is not abelian, then $\mathrm{Inn}(G)$ is nontrivial. Now consider the case G is abelian, then the map $g \mapsto g^{-1}$ is an automorphism. Suppose even further that every element is equal to its inverse, then G is a vector space over $\mathbb{F}_2$. If the dimension is strictly greater than 1, then G has a non-trivial automorphism.

Notice that we've used the Axiom of Choice in the last step. □

Theorem 2.5.8 ($G/\mathrm{Z}(G)$ cyclic implies G abelian)
If the quotient group $G/\mathrm{Z}(G)$ is cyclic, then G is abelian and hence $G/\mathrm{Z}(G)$ is cyclic of order 1 (=trivial).

Proof. Since $\mathrm{Inn}(G) \simeq G/\mathrm{Z}(G)$ is cyclic, there exists $\gamma \in G$ such that $\mathrm{Inn}(G)$ is generated by a single element $\mathrm{con}^{\mathrm{L}}_\gamma$.

Since $\mathrm{con}^{\mathrm{L}}_\gamma(\gamma) = \gamma$ and $\mathrm{con}^{\mathrm{L}}_\gamma$ is the generator for $\mathrm{Inn}(G)$, so for any $g \in G$ we also have $\mathrm{con}^{\mathrm{L}}_g(\gamma) = \gamma$, which really means $\gamma \in \mathrm{Z}(G)$. This makes $\mathrm{con}^{\mathrm{L}}_\gamma$ the identity map and hence $\mathrm{Inn}(G)$ is trivial. □

Corollary 2.5.9
The index $[G : \mathrm{Z}(G)]$ cannot be a prime number. In particular, every group of order p^2 (where p is a prime) is abelian.

Proof. A group of prime order must be cyclic. □

Exercise 2.5.10 ($\mathrm{Out}(\mathrm{S}_n)$)
Show that if $n \neq 6$, then $\mathrm{Out}(\mathrm{S}_n)$ is trivial.

2.6 More on Actions

Theorem 2.6.1 (coset permutation representation, Cayley)
Let $H \leq G$ be a subgroup of index $[G : H] = n$. Then the core of H given by

$$\mathrm{core}_G(H) = \bigcap_{g \in G} gHg^{-1}$$

is a normal subgroup of G, and $G/\mathrm{core}_G(H)$ is isomorphic to a subgroup of S_n. If $\mathrm{core}_G(H)$ is trivial, then G is embedded into S_n in this way.

In particular, if G has any subgroup of finite index n, then G has a normal subgroup of finite index dividing $n!$.

Proof. The left translation action on cosets gives us a homomorphism

$$G \to \mathrm{Perm}(G/H) \simeq \mathrm{S}_n$$

with kernel equal to $\mathrm{core}_G(H)$. □

If $K \leq G$ is a normal subgroup. Then $K \leq H \leq G$ implies $K \leq \mathrm{core}_G(H)$.

The normal core gives us some new ways to show that a subgroup is normal:

Corollary 2.6.2 (small-prime normality theorem)
Let G be a finite group and p be the smallest prime dividing $\mathrm{Card}(G)$. Then any subgroup $H \leq G$ of index p is normal. In particular, every subgroup with index 2 is normal.

Proof. We have $[G : \mathrm{core}_G(H)] = [G : H][H : \mathrm{core}_G(H)] = p[H : \mathrm{core}_G(H)]$. We now claim that $[H : \mathrm{core}_G(H)] = 1$ and hence $H = \mathrm{core}_G(H)$ will be a normal subgroup of G.

If $l = [H : \mathrm{core}_G(H)] > 1$, say this number l is divisible by some prime number q. Since $l|\mathrm{Card}(G)$ we must have $q \geq p$.

But $G/\mathrm{core}_G(H)$ is isomorphic to the symmetric group S_p whose order is $p!$, so pl divides $p!$ and hence $q|(p-1)!$, contradict to the fact that $q \geq p$. □

Corollary 2.6.3 (big-prime normality theorem)
Let G be a finite group and $H \leq G$ be a subgroup or order p where p is a prime. If $p > [G : H]$ then H is a normal subgroup of G.

Proof. Let $l = [H : \mathrm{core}_G(H)]$, then $l = 1$ or p. If $l = 1$ then $H = \mathrm{core}_G(H)$ is normal in G. If $l = p$ then $\mathrm{core}_G(H)$ is trivial and G is isomorphic to a subgroup of S_q where $q = [G : H] < p$. Consider H which is again isomorphic to a subgroup of S_q, we have $p|q!$ which is impossible. □

Theorem 2.6.4
Let $H \leq G$ be a subgroup of finite index. Then $\mathrm{Card}((G/H)^H) = [\mathrm{N}_G(H) : H]$.

Proof. By definition,

$$(G/H)^H = \{tH | htH = tH \text{ for all } h \in H\} = \mathrm{N}_G(H)/H$$

They are equal not only as sets, but also as left $\mathrm{N}_G(H)$-sets. □

2.7 Finite p-Groups and Sylow p-Subgroups

We start this section by a simple observation: if G is a finite p-group, and G acts on some set X. Then every orbit Gx is finite of cardinality some power of the prime p. If X is a finite set, then the cardinality of the set of fixed points

$$X^G = \{x \in X | Gx = \{x\}\} = \{x \in X | gx = x \text{ for all } g \in G\}$$

is congruent to $\mathrm{Card}(X)$ modulo p: $\mathrm{Card}(X^G) \equiv \mathrm{Card}(X) \bmod p$.

This observation can be used in many clever ways. For example, if X^G is non-empty, then X^G contains at least p elements.

Theorem 2.7.1 (Cauchy's theorem)
Let G be a finite group and $\gamma \in \mathrm{Z}(G)$. Let $q = p^t$ be a power of a prime p, then the number $N_q(\gamma)$ of solutions $g \in G$ to the equation $g^q = \gamma$ is congruent to $\mathrm{Card}(G)^{q-1}$ modulo p.

In particular, if p divides $\mathrm{Card}(G)$, then there are nontrivial solutions.

Proof. If $g_1, \ldots, g_q \in G$ with $g_1 g_2 \cdots g_q = \gamma$, then

$$g_2 \cdots g_q g_1 = g_1^{-1} \gamma g_1 = \gamma$$

So $\mathbb{Z}/q\mathbb{Z}$ acts on the set $\{(g_1, \ldots, g_q) | g_1 g_2 \cdots g_q = \gamma\}$ by simply permuting the subscripts. The fixed points of this action are of the form $(g, \ldots, g)$. □

By Cauchy's theorem, if $p \in \mathrm{Supp}(G)$ is a prime number dividing the order of G, then G has a subgroup which is a p-group (simply called a p-subgroup). This subgroup arises from any nontrivial solution to the equation $g^q = 1_G$, but in general we can't conclude the order of g. The order of this (cyclic) subgroup is a power of p, but it can be just p. Can we find some larger p-subgroups?

The only restriction on the order of p-subgroups is the Lagrange's theorem: if H is a p-subgroup of G with order $q = p^u$, then q divides $\mathrm{Card}(G)$. Write the p-adic valuation of $\mathrm{Card}(G)$ simply by $v_p(G)$, then Lagrange told us $u \leq v_p(G)$.

2.7.1 Sylow's Theorems

Theorem 2.7.2 (Sylow's 1st Theorem)
For every $u \leq v_p(G)$, G contains at least one subgroup of order p^u.

Proof. Induct on u, suppose $H \leq G$ is a subgroup of order p^u and $u+1 \leq v_p(G)$, we will construct a subgroup K containing H of order p^{u+1}.

Consider the left G-set $X = G/H$, then we have $\mathrm{Card}(X^H) = [\mathrm{N}_G(H) : H]$ and it is congruent to $\mathrm{Card}(X) = [G : H]$ modulo p since H is a p-group. The fact that $u < v_p(G)$ implies that p divides the order of the quotient group $\mathrm{N}_G(H)/H$. Cauchy's theorem gives us a subgroup $L \subseteq \mathrm{N}_G(H)/H$ of order p and we lift L by the fourth isomorphism theorem to a subgroup K of $\mathrm{N}_G(H)$. Thus we have a subgroup $K \leq G$ with order $\mathrm{Card}(K) = [K : H]\mathrm{Card}(H) = p^{u+1}$. □

Sylow's first theorem actually gives us a chain of p-subgroups:

$$1 < P_1 < P_2 < \cdots < P_u \leq G, \quad \mathrm{Card}(P_u) = p^u$$

All p-subgroups of G form a lattice in general, not a chain. (Actually, if the subgroup lattice of a finite group G is a chain, then G is a cyclic p-group.) But every p-subgroup is a subconjugate of every Sylow-p-subgroup:

Theorem 2.7.3 (Sylow's 2$^{\mathrm{nd}}$ Theorem)
Let P_0 be a p-subgroup of G and P be a Sylow-p-subgroup of G. Then there exists a G-map from G/P_0 to G/P. In particular, there exists $\gamma \in G$ such that $P_0 \subseteq \mathrm{con}^{\mathrm{L}}_{\gamma}(P)$, and every two Sylow-$p$-subgroups are conjugate.

Proof. To show that X^{P_0} is non-empty where $X = G/P$, we use again the fact that P_0 is a p-group. So $\mathrm{Card}(X^{P_0}) \equiv \mathrm{Card}(X) \bmod p$. Now since P is a Sylow-p-subgroup, we have $\mathrm{Card}(X) \not\equiv 0 \bmod p$. □

The set $\mathrm{Syl}_p(G)$ of all Sylow-p-subgroups of G is transitive G-set where the action is conjugation. So the number of Sylow-p-subgroups of G is equal to $\mathrm{s}_p(G) = [G : \mathrm{N}_G(P)]$ for all $P \in \mathrm{Syl}_p(G)$. Apart from $\mathrm{s}_p(G) | \mathrm{Card}(G)$, what else do Sylow have?

Theorem 2.7.4 (Sylow's 3$^{\mathrm{rd}}$ Theorem)
The number of Sylow-p-subgroups of G is congruent to 1 modulo p.

Proof. Choose any $P \in \mathrm{Syl}_p(G)$ and let it acts on $\mathrm{Syl}_p(G)$ by conjugation. This action is **not** transitive, but $\mathrm{s}_p(G) \equiv \mathrm{Card}(\mathrm{Syl}_p(G)^P) \bmod p$ again since P is a p-group. We now show that the only fixed point is P, that is:

$$\mathrm{Syl}_p(G)^P = \left\{ Q \in \mathrm{Syl}_p(G) \middle| \mathrm{con}^{\mathrm{L}}_x(Q) = Q \text{ for all } x \in P \right\} = \{P\}$$

Say $Q \in \mathrm{Syl}_p(G)^P$, notice that $P, Q \in \mathrm{Syl}_p(\mathrm{N}_G(Q))$, so $P = \mathrm{con}^{\mathrm{L}}_y Q$ for some $y \in \mathrm{N}_G(Q)$ by Sylow's second theorem. We have $P = \mathrm{con}^{\mathrm{L}}_y Q = Q$. □

We end this section with the Frattini's argument:

Theorem 2.7.5 (Frattini)
Maybe not.

2.8 Möbius Transformations

Let $\mathbb{H} = \{z \in \mathbb{C} | \Im(z) > 0\}$ be the complex upper half plane. Then the special linear group $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathbb{H}$ in the following way:

$$\mathrm{SL}_2(\mathbb{R}) \ni \begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \mapsto \frac{az+b}{cz+d}$$

This action factors through the normal subgroup $\{\mathbf{I}_2, -\mathbf{I}_2\}$, so from now on, $\mathbb{H}$ will always be viewed as a left $\mathrm{PSL}_2(\mathbb{R})$-set. Consequently, every subgroup of $\mathrm{PSL}_2(\mathbb{R})$ also acts on $\mathbb{H}$, for example $\mathrm{PSL}_2(\mathbb{Z})$.

Chapter 3

Small Groups

Chapter 4

Permutation Groups

Chapter 5

Linear Groups