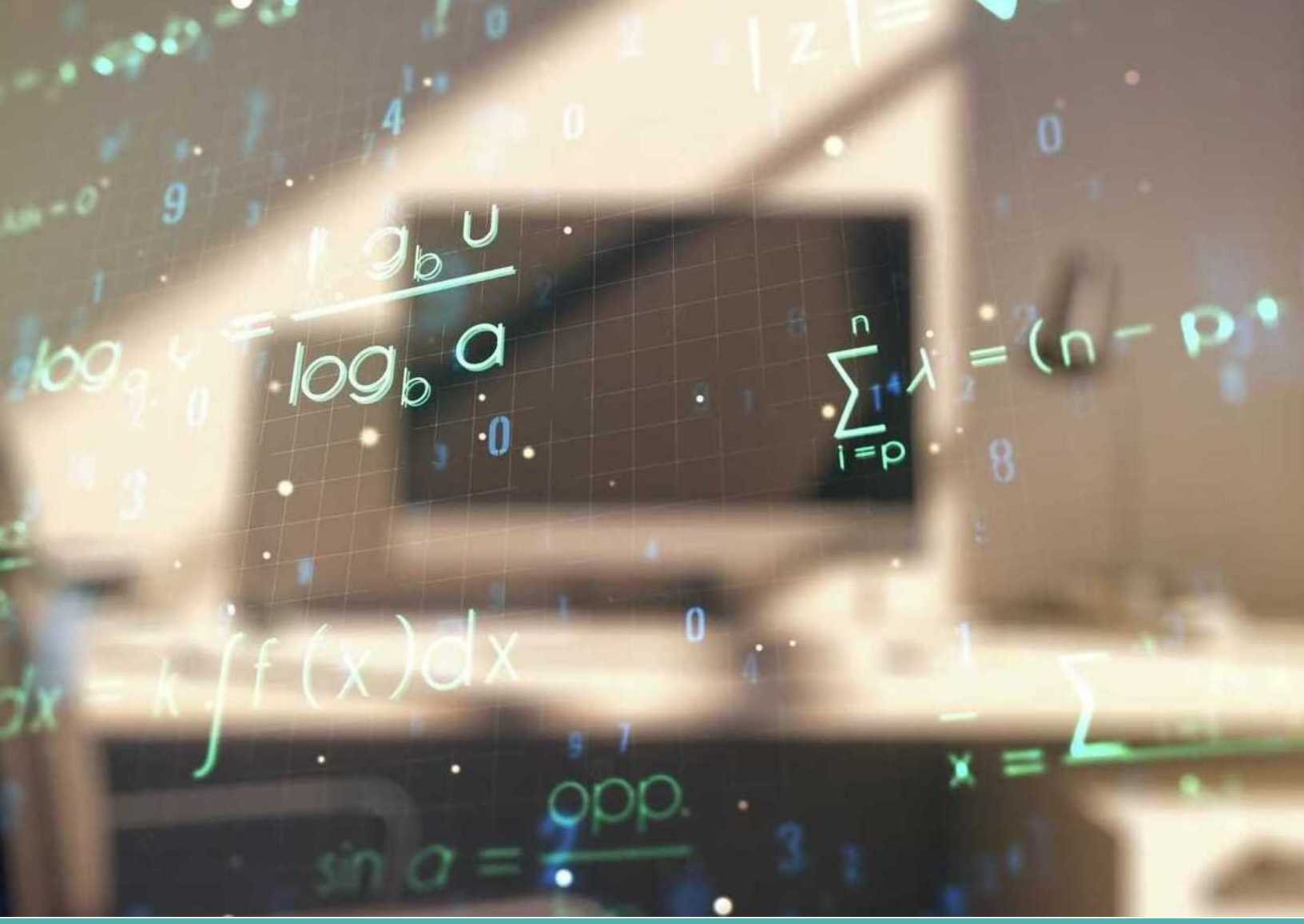


AS.110.411: Honors Algebra I

Author: Tian Zhou

Institute: Johns Hopkins University

Date: December 21, 2023

Version: 1

Year: Fall 2023

***Textbook**: Algebra: Chapter 0 - Paolo Aluffi*

Contents

Chapter 1 Preliminaries

Introduction

- ❏ *Naive Set Theory and Functions*
- ❏ *Category*
- ❏ *Morphisms*
- ❏ *Universal Properties*

1.1 Functions

1.1.1 Functions

Function The function $f : A \to B$ is a subset of $A \times B$ for which $(\forall\, a \in A)(\exists!\, b \in B), f(a) = b$. The notation B^A denotes collection of all functions from the set A to B.

If S is a subset of A, we denote by $f(S)$ the subset of B defined by $f(S) = \{b \in B \,|\, (\exists\, a \in A)\, b = f(a)\}$; in particular, $f(A)$ is the image of f, denoted by im f. We denote by $f|_S$ the *restriction* of f to S, $f|_S : S \to B$ is defined by $f|_S(x) = f(x)$ for all $x \in S$.

Composition If $f : A \to B$ and $g : B \to C$, the composition $g \circ f : A \to C$ is defined by $(g \circ f)(x) := g(f(x))$. Note that composition is associative, and the identity function id_A is the identity element in composition.

Definition 1.1 (Injection, Surjections, Bijection)

A function $f : A \to B$ is

- ***injective*** *(one-to-one) if $a \neq a' \Rightarrow f(a) \neq f(a')$, or equivalently, $f(a) = f(a') \Rightarrow a = a'$;*
- ***surjective*** *(onto) if $(\forall\, b \in B)(\exists\, a \in A)\, b = f(a)$, or equivalently, im $f = B$;*
- ***bijective*** *(one-to-one correspondence) if f is both injective and surjective.*

♣

Proposition 1.1

Assume $f : A \to B$ where $A \neq \varnothing$, then f has a left inverse if and only if it is injective, and f has a right inverse if and only if it is surjective.

♠

Proof (1) For sufficiency, suppose there is $g : B \to A$ such that $g(f(a)) = a$ for all $a \in A$. Suppose $f(a) = f(a')$, then $g(f(a)) = g(f(a'))$, implying that $a = a'$. Then f is injective. For necessity, suppose f is injective. Choose an arbitrary element $a_0 \in A$. Let $g : B \to A$ be defined by $g(b) = a$ if $f(a) = b$ for some $a \in A$, and otherwise $g(b) = a_0$. It is not hard to show g is well-defined by the injectivity of f. For all $a \in A$, $g(f(a)) = a$ by the construction of g, so f has a left inverse. The proof of right inverse is nanlogous. ■

Remark If f is injective but not surjective, it will have more than one left-inverse, and the similar statement holds if f is surjective but not injective.

Corollary 1.1

A function $f : A \to B$ is a bijection if and only if it has a inverse, denoted by f^{-1}. ♡

For $f : A \to B$ not bijective, we denote by $f^{-1}(T)$, where $T \subset B$, the subset of A of all elements that map to T, namely $f^{-1}(T) = \{a \in A \mid f(a) \in T\}$.

Consider the equivalence relation $\sim$ on A as follows: for $a, a' \in A$, $a \sim a'$ if and only if $f(a) = f(a')$, we obtain the canonical decomposition:

Proposition 1.2 (Canonical Decomposition)

Let $f : A \to B$ be a function and define $\sim$ as above. Then f decomposes as the composition of the canonical projection $A \to A/\sim$ (surjection), followed by a bijection $\bar{f} : A/\sim \xrightarrow{\sim} \operatorname{im} f$ defined by $\bar{f}([a]_\sim) = f(a)$, followed by the inclusion function $\operatorname{im} f \to B$ (injection). ♠

Remark The commutative diagram of the canonical decomposition is shown as:

$$\begin{array}{ccccc} A & \twoheadrightarrow & (A/\sim) & \xrightarrow[\bar{f}]{\sim} & \operatorname{im} f \hookrightarrow B \\ & \searrow & & \nearrow & \\ & & f & & \end{array}$$

1.1.2 Monomorphisms and Epimorphisms

Definition 1.2 (Monomorphism, Epimorphism)

*A function $f : A \to B$ is a **monomorphism** if for all sets Z and all functions $\alpha, \alpha' : Z \to A$, $f \circ \alpha = f \circ \alpha' \Rightarrow \alpha = \alpha'$; and f is an **epimorphism** if for all sets Z and all functions $\alpha, \alpha' : B \to Z$, $\alpha \circ f = \alpha' \circ f \Rightarrow \alpha = \alpha'$.* ♣

Proposition 1.3

A function is injective if and only if it is a monomorphism. A function is surjective if and only if it is a monomorphism. ♠

Remark This proposition holds only when f is a set-function.

Proof For sufficiency, suppose f is injective. Let Z be a set, $\alpha, \alpha' : Z \to A$, and $f \circ a = f \circ a'$. For all $x \in Z$, $f(\alpha(x)) = f(\alpha'(x))$, so $\alpha(x) = \alpha'(x)$ by the injectivity of f. That is, $\alpha = \alpha'$.

For necessity, suppose f is a monomorphism and $f(x) = f(x')$. Let $Z = \{p\}$ and define $\alpha, \alpha' : Z \to A$ by $\alpha(p) = x$ and $\alpha'(p) = x'$. Then $(f \circ \alpha)(p) = f(x) = f(x') = (f \circ \alpha')(p)$, so $f \circ \alpha = f \circ \alpha'$, followed $\alpha = \alpha'$ since f is a monomorphism. Therefore, $x = \alpha(p) = \alpha'(p) = x'$, it follows that f is injective.

The proof for surjective functions is analogous. ■

1.2 Category

Definition 1.3 (Category)

*A **category** $\mathcal{C}$ consists of (i) a class $Obj(\mathcal{C})$ of **objects** of the category and (ii) for every two objects A, B of $\mathcal{C}$, a set $\hom_{\mathcal{C}}(A, B)$ of **morphisms**, together with the following data:*

- ***identities**: for every object A of $\mathcal{C}$, there exists (at least one) morphism $1_A \in \hom_{\mathcal{C}}(A, A)$, the identity ($id_A$) on A, and*
- ***composition**: two morphisms $f \in \hom_{\mathcal{C}}(A, B)$ and $g \in \hom_{\mathcal{C}}(B, C)$ determine a morphism $gf \in \hom \mathcal{C}(A, C)$, the composite of g with f,*

such that the following laws holds:

- *associativity: composition is associative,*
- *unit: the identity morphism is identity with respect to composition.*

♣

Remark One further requirement is that the sets $\hom_{\mathcal{C}}$, $\hom_{\mathcal{C}}(C, D)$ is either disjoint unless $A = C$, $B = D$. The morphism of an object $A \in \mathcal{C}$ to itself is called an *endomorphism*; $\hom_{\mathcal{C}}(A, A)$ is denoted by $\mathrm{End}_{\mathcal{C}}(A)$.

Example 1.1 The sets (as objects), together with set-functions (as morphisms), form a category, and we denote by Set this category. The vector spaces together with linear maps form a category Vect.

Example 1.2 Consider the set $\mathbb{Z}$ and the relation $\leq$, the preorder on $\mathbb{Z}$, which is reflexive and transitive. We can encode this data into a category $\mathcal{C}$: for $x, y \in \mathbb{Z}$, the morphism is $\hom(x, y) = \{(x, y)\}$ if $x \leq y$ and $\hom(x, y) = \varnothing$ otherwise. The identity is defined as $(x, x) \in \hom(x, x)$, and the composition is defined as $(y, z) \circ (x, y) = (x, z)$.

Similarly, every set S along a reflexive and transitive relation forms a category. These are examples of *small categories*, since the objects in this category is a set.

Example 1.3 Let $\mathcal{C}$ be a category, and $A \in \mathrm{ob}(\mathcal{C})$. We define the *slice category*, denoted by $\mathcal{C}_A$, by the category for which:

- the objects of $\mathcal{C}_A$ are morphisms $f \in \hom_{\mathcal{C}}(Z, A)$ for some $Z \in \mathrm{ob}(\mathcal{C})$, and
- the morphisms between $f_1 \in \hom_{\mathcal{C}}(Z_1, A)$ and $f_2 : \hom_{\mathcal{C}_A}(Z_2, A)$ is defined by the triple (Z_1, Z_2, σ) where $\sigma : Z_1 \to Z_2$ satisfies that $g_1 = g_2\sigma$.

1.3 Morphisms

Definition 1.4 (Isomorphism)

*A morphism $f \in \hom_{\mathcal{C}}(A, B)$ is an **isomorphism** if it has an inverse under composition: that is, if there exists $g \in \hom_{\mathcal{C}}(B, A)$ such that $gf = 1_A$ and $fg = 1_B$.*

We say A and B are isomorphic, denoted by $A \simeq B$, if there exists an isomorphism $f : A \to B$. ♣

Remark In general, isomorphisms are not the morphisms that are both monomorphism and epimorphism.

Example 1.4

- In the category of SET, the isomorphisms are precisely the bijections.
- In the preorder category $(P, \leq)$, the isomorphisms are (x, x) where $x \in P$, namely the set of identities.
- In the category of matrices MAT, the isomorphisms are square matrices whose determinant is nonzero, this is also known as the general linear group $\mathrm{GL}(\mathbb{R})$.

Proposition 1.4

The inverse of an isomorphism is unique. ♠

Proof Suppose $f \in \hom_{\mathcal{C}}(A, B)$ is an isomorphism, and g_1, g_2 are the inverses of f. Then $g_1 = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = g_2$. ■

Proposition 1.5

- *Each identity 1_A is an isomorphism and is its own inverse.*
- *If f is an isomorphism, the f^{-1} is an isomorphism and further $(f^{-1})^{-1} = f$.*
- *If $f \in \hom_{\mathcal{C}}(A, B)$ and $f \in \hom_{\mathcal{C}}(B, C)$ are isomorphisms, then the composition gf is an isomorphism and $(gf)^{-1} = f^{-1}g^{-1}$.* ♠

An ***automorphism*** of an object A of a category $\mathcal{C}$ is an isomorphism from A to itself. The category of automorphisms of A is denoted $\mathrm{Aut}_{\mathcal{C}}(A)$, endowed with the following structures:

- the composition of $f, g \in \mathrm{Aut}_{\mathcal{C}}(A)$ is an element $gf \in \mathrm{Aut}_{\mathcal{C}}(A)$, and
- the identity is the identity morphism $1_A : A \to A$ in $\mathcal{C}$.

(Notice that $\mathrm{Aut}_{\mathcal{C}}(A)$ is a group.)

Definition 1.5 (Monomorphism, Epimorphism)

*Let $\mathcal{C}$ be a category. A morphism $f \in \hom(A, B)$ is a **monomorphism** if for all objects $Z \in ob(\mathcal{C})$ and all morphisms $\alpha', \alpha'' \in \hom(Z, A)$, $f \circ \alpha' = f \circ \alpha'' \Rightarrow a' = a''$; f is an **epimorphism** if for all objects $Z \in ob(\mathcal{C})$ and all morphisms $\beta', \beta'' \in \hom_(B, Z)$, $\beta' \circ f = \beta'' \circ f \Rightarrow \beta' = \beta''$.*

♣

Remark If a morphism f is an isomorphism, then f is monic and epic. However, the converse does not necessarily holds.

Example 1.5 In **Set**, monomorphism is equivalent to injection, and epimorphism is equivalent to surjection. However, in the category $(\mathbb{Z}, \leq)$ as described in example 1.2, every morphism is both a monomorphism and an epimorphism, but the only isomorphisms are the identities.

1.4 Universal Property

Introduction The universal property generalize constructions, such as cartesian product and quotient, uniquely up to isomorphism. Although the constructions may not exists for arbitrary objects in a general category, it is a more flexible notion.

Definition 1.6 (Initial Objects, Final Objects)

*Let $\mathcal{C}$ be a category. An object I of $\mathcal{C}$ is said to be **initial** if for every object $A \in ob(\mathcal{C})$, there exists an unique morphism in $\hom_{\mathcal{C}}(I, A)$; F is said to be **final** if for all for every object $A \in ob(\mathcal{C})$, there exists an unique morphism in $\hom_{\mathcal{C}}(A, F)$.*

♣

Example 1.6 Initial and final objects do not necessarily exists in a category, consider $(\mathbb{Z}, \leq)$.

In Set, the empty set $\varnothing$ is the unique initial object, and every singleton is final in Set.

Proposition 1.6

Let $\mathcal{C}$ be a category.

- *If I_1, I_2 are both initial objects in $\mathcal{C}$, then $I_1 \cong I_2$.*
- *If F_1, F_2 are both final objects in $\mathcal{C}$, then $F_1 \cong F_2$.*

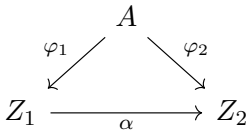
Further, these isomorphisms are uniquely determined.

♠

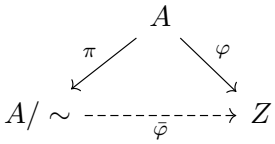
Proof Since I_1 and I_2 are initial, $f : I_1 \to I_2$ and $g : I_2 \to I_1$ are unique. Notice that $g \circ f \in \hom(I_1, I_1) = \{\mathrm{id}_{I_1}\}$ since I_1 is initial, so $g \circ f = \mathrm{id}_{I_1}$. Without loss of generality, $f \circ g = \mathrm{id}_{I_2}$. It follows that f is an isomorphism because g is its inverse, so $I_1 \cong I_2$. The proof for final objects is analogous. ■

Example 1.7 Let $A/\sim$ be a quotient set of a set A by equivalence relation $\sim$. Define the category as follows:

- The objects are (Z, φ) where $\varphi : A \to Z$ is a morphism in $\mathcal{C}$ such that for all $a, a' \in A$, $a \sim a' \Rightarrow \varphi(a) = \varphi(a')$.
- The morphisms $\alpha : (Z_1, \varphi_1) \to (Z_2, \varphi_2)$ are morphisms $\alpha : Z_1 \to Z_2$ such that

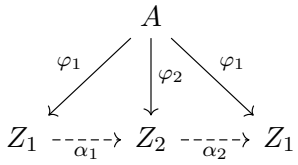


Let $\pi : A \to A/\sim$ be the canonical projection, then $(A/\sim, \pi)$ define an initial object. In other word, $(A/\sim, \pi)$ is universal with the property with respect to the property of mapping A to a set in such a way that equivalent elements have the same image.



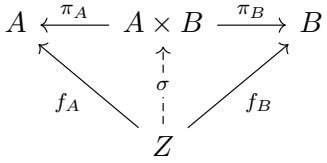
Remark The universal property defines the universal morphisms unique up to a unique isomorphism. For instance,

in the above example, suppose Z_1, Z_2 both satisfy the universal property,



Then composition $\alpha_1 \circ \alpha_2$ is unique since Z_1 is an initial object, so $\alpha_1 \circ \alpha_2 = \mathrm{id}_{Z_1}$, hence $Z_1 \cong_{\alpha_1} Z_2$.

Example 1.8 The product of two sets can also be constructed using the universal property.



In other words, products of sets together with projection, namely $(A \times B, \pi_A, \pi_b)$, are final objects in the category $\mathcal{C}_{A,B}$.

Chapter 2 Group Theory I

Introduction

- ❏ *Group*
- ❏ *Free Groups and Subgroups*
- ❏ *Lagrange Theorem*
- ❏ *Group Actions*
- ❏ *Group Homomorphisms*
- ❏ *Normal Subgroup and Quotient Group*
- ❏ *Isomorphism Theorems*

2.1 Definition of Group

2.1.1 Group

Let G be a nonempty set, the **binary operation** endowed in G is a "multiplication" map: $\cdot : G \times G \to G$. We commonly denote $g \cdot h$ or gh by the mapping of (g, h) by $\cdot$.

Definition 2.1 (Group $(G, \cdot)$)

*The set, endowed with the binary operation $\cdot$, denoted $(G, \cdot)$, is a **group** if*

*(a) **Associativity**: the operation $\cdot$ is associative, that is, for all $g, h, k \in G$, $(g \cdot h) \cdot k = g \cdot (h \cdot k)$.*

*(b) **Identity**: there exists an identity element e_G for $\cdot$, that is, for all $g \in G$, $e_G \cdot g = g = g \cdot e_G$.*

*(c) **Inverse**: every element in G has an inverse with respect to $\cdot$, that is, for all $g \in G$, there exists $h \in G$ such that $h \cdot g = e_G = g \cdot h$. We usually denote g^{-1} by the inverse of g.*

*A group $(G, \cdot)$ is **abelian** (commutative group) if $(G, \cdot)$ is forms a group and the operation $\cdot$ is commutative.* ♣

Example 2.1 $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are common examples of group; indeed, they are abelian groups (commutative group).

The set of $n \times n$ invertible matrices with real entries, denoted by $GL_n(\mathbb{R})$ (general linear group), is an example of non-commutative group.

Proposition 2.1

The identity element and inverse are unique. ♠

Proof (1) Suppose e_G and e'_G are identity elements, then $e_G = e_G e'_G = e'_G$.

(2) Suppose g and g' are inverses of $f \in G$, then $g = g(fg') = (gf)g' = g'$. ■

In addition, the cancellation holds in groups, that is, $ga = ha \Rightarrow g = h$ and $ag = ah \Rightarrow g = h$.

2.1.2 Order

Definition 2.2 (Order)

*An element of g if a group G has **finite order** if $g^n = e$ for some $n \in \mathbb{Z}_{>0}$. In this case, the **order** $|g|$ is the least positive n such that $g^n = e$. If g does not have finite order, we write $|g| = \infty$.*

*If G is a finite set, its **order** $|G|$ is the number of its element, we write $|G| = \infty$ if G is infinite.*

♣

Proposition 2.2

Let $g \in G$ be an element of finite order, then $g^n = e$ if and only if $|g|$ divides n.

♠

Proof Suppose $|g| \nmid n$. We can write $n = q \cdot |g| + r$ for some $q, r \in \mathbb{Z}_{\geq 0}$ such that $0 < r < |g|$. Then

$$g^r = g^{n-q\cdot|g|} = g^n \cdot (g^{|g|})^{-q} = e \cdot e^{-q} = e$$

contradicting that $|g|$ is the order of g. The converse is obvious. ■

Proposition 2.3

Let $g \in G$ be an element of finite order, then g^m has finite order for all $m \geq 0$, and in fact $|g^m| = |g|/\gcd(m, |g|) = lcm(m, |g|)/m$.

♠

Proof Let $d = \gcd(m, |g|)$. By the definition of $|g^m|$, $g^{m\cdot|g^m|} = e$, so $|g| \mid (m \cdot |g^m|)$, thus $(|g|/d) \mid |g^m|$. Conversely, since $d \mid m$, then $(g^m)^{|g|/d} = (g^{|g|})^{m/d} = e^{m/d} = e$, so $|g^m| \mid (|g|/d)$. Hence $|g^m| = |g|/d$. ■

Note ***Proposition**: If $gh = hg$, then $|gh| \mid lcm(|g|, |h|)$.*

2.1.3 Examples of groups

Symmetric Group Let A be a set. The ***symmetric group***, or group of permutation of A, denoted S_A, is the group $\mathrm{Aut}_{\mathbf{Set}}(A)$. The group of permutation of the set $\{1, \cdots, n\}$ is denoted by S_n.

The groups S_A are large, for instance, $|S_n| = n!$. It worth to note that the multiplication fg is defined to be the composition $g \circ f$. In other words, we adopt the convention of writing functions *after* the element, for instance, $(p)(fg) = (g \circ f)(p)$ for $p \in A$. In addition, the commutativity does not necessarily hold.

Dihedral Groups A "symmetry" is a transformation which preserves a structure. The ***dihedral groups*** may be defined as the groups of symmetries for the regular polygons. The dihedral group for regular n-sided polygon, denoted D_{2n}, includes n rotations by $2\pi/n$ radians and n reflections.

Cyclic Groups and Modular Arithmetic Define the ***congruence modulo n*** on $\mathbb{Z}$ by $a \equiv b \pmod{n}$ if and only if $n \mid (b - a)$. The equivalence classes is $\mathbb{Z}_n$.

By defining $[x] + [y] = [x + y]$, the structure $(\mathbb{Z}_n, +)$ becomes an abelian group. The abelian group we obtained is called ***cyclic groups***, denoted C_n, which is the group generated by one element x with the relation $x^n = e$. In $(\mathbb{Z}_+, +)$, a generator is $[1]_n$. It follows immediately from Proposition (2.3) that $|[m]_n| = |m \cdot [1]_n| = n/\gcd(m, n)$, and thus $[m]_n$ generated $\mathbb{Z}_n$ if and only if $\gcd(m, n) = 1$.

By defining $[x] \cdot [y] = [xy]$, and let $\mathbb{Z}_n^\times = \{[m]_n \in \mathbb{Z}_n \mid \gcd(m, n) = 1\}$. We recognize the structure $(\mathbb{Z}_n^\times, \cdot)$ as an abelian group.

2.2 The Category of Grp

For two groups $(G, \cdot)$ and $(H, *)$, a ***group homomorphism*** $\varphi : (G, \cdot) \to (H, *)$ is a function between groups that preserves the structure, and in this case the diagram below commutes.

$$\begin{array}{ccc} G \times G & \xrightarrow{\varphi \times \varphi} & H \times H \\ \downarrow{\scriptstyle \cdot} & & \downarrow{\scriptstyle *} \\ G & \xrightarrow{\varphi} & H \end{array}$$

Definition 2.3 (Group Homomorphism)

*The set function $\varphi : (G, \cdot) \to (H, *)$ is a **group homomorphism** if for all $a, b \in G$, $\varphi(a \cdot b) = \varphi(a) * \varphi(b)$.* ♣

Definition 2.4 (Grp)

The category of Grp is a category whose (a) objects of Grp are groups, and (b) for every pair of groups G, H, the morphisms $\hom_{Grp}(G, H)$ are the set of group homomorphisms $G \to H$. ♣

We now need to verify Grp is well-defined. Suppose G, H, K are groups and $\varphi : G \to H$, $\psi : H \to K$ are group homomorphisms, then the composition $\psi \circ \varphi : G \to K$ is a group homomorphism:

$$(\psi \circ \varphi)(a \cdot_G b) = \psi(\varphi(a) \cdot_H \varphi(b)) = (\psi \circ \varphi)(a) \cdot_K (\psi \circ \varphi)(b).$$

It is obvious that composition is associative and that the identity function $\mathrm{id}_G : G \to G$ is a group homomorphism. Therefore, Grp is indeed a category.

Proposition 2.4

Let $\varphi : G \to H$ be a group homomorphism. Then

(a) $\varphi(e_G) = e_H$;

(b) $\forall\, g \in G$, $\varphi(g^{-1}) = \varphi(g)^{-1}$. ♠

Remark The group homomorphism preserves the structure, in particular, the identity element e and the inverse.

Proof (a) $\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G)$, implying that $\varphi(e_G) == e_H$ by the cancellation.

(b) $\varphi(g^{-1}) \cdot \varphi(g) = \varphi(g^{-1} \cdot g) = e_H = \varphi(g)^{-1} \cdot \varphi(g)$, implying that $\varphi(g^{-1}) = \varphi(g)^{-1}$ by the cancellation. ■

Proposition 2.5

With operation defined componentwise, $G \times H$ is a product in Grp. ♠

The category of abelian groups Ab is a category whose objects are abelian groups and whose morphisms are group homomorphism.

2.3 Group Homomorphisms

Example 2.2 Suppose G is a group, the conjugation $\gamma_g : G \to G$, $a \mapsto gag^{-1}$, is a group homomorphism and indeed an isomorphism. The left translation $\lambda_g : G \to G$, $a \mapsto ga$, is a bijection but not a group homomorphism. The group action $\lambda : G \to S_G$, $\lambda : g \mapsto \lambda_g$, is a group homomorphism.

Proposition 2.6

Let $\varphi : G \to H$ be a group homomorphism, and let $g \in G$ be an element of finite order. Then $|\varphi(g)|$ divides $|g|$.

♠

Proof Note that $\varphi(g)^{|g|} = \varphi(g^{|g|}) = \varphi(e_G) = e_H$, then $|\varphi(g)|$ divides $|g|$. ■

Example 2.3 There is no nontrivial homomorphism $\varphi : C_4 \to C_7$. The orders of elements in C_4 divide 4 and the order of elements in C_7 divide 7, so $\varphi(g)$ divides both 4 and 7, implying that $\varphi(g) = e$ for all $g \in C_4$.

Definition 2.5 (Isomorphisms, Isomorphic)

*An **isomorphism** of groups $\varphi : G \to H$ is an isomorphism in Grp, i.e., a group homomorphism admitting an inverse $\varphi^{-1} : H \to G$.*

*Two groups G, H are **isomorphic** in Grp if there is an isomorphism $G \to H$.*

♣

Proposition 2.7

Let $\varphi : G \to H$ be a group homomorphism. Then φ is an isomorphism of groups if and only if it is a bijection.

♠

Proof Suppose φ is an isomorphism, then it is a bijection. Conversely, suppose φ is a bijective homomorphism. There exists an inverse $\varphi^{-1} : H \to G$ of φ in Set. For all $h_1, h_2 \in H$, $h_1 = \varphi(g_1)$ and $h_2 = \varphi(g_2)$ for some g_1, g_2, then

$$\varphi^{-1}(h_1 \cdot h_2) = \varphi^{-1}(\varphi(g_1) \cdot \varphi(g_2)) = \varphi^{-1}(\varphi(g_1 \cdot g_2)) = g_1 \cdot g_2 = \varphi^{-1}(h_1) \cdot \varphi^{-1}(h_2).$$

Thus, φ^{-1} is a homomorphism, so φ is an isomorphism. ■

Definition 2.6 (Cyclic Group)

A group G is cyclic if it is isomorphic to $\mathbb{Z}$ or to $C_n = \mathbb{Z}/n\mathbb{Z}$ for some n.

♣

Remark Equivalently, G is a cyclic group if and only if $G = \{g^n \mid n \in \mathbb{Z}\}$ for some $g \in G$.

Example 2.4 For example, $C_2 \times C_3$ is cyclic of order 6, since $C_2 \times C_3 \simeq C_6$. More generally, $C_m \times C_n$ is cyclic if $\gcd(m, n) = 1$.

If p is prime, the group $(\mathbb{Z}_p^*, \cdot)$ is cyclic.

Proposition 2.8

Let $\varphi : G \to H$ be an isomorphism,

- *For all $g \in G$, $|\varphi(g)| = |g|$.*
- *G is abelian if and only if H is abelian.*

♠

Proof The first assertion follows from $|\varphi|$ divides $|g|$ and $|g| = |\varphi^{-1}(\varphi(g))|$ divides $|\varphi(g)|$ by Proposition (2.6). For the second assertion, suppose $h_1 = \varphi(g_1)$ and $h_2 = \varphi(g_2)$, then $h_1h_2 = \varphi(g_1g_2) = \varphi(g_2g_1) = h_2h_1$ if and only if $g_1g_2 = g_2g_1$. ■

Remark "Homomorphism" in Grp correspond to "continuous" map in topology, and "isomorphism" corresponds to "homeomorphism". Two groups being isomorphic means that the underlying structure of the groups is identical.

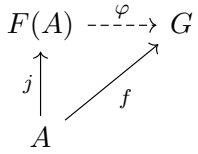
2.4 Free Groups

2.4.1 Universal Property

Motivation The motivation of free groups is that given a set A, we want to construct a smallest group $F(A)$ containing A such that the elements of A have no special group-theoretic property. For instance, if $A = \{a\}$ is a singleton, $F(A) = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ is the infinite cyclic group generated by a.

Universal Property Consider the coslice category $\mathcal{F}^A$ whose objects are pairs (j, G) and the morphisms are group homomorphisms.

In the language of universal property, $F(A)$ is a ***free group*** on set A if there is a set-function $j : A \to F(A)$ such that for all $G \in \textsc{Grp}$ and $f : A \to G$, there exists a unique group homomorphism $\varphi : F(A) \to G$ such that



That is, the *free group* $F(A)$ on A is an initial object in $\mathcal{F}^A$, up to isomorphism.

Example 2.5 Infinite cyclic groups $\mathbb{Z}$ satisfies the universal property for free groups over a singleton. Indeed, define $j : a \to 1$, for all G and $f : a \mapsto g$, homomorphism condition forces $\varphi(n) = g^n$.

2.4.2 Free Group Construction

Let A be a set, thought as an alphabet consisting of letters $a \in A$. Let $A' = \{a^{-1} \mid a \in A\}$ be the set of formal inverses, we have $A \cong A'$ and $A \cap A' = \varnothing$. A ***word*** over A is a juxtaposition of letters $w = a_1 a_2 \cdots a_n$ where $a_i \in A \cup A'$, and the ***empty word*** is $\varepsilon = ()$. We call $l(w) = n$ the ***length*** of n, and $W(A)$ the set of (finite) words w over A.

Let $r : W(A) \to W(A)$ be the ***elementary reduction map***: suppose $w \in W(A)$, r searches and remove the first occurrence of a pair aa^{-1} or $a^{-1}a$ in w. Note that $r(w) = w$ if and only if w cannot be reduced, we called w a ***reduced word***.

Proposition 2.9

If $w \in W(A)$ has length n, then $r^{\lfloor n/2 \rfloor}(w)$ is a reduced word. ♠

We may define the reduction $R : W(A) \to W(A)$ by $R(w) = r^{\lfloor n/2 \rfloor}(w)$ where n is the length of w. Then the binary operation on $F(A)$ by juxtaposition and reduction can be defined, as $w \cdot w' = R(ww')$. It is not hard to verify $(F(A), \cdot)$ is a group if $F(A) = \operatorname{im} W(A)$.

Proposition 2.10

Let $j : A \to F(A)$ be defined by sending the element $a \in A$ to the word $w = a \in W(A)$. The pair $(j, F(A))$ satisfies the universal property for free groups on A.

Proof We can extend $\varepsilon : F(A) \to G$ to the set-function $\tilde{\varphi} : W(A) \to G$ such that $\tilde{\varphi}(a) = f(a)$ for $a \in A \cup A'$ and compatible with juxtaposition $\tilde{\varphi}(ww') = \tilde{\varphi}(w)\tilde{\varphi}(w')$, and the reduction is invisible $\tilde{\varphi}(R(w)) = \tilde{\varphi}(w)$. Note that φ agrees with $\tilde{\varphi}$ on reduced words, we have $\varphi(w \cdot w') = \tilde{\varphi}(R(ww')) = \tilde{\varphi}(ww') = \tilde{\varphi}(w)\tilde{\varphi}(w') = \varphi(w)\varphi(w')$. ■

Remark We need to extend φ to $\tilde{\varphi}$ because the reduction inside φ is not well-defined, so we cannot conclude $\varphi(R(ww')) = \varphi(w)\varphi(w')$.

Remark Therefore, we can define the set of all reduced words in $W(A)$ to be the free group of set A (up to isomorphism).

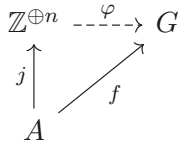
2.4.3 Free Abelian Group

Suppose $A = \{1, \cdots, n\}$, denote by $\mathbb{Z}^{\oplus n}$ the direct sum $\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$. We view $\mathbb{Z}^{\oplus n}$ as the coproduct where $j : A \to \mathbb{Z}^{\oplus}$ is defined by $j(i) = (0, \cdots, 0, 1, 0, \cdots, 0)$ (1 is on the i-th index).

Proposition 2.11

For $A = \{1, \cdots, n\}$, $\mathbb{Z}^{\oplus n}$ is a free abelian group on A.

Proof Note that every element of $\mathbb{Z}^{\oplus n}$ can be written uniquely in the form $\sim_{i=1}^{n} m_i j(i)$. Define $\varphi : \mathbb{Z}^{\oplus n} \to G$ by $\varphi(\sum m_i j(i)) = \prod f(i)^{m_i}$. This definition is unique because of the commutativity of the diagram



and by the homomorphism condition, as desired. ■

For the general case: if A is a set, define $H^{\oplus A} := \{\alpha : A \to H \mid \alpha(a) = e_H$ for all but finitely many elements $a \in A\}$, that is, $H^{\oplus A}$ is an A-indexed finite tuple. For $H = \mathbb{Z}$, the natural function $j : A \to \mathbb{Z}^{\oplus A}$ is obtained by sending $a \in A$ to $j_a : A \to \mathbb{Z}$ such that

$$j_a(x) := \begin{cases} 1 & \text{if } x = a \\ 0 & \text{if } x \neq a \end{cases}$$

making $H^{\oplus A}$ as a coproduct.

Corollary 2.1

For every set A, $F^{ab}(A) \cong \mathbb{Z}^{\oplus A}$.

2.5 Subgroups

2.5.1 Subgroups

Definition 2.7 (Subgroup)

*Let $(G, \cdot)$ be a group and $(H, \cdot)$ be another group whose underlying set H is a subset of G. $(H, \cdot)$ is a **subgroup** of G, denoted by $H \leq G$, if the inclusion function $i : H \to G$ is a group homomorphism.* ♣

Remark The operation of a subgroup H is induced by the operation $\cdot$ in G (by the property of homomorphism). In addition, $(H, \cdot)$ is a subgroup of $(G, \cdot)$ if and only if

(a) H contains the identity element, namely $1 \in H$, and

(b) H is closed under multiplication and inverse.

Theorem 2.1

A nonempty subset H of a group G is a subgroup if and only if $ab^{-1} \in H$ for all $a, b \in H$. ♡

Proof ($\Rightarrow$) This direction is obvious because a subgroup is closed under multiplication and inverse.

($\Leftarrow$) Suppose $ab^{-1} \in H$ for all $a, b \in H$. The associativity in H follows immediately from the associativity in G. H contains the identity element since for an arbitrary $h \in H$, $e_G = hh^{-1} \in H$. Inverse is closed: if $h \in H$, then $h^{-1} = e_G h^{-1} \in H$ for all h. In addition, multiplication is closed: if $h_1, h_2 \in H$, then $h_2^{-1} \in H$, so $h_1 h_2 = h_1 (h_2^{-1})^{-1} \in H$. Hence H is a subgroup. ■

Proposition 2.12

Arbitrary intersections of subgroups is a subgroup. In other words, if $\{H_\alpha\}_{\alpha \in A}$ is a family of subgroups of a group G, then $H = \bigcap_{\alpha \in A} H_\alpha$ is a subgroup of G. ♠

Proof H is nonempty because $1 \in H$. The proposition follows immediately from Proposition 2.1 since for all $\alpha \in A$ and $a, b \in H$, $a, b \in H_\alpha$, so $ab^{-1} \in H_\alpha$ for all $\alpha \in A$, thus $ab^{-1} \in H$. ■

Proposition 2.13

Let $\varphi : G \to G'$ be a group homomorphism, and let H' be a subgroup of G'. Then $\varphi^{-1}(H')$ is a subgroup of G. ♠

Proof For all $a, b \in \varphi^{-1}(H')$, $\varphi(a), \varphi(b) \in H'$, so does $\varphi(a)\varphi(b)^{-1} = \varphi(ab^{-1})$, thus $ab^{-1} \in \varphi^{-1}(H')$. The statement therefore follows from Proposition 2.1. ■

Definition 2.8 (Subgroup Generated by a Subset)

If $A \subset G$ is a subset, there exists a unique homomorphism $\varphi_A : F(A) \to G$ by the universal property of free groups, compatible with the inclusion map. Then im φ_A is the ***subgroup generated by A****, denoted by $\langle A \rangle$.*

Note *Equivalently, the subgroup generated by A is the intersection of all subgroups of G containing A, namely $\langle A \rangle = \bigcap_{A \subset H \leq G} H$.*

If $A = \{g\}$ is a singleton, then $\langle A \rangle = \{g^n \mid n \in \mathbb{Z}\}$.

Example 2.6 G is a subgroup of $\mathbb{Z}$ if and only $G = d\mathbb{Z}$ for some $d \in \mathbb{N}$. The proof involves using Euclid division lemma to prove that G is can be generated by a singleton.

Let G be a subgroup of $\mathbb{Z}_n$ for some $n \in \mathbb{Z}_{>0}$, then G is a cyclic subgroup generated by $d + n\mathbb{Z}$ for some $d \mid n$.

2.5.2 Kernel and Image

Definition 2.9 (Kernel, Image)

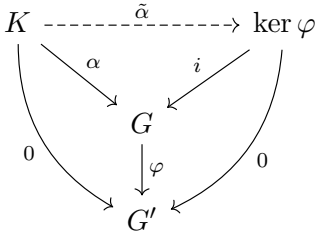
The ***kernel*** *of group homomorphism $\varphi : G \to G'$ is a subset of G consisting of elements mapping to the identity in G': $\ker \varphi := \{g \in G \mid \varphi(g) = e_{G'}\} = \varphi^{-1}(e_{G'})$.*

The ***image*** *is defined to be im $\varphi = \{g' \in G' \mid \exists\, g \in G,\ \varphi(g) = g'\}$.*

Proposition 2.14

Let $\varphi : G \to G'$ be a homomorphism. Then the inclusion $i : \ker \varphi \hookrightarrow G$ is final in the category of group homomorphism $\alpha : K \to G$ such that $\varphi \circ \alpha$ is the trivial map.

That is, there exists a unique $\tilde{\alpha}$ such that the below diagram commutes:



Proof If $\alpha : K \to G$ us such that $\varphi \circ \alpha = 0$, then $\text{im}(\varphi \circ \alpha) = \{0\}$ implies im $\alpha \subset \ker \varphi$. Therefore, $\tilde{\alpha}$ defined by $\tilde{\alpha}(k) = \alpha(k)$ satisfies the commutativity of the diagram, and it is the only map such that $\tilde{\alpha} \circ i = \alpha$. ■

Proposition 2.15

The following are equivalent:

(a) φ is a monomorphism;

(b) $\ker \varphi = \{e_G\}$;

(c) $\varphi : G \to G'$ *is injective (as a set-function).*

Remark For analogous statement of epimorphism, see Proposition 2.25.

Proof $(a) \Rightarrow (b)$: Consider $i : \ker \varphi \to G$ be the inclusion map and $e : \ker \varphi \to G$ be the trivial homomorphism,

$$\ker \varphi \underset{e}{\overset{i}{\rightrightarrows}} G \xrightarrow{\varphi} G'$$

then $\varphi \circ i = \varphi \circ e$ since both are trivial homomorphisms. The monomorphism condition implies that $i = e$, so $\ker \varphi = \text{im } e = \text{im } i = \{e_G\}$.

$(b) \Rightarrow (c)$: Suppose $\ker \varphi = \{e_G\}$ and $\varphi(g_1) = \varphi(g_2)$. Then

$$\varphi(g_1) = \varphi(g_2) \Rightarrow \varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = e_{G'} \Rightarrow g_1 g_2^{-1} \in \ker \varphi = \{e_G\} \Rightarrow g_1 = g_2,$$

followed by φ is injective.

$(c) \Rightarrow (a)$: Suppose φ is injective, φ is a monomorphism in Set. Since φ is a group homomorphism, and in particular, $\varphi \circ \alpha = \varphi \circ \alpha' \Leftrightarrow \alpha = \alpha'$ holds if α, α' are homomorphisms, so φ is a monomorphism in Grp. ■

2.6 Quotient Groups

2.6.1 Normal Subgroups and Cosets

Definition 2.10 (Normal Subgroups)

*A subgroup N of a group G is **normal** if for all $g \in G$ and $n \in N$, $gng^{-1} \in N$. We denote by $N \trianglelefteq G$ if N is a normal subgroup of G.*

♣

Remark Equivalently, a subgroup is normal if and only if $gN = Ng$ for all $g \in G$.

Proposition 2.16

If $\varphi : G \to G'$ is a group homomorphism, then $\ker \varphi$ is a normal subgroup of G.

♠

Proof Suppose $n \in \ker \varphi$ and $g \in G$, then $\varphi(gng^{-1}) = \varphi(g)\varphi(n)\varphi(g)^{-1} = \varphi(g)e_{G'}\varphi(g)^{-1} = e_{G'}$, so $gng^{-1} \in \ker \varphi$. ■

Proposition 2.17

Suppose $\sim$ is an equivalence relation on G. The operation $[a] \cdot [b] = [ab]$ defines a group structure on $G/\sim$ if and only $a \sim a' \Rightarrow ga \sim ga'$ and $ag \sim a'g$ for all $a, a', g \in G$.

In this case the quotient function $\pi : G \to G/\sim$ is a homomorphism and is universal with respect to homomorphisms $\varphi : G \to G'$ such that $a \sim a' \Rightarrow \varphi(a) = \varphi(a')$.

♠

We say that $\sim$ is *compatible* with the group structure of G if the condition above holds.

Proof Sketch: (a) $a \sim a' \Rightarrow ga \sim ga'$ and $ag \sim a'g$ holds if and only the operation is well-defined, and then it is not hard to verify the group structure.

(b) Since $G/\sim$ satisfies the corresponding universal property in Set, there exists an unique function $\tilde{\varphi} : G/\sim \to G'$ defined by $[a] \to \varphi(a)$, and $\tilde{\varphi}$ is a homomorphism because φ is a homomorphism. Hence $((G/\sim), \pi)$ is initial. ■

Definition 2.11 (Cosets)

*The **left-cosets** of a subgroup H in a group are the sets aH, for $a \in G$. The **right-cosets** of H are the sets Ha, for $a \in G$.*

♣

2.6.2 Quotient Groups

We will analyze the properties of $a \sim a' \Rightarrow ga \sim ga'$ and $a \sim a' \Rightarrow ag \sim a'g$ separately.

Proposition 2.18

Let $\sim$ be an equivalence relation on a group G, satisfying $a \sim b \Rightarrow ga \sim gb$ for all $g, a, b \in G$, then

- *the equivalence class of e_G is a subgroup H of G; and*
- *$a \sim b \Leftrightarrow a^{-1}b \in H \Leftrightarrow aH = bH$.*

Conversely, if H is a subgroup of G, the relation $\sim_L$ defined by $a \sim_L b \Leftrightarrow a^{-1}b \in H$ is an equivalence relation satisfying $a \sim b \Leftrightarrow ga \sim gb$.

♠

Proof (a) Suppose $a, b \in H$, namely $a \sim b \sim e_G$. Since $b^{-1} = e_G b^{-1} \sim bb^{-1} = e_G$, then multiplying a on left yields $ab^{-1} \sim ae_G \sim e_G$, followed by $ab^{-1} \in H$, so H is a subgroup.

(b) Suppose $a \sim b$, multiply by a^{-1} on the left gives $a^{-1}b \sim e_G$, so $a^{-1}b \in H$. Since the multiplication is closed, $a^{-1}bH \subset H$, thus $aH \subset bH$. Without loss of generality, $bH \subset aH$, so $aH = bH$. Conversely, suppose $aH = bH$, then $a = ae_G \in bH$, so $a^{-1}b \in H$, thus $a \sim b$.

(c) It is trivial to prove $\sim_L$ is an equivalence relation. To prove the it satisfies the given property, $a \sim_L b \Rightarrow a^{-1}b \in H \Rightarrow (ga)^{-1}(gb) = a^{-1}b \in H \Rightarrow ga \sim_L g_b$. ■

Proposition 2.19

There is a one-to-one correspondence between subgroups of G and equivalence relations on G satisfying $a \sim b \Rightarrow ga \sim gb$; for the relation $\sim_L$ corresponding to a subgroup H, $G/\sim_L$ may be described as the set of left-cosets aH of H.

♠

Proof Follows directly from Proposition 2.18. ■

The preceding two proposition for right cosets are analogous.

Proposition 2.20

The relations $\sim_L$ and $\sim_R$ coincides if and only if H is normal.

♠

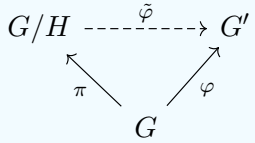
Definition 2.12 (Quotient Group)

*Let H be a normal subgroup of a group G. The **quotient group** of G modulo H, denoted G/H, is the group $G/\sim$ obtained from the relation $\sim$. In terms of cosets, the product G/H is defined by $(aH)(bH) = (ab)H$, and the identity element $e_{G/H}$ is the coset of the identity.*

♣

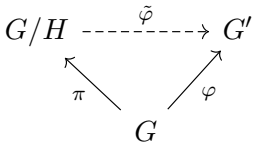
Proposition 2.21

Let H be a normal subgroup of a group G, then for every group homomorphism $\varphi : G \to G'$ such that $H \subset \ker \varphi$ there exists a unique group homomorphism $\tilde{\varphi} : G/H \to G'$ so that the diagram



commutes.

Proof $H \subset \ker \varphi$ implies $a^{-1}b \in H \Rightarrow \varphi(a) = \varphi(b)$. By the definition of relation $\sim$ corresponding to H, then $a \sim b \Rightarrow a^{-1}b \Rightarrow \varphi(a) = \varphi(b)$. Hence by Proposition 2.17 there is an unique desired homomorphism $\tilde{\varphi}$. ■



2.7 Canonical Decomposition and Lagrange's Theorem

2.7.1 Canonical Decomposition and Isomorphism Theorems

Proposition 2.22

Every group homomorphism $\varphi : G \to G'$ may be decomposed as follows:

$$G \twoheadrightarrow G/\ker\varphi \xrightarrow[\tilde{\varphi}]{\sim} \mathit{im}\,\varphi \hookrightarrow G' \qquad (G \xrightarrow{\varphi} G')$$

where the isomorphism $\tilde{\varphi}$ in the middle is the homomorphism induced by φ. ♠

Theorem 2.2 (First Isomorphism Theorem)

Suppose $\varphi : G \to G'$ is a surjective group homomorphism. Then $G' \cong G/\ker\varphi$. ♡

Proof Since $\operatorname{im}\varphi = G'$, it follows that $\tilde{\varphi}$ is an isomorphism between $G/\ker\varphi$ and $\operatorname{im}\varphi = G'$. ■

Proposition 2.23

If $H_1 \trianglelefteq G_1$ and $H_2 \trianglelefteq G_2$, then $H_1 \times H_2 \trianglelefteq G_1 \times G_2$, and $(G_1 \times G_2)/(H_1 \times H_2) \cong (G_1/H_1) \times (G_2/H_2)$. ♠

Proof Define $\pi = \pi_1 \times \pi_2 : G_1 \times G_2 \to (G_1/H_1) \times (G_2/H_2)$ explicitly by $\pi(g_1, g_2) = (g_1H_1, g_2H_2)$, i.e., the product of compositions between projection and morphism to the quotient; $\tilde{\pi}$ is a surjective homomorphism whose kernel is $H_1 \times H_2$, the proposition follows immediately from Theorem 2.2. ■

Example 2.7 The cyclic group C_6 can be identified as $C_2 \times C_3$, so $C_6/C_3 \cong (C_2 \times C_3)/C_3 \cong C_2$.

The cyclic group C_3 can be viewed as a subgroup of the dihedral group C_6. Then C_3 is normal in D_6 and $D_6/C_3 \cong C_2$.

Presentation Every group is a quotient of a free group, and every abelian group is a quotient of a free abelian group. A ***presentation*** of a group G is an explicit isomorphism $G \cong F(A)/R$ where $A \in \textsc{Set}$ and R is a subgroup relations; that is, a presentation is an explicit surjection $\rho : F(A) \twoheadrightarrow G$ of which R is the kernel.

A presentation is usually encoded as a pair $(A \,|\, \mathcal{R})$, where A is a set and $\mathcal{R} \subset F(A)$ is a set of words such that $\ker\rho = R$ is generated by $\mathcal{R}$.

Example 2.8 The symmetry group S_3 can be presents as a quotient of the free group $F(\{x, y\})$ by the smallest normal subgroup containing x^2, y^3, and $yx = xy^2$, namely S_3 is $(x, y \,|\, x^2, y^3, xyxy)$.

Proposition 2.24

Suppose $H \trianglelefteq G$, then for every $K \leq G$ containing H, K/H may be identified with a subgroup G/H. The function

$$u : \{\text{subgroups } K \text{ of } G \text{ containing } H\} \to \{\text{subgroups of } G/H\}$$

defined by $u(K) = K/H$ is a bijection preserving inclusions. ♠

Remark In other words, every subgroup H' of G/N can be written as $H' = H/N$ for some $H \leq G$.

Proof For every subgroup K containing H, $K/H = \{aH \,|\, a \in K\} \subset G/K$, then it is not hard to verify $K/H \leq G/H$ since $aH, bH \in K/H \Rightarrow a, b \in H \Rightarrow ab^{-1} \in H \Rightarrow (aH)(bH)^{-1} \in K/H$.

u preserves inclusions: if $H \subset K \subset K'$, $u(K) = K/H \subset K'/H = u(K')$. Define $v(K') = \{a \in G \,|\, aH \in K'\}$ for every $K' \leq G/H$. It is not hard to show $v(K')$ is a subgroup and v is the inverse of u. Hence u is a bijection preserving inclusions. ■

Theorem 2.3 (Second Isomorphism Theorem)

Denote by AB the subset $AB := \{ab \,|\, a \in A, b \in B\}$. Let $H \trianglelefteq G$ and $K \leq G$. Then

(a) HK is a subgroup of G, and H is normal in HK;

(b) $H \cap K$ is normal in K, and $HK/H \cong K/(H \cap K)$. ♡

Proof (a) Suppose $k_1h_1, k_2h_2 \in HK$. Note that H is normal, so $k_1(h_1h_2^{-1}) = h'k_1$ for some $h' \in H$. Then $(k_1h_1)(k_2h_2)^{-1} = (k_1h_1h_2^{-1})k_2^{-1} = h'k_1k_2 \in HK$, so HK is a subgroup of G. It is clear that H is normal in $HK \leq G$.

(b) $H \cap K$ is clearly normal in K since $H \trianglelefteq G$. Consider $\varphi : K \to HK/H$ defined by $\varphi(k) = Hk$. φ is surjective: for all $Hhk \in HK/H$, $Hhk = Hk = \varphi(k)$. The kernel of φ is $\ker\varphi = \{k \in K \,|\, \varphi(k) = Hk = H\} = H \cap K$. Hence $K/(H \cap K) \cong HK/H$ by the first isomorphism theorem. ■

Theorem 2.4 (Third Isomorphism Theorem)

Let $H \leq N \leq G$ for which $H \trianglelefteq G$. Then N/H is normal in G/H if and only if N is normal in G, and in this case, $(G/H)/(N/H) \cong G/N$. ♡

Proof N/H is normal if and only if for all $gH \in G/H$ and $nH \in N/H$, $(gH)(nH)(gH)^{-1} = (ghg^{-1})H \in N/H$, which holds if and only if $ghg^{-1} \in N$, namely $N \trianglelefteq G$ by definition.

In this case, define $\varphi : G/H \to G/N$ by $\varphi(gH) = gN$. φ is well-defined because $g_1H = g_2H \Longrightarrow g_1g_2^{-1} \in H \subset N \Longrightarrow g_1N = g_2N$. φ is surjective because for all $gN \in G/N$, $\varphi(gH) = gN$. The kernel of φ is $\ker\varphi = \{gH \,|\, gN = N\} = \{gH \,|\, g \in N\} = N/H$. Hence $(G/H)/(N/H) = (G/H)/\ker\varphi \cong G/N$ by the first isomorphism theorem. ■

2.7.2 The Lagrange Theorem

Definition 2.13 (Index)

*The notation G/H denote the set of left-cosets of H, regardless of whether H is normal in G. The **index** of H in G, denoted $[G : H]$, is the number of elements $|G/H|$ of G/H, when this is finite, and ∞ otherwise.* ♣

Theorem 2.5 (Lagrange's Theorem)

If G is a finite group and $H \subset G$ is a subgroup, then $|G| = [G : H] \cdot |H|$. In particular, $|H|$ is a divisor of $|G|$. ♡

Proof For all $g \in G$, the function $\lambda_g : H \to gH$ defined by $\lambda_g(h) = gh$ is clearly a bijection, so $|H| = |gH|$. Note that G is the disjoint union of $[G : H]$ distinct cosets gH, so $|G| = [G : H] \cdot |gH| = [G : H] \cdot |H|$. ■

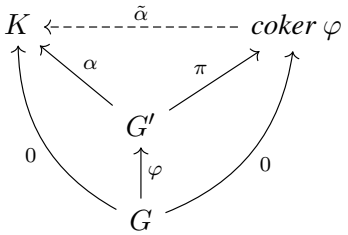
Example 2.9

- The order $|g|$ if any element g of a finite group G is a divisor of $|G|$, indeed, $|g|$ equals the order of subgroup $\langle g \rangle$ generated by g.
- If $|G|$ is a prime integer p, the necessarily $G \cong \mathbb{Z}_p$.

Note *The index is multiplicative: if $H \leq K \leq G$, then $[G : H] = [G : K][K : H]$, provided that the indices are finite. By second isomorphism theorem, if $H \trianglelefteq G$ and $K \leq G$, then $|HK| = (|H| \cdot |K|)/|H \cap K|$.*

2.7.3 Epimorphisms and Cokernels

Note *Define the cokernel coker φ equipped with a homomorphism $\pi : G' \to \operatorname{coker} \varphi$ to be the universal solution to*



In Ab, $\operatorname{im} \varphi$ is a subgroup and hence a normal subgroup of G', so $\operatorname{coker} \varphi \cong G'/\operatorname{im} \varphi$. However, $\operatorname{im} \varphi$ is not necessarily normal in Grp. Let's consider the abelian case:

Proposition 2.25

Let $\varphi : G \to G'$ be a homomorphism of abelian groups. The following are equivalent:

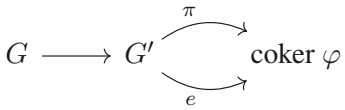
(a) φ is an epimorphism;

(b) $\operatorname{coker} \varphi$ is trivial;

(c) $\varphi : G \to G'$ is surjective (as a set-function); ♠

Remark For analogous statement of monomorphisms, see Proposition 2.15.

Proof $(a) \Rightarrow (b)$: Suppose φ is an epimorphism, consider $\pi : G' \to G'/\text{im } \varphi$ defined by $\pi(g) = g \text{ im } \varphi$ and the trivial homomorphism e. The following diagram commutes:



so $\pi = e$, it follows that coker φ is trivial.

$(b) \Rightarrow (c)$: Suppose coker $\varphi = G'/\text{im } \varphi$ is trivial, im $\varphi = G'$, so φ is surjective.

$(c) \Rightarrow (a)$: Suppose φ is surjective, it is an epimorphism in SET. In particular, $\alpha \circ \varphi = \alpha' \circ \varphi$ implies $\alpha = \alpha'$ if α and α' are homomorphisms, so φ is an epimorphism in GRP. ■

2.8 Group Actions

2.8.1 Group Actions

Definition 2.14 (Group Action)

*An **action** of group G on an object A of a category $\mathcal{C}$ is a homomorphism $\sigma : G \to Aut_{\mathcal{C}}(A)$, it is **faithful** (or **effective**) if $\sigma : G \to Aut_{\mathcal{C}}(A)$ is injective.*

Definition 2.15 (Group Action on a Set)

An action of a group G on a set A is a set-function $\rho : G \times A \to A$ such that

(a) $\rho(e_G, a) = a$ for all $a \in A$, and

(b) for all $g, h \in G$ and for all $a \in A$, $\rho(gh, a) = \rho(g, \rho(h, a))$.

Remark That is, if we denote g acts on a by $g \bullet a$, then (a) $e_G \bullet a = a$ and (b) $(gh) \bullet a = g \bullet (h \bullet a)$.

We can define $\sigma : G \to S_A = \text{Aut}(A)$ by $\sigma(g)(a) = \rho(g, a)$. This function preserves the operation $\sigma(gh)(a) = \sigma(g) \circ \sigma(h)(a)$, and the image of σ consists of invertible set-functions since $\sigma(g^{-1})$ acts as the inverse of $\sigma(g)$. Hence $\sigma : G \to S_A$ is a desired homomorphism. Indeed, there is a bijection between the set of actions and the set of actions on a set, implying that the two definitions are equivalent.

Note *The action is faithful if and only if the identity e_G is the only element g of G such that $g \bullet a = a$ for all $a \in A$.*

Example 2.10

- The *left translation* $\rho : G \times G \to G$ defined by $\rho(g, h) = gh$ is a group action of G on itself.
- The conjugation action defined by $\rho(g, h) = ghg^{-1}$ is another action of G on itself.
- The left translation of left cosets $\rho(g, aH) = (ga)H$ is an action of G on G/H.

Proposition 2.26 (Cayley's Theorem)

Every group acts faithfully on some set. That is, every group may be realized as a subgroup of a permutation group.

Proof The action of left-multiplication $\sigma : G \to \text{Aut}_{\text{GRP}}(G)$ defined by $\sigma(g)(h) = gh$ is a faithful group action. ■

Definition 2.16 (Transitive Action, Free Action)

*An action of a group G on a set A is **transitive** if for all $a, b \in A$, there exists $g \in G$ such that $b = g \bullet a$.*

*An action is **free** if e_G is the only element fixing any element of A.*

Definition 2.17 (Orbit, Stabilizer)

*The **orbit** of $a \in A$ under an action of group G is the set $O_G(a) := \{g \bullet a \mid g \in G\}$. The **stabilizer** subgroup of $a \in A$ consists of element of G which fix a, i.e., $Stab_G(a) := \{g \in G \mid g \bullet a = a\}$.* ♣

2.8.2 The Category of G-Set

The Category of G-Set For every group G, sets endowed with a G-action form a category G-Set: the objects are pairs (ρ, A) where $\rho : G \times A \to A$ is an action, and morphisms between objects are set-functions which are compatible with the actions. That is, a morphism $(\rho, A) \to (\rho', A')$ in G-Set amounts to a set-function $\varphi : A \to A'$ such that the diagram

$$\begin{array}{ccc} G \times A & \xrightarrow{\mathrm{id}_G \times \varphi} & G \times A' \\ {\scriptstyle \rho}\downarrow & & \downarrow{\scriptstyle \rho'} \\ A & \xrightarrow[\varphi]{} & A' \end{array}$$

commutes. That is, $g \bullet \varphi(a) = \varphi(g \bullet a)$ (such functions are called ***equivariant***). The isomorphisms of G-Set are indeed the equivariant bijections.

Proposition 2.27

Every transitive left-action of G on a set A is isomorphic to the left-multiplication of G on G/H for $H = Stab_G(a)$ of any $a \in A$. ♠

Proof Define $\varphi : G/H \to A$ by $\varphi(gH) = g \bullet a$. φ is well-defined: $g_1 H = g_2 H \Rightarrow g_1 g_2^{-1} \in H \Rightarrow g_1 g_2^{-1} \bullet a = a \Rightarrow g_1 \bullet a = g_2 \bullet a$. Since $\varphi(g'(gH)) = g' \bullet \varphi(gH)$, φ is equivariant. To verify φ is bijective, define $\psi : A \to G/H$ by $\psi(g \bullet a) = gH$, this is well-defined because the action is transitive, and it is clear that ψ and φ are inverse of each other, so φ is bijective. ■

Remark The above proposition implies that $O_G(a)$ and $G/\mathrm{Stab}_G(a)$ are bijective. Then the Orbit-Stabilizer theorem $|G| = |O_G(a)| \cdot |\mathrm{Stab}_G(a)|$ follows immediately.

Proof: Define $\varphi : G/H \to O_a$ (where $H = \mathrm{Stab}_G(a)$) by $\varphi(g) = g \bullet a$. Note that

$$x_1 H = x_2 H \Leftrightarrow x_1^{-1} x_2 \in H \Leftrightarrow x_1^{-1} x_2 \bullet a = a \Leftrightarrow \varphi(x_1 H) = x_1 \bullet a = x_2 \bullet a = \varphi(x_2 H),$$

thus, the mapping φ is well-defined and injective. It is clearly surjective. Hence φ is a bijection. ■

Corollary 2.2

If $O_G(a)$ is an orbit of the action of a finite group G in a set A, then $O_G(a)$ is finite and $|O_G(a)|$ divides $|G|$. ♡

Proposition 2.28

Suppose a group acts on a set A, and let $a \in A$, $g \in G$, $b = g \bullet a$. Then $Stab_G(b) = gStab_G(a)g^{-1}$.

Proof Suppose $h \in \text{Stab}_G(a)$, note that $a = g^{-1} \bullet b$, then $(ghg^{-1}) \bullet b = gh \bullet a = g \bullet a = b$, so $g\text{Stab}_G(a)g^{-1} \subset \text{Stab}_G(b)$. The inclusion of other direction follows without loss of generality. ■

Remark In other words, the stabilizers of an action are isomorphic if they are in the same class (i.e., they have the same orbit).

Chapter 3 Group Theory II

Introduction

- ❏ *Center, Centralizer, and Normalizer*
- ❏ *Sylow Theorems*
- ❏ *Class Formula*
- ❏ *Semidirect Product*
- ❏ *Symmetric Group, Alternating Group*
- ❏ *Classification of Finite Abelian Group*

3.1 The Conjugation Action

3.1.1 Center, Centralizer, Conjugacy Classes

Definition 3.1 (Center)

*The **center** of G, denoted $Z(G)$, is the subgroup* $\ker \sigma$ *of G, where σ is the conjugate action. In other words,* $Z(G) := \{g \in G \mid \forall\, a \in G : ga = ag\}$.

♣

Remark For conjugate action, the center $Z(G)$ fixes every element $g \in G$ when acting on itself, and they are fixed points G acts on them. That is, for all $a \in G$, $g \bullet a = a$ and $a \bullet g = g$.

Remark $Z(G)$ is abelian and thus normal in G.

Lemma 3.1

Let G be a finite group, if $G/Z(G)$ is cyclic, then G is commutative and hence $G/Z(G)$ is trivial.

♡

Proof Suppose $G/Z(G)$ is generated by $xZ(G)$. For all $g_1 \in G$, $g_1 \in x^m Z(G)$ so $g_1 = x^n h_1$ for some $h_1 \in Z(G)$. Similarly, $g_2 = x^m h_2$ for $h_2 \in Z(G)$. Then

$$g_1 g_2 = (x^n h_1)(x^m h_2) = x^{n+m} h_1 h_2 = (x^m h_2)(x^n h_1) = g_2 g_1,$$

so G is commutative. ■

Definition 3.2 (Centralizer of a)

*The **centralizer** of $a \in G$ is its stabilizer under conjugation, namely* $Z_G(a) = \{g \in G \mid gag^{-1} = a\} = \{g \in G \mid ga = ag\}$.

♣

Remark The centralizer $Z_G(a)$ fixes a when acting as conjugate action on itself, and they are fixed when a acts on them. That is, $g \bullet a = a$ and $a \bullet g = g$

Definition 3.3 (Conjugacy Class)

*The **conjugacy class** of $g \in G$ is the orbit $[g]$ of g under the conjugation action. Two elements $g, h \in G$ are **conjugate** if they belong to the same conjugacy class.*

♣

Remark Normal subgroup of a group is a disjoint union of conjugacy classes.

3.1.2 Class Formula

Proposition 3.1 (Class Formula)

Let G be a group acting on a finite set S, and Z be the fixed points of the action. Then $|S| = |Z| + \sum_{a \in A}[G : G_a]$, where $A \subset G$ is a set containing one representative for each nontrivial orbit in G.

In particular, when considering the conjugation action of G on itself, we have

$$|G| = |Z(G)| + \sum_{a \in A}[G : Z_G(a)]$$

*as known as the **class formula**.*

♠

Proof The orbit form a partition of S, and Z collects the trivial orbits, so $|S| = |Z| + \sum_{a \in A} |O_a|$. Note that $|O_a| = |G/G_a| = [G : G_a]$ by Proposition 2.27, this yields the desired formula. ■

Definition 3.4 (p-group)

*A **p-group**, where p is prime, is a finite group G such that $|G| = p^n$ for some $n \in \mathbb{Z}$.*

♣

Corollary 3.1

(a) Let G be a p-group acting on a finite set A, and let Z be the fixed point set, then $|Z| \equiv |S| \pmod{p}$.

(b) Let G is be a nontrivial p-group, then $Z(G)$ is nontrivial.

♡

Proof (a) Since $O_a \cong G/G_a$ is a nontrivial subgroup of S, so p divides $[G : G_a]$. Then $|S| = |Z| + \sum_{a \in A}[G : G_a] \equiv |Z| \pmod{p}$.

(b) By part (a) and the class formula, $|Z(G)| \equiv |G| \equiv 0 \pmod{p}$, so $Z(G)$ is nontrivial. ■

3.1.3 Conjugation of Subsets and Subgroups

The ***conjugation*** of A is the subset gAg^{-1}, and it is not hard to verify that $A \cong gAg^{-1}$.

Definition 3.5 (Centralizer and Normalizer of A)

*The **normalizer** $N_G(A)$ of A is its stabilizer under conjugation, i.e., $N_G(A) := \{g \in G \,|\, gA = Ag\}$. The **centralizer** of A is the subgroup $Z_G(A) \subset N_G(A)$ fixing each element of A, i.e., $Z_G(A) := \{g \in G \,|\, \forall\, a \in$*

$A : ga = ag\}$. ♣

Remark Centralizer and normalizer of a subgroup A of G are subgroups of G, and $Z_G(A)$ is a normal subgroup of $N_G(A)$.

In addition, if A is a subgroup of G, then A is the largest normal subgroup in $N_G(A)$.

Lemma 3.2

Let $H \subset G$ be a subgroup. Then (if finite) the number of subgroups conjugate to H equals the index $[G : N_G(H)]$ of the normalizer of H in G. ♡

Proof Consider the group action defined by $g \bullet A = gAg^{-1}$. Note that $\text{Stab}_G(H) = \{g \in G \,|\, gAg^{-1} = A\} = N_G(H)$, then the orbit-stabilizer theorem gives that $|\{gAg^{-1} \,|\, g \in G\} = ||O_A| = [G : N_G(G)]$. ■

3.2 Symmetric Group

3.2.1 Cycles and Types

Definition 3.6 (Cycle Notation)

*A (nontrivial) **cycle** is an element S_n with exactly one nontrivial orbit. For distinct $a_1, \cdots, a_r$, the notation $(a_1 a_2 \cdots a_r)$ denotes the cycle in S_n with nontrivial orbit $\{a_1, \cdots, a_r\}$, acting as $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_r \mapsto a_1$. In this case, r is the length of the cycle, and the cycle is called an **r-cycle**.*

That is, $\sigma(a_r) = a_1$, $\sigma(a_i) = a_{i+1}$ for $i < r$, and $\sigma(a) = a$ for all $a \notin \{a_1, \cdots, a_r\}$. Note that $(a_1 a_2 \cdots a_r) = (a_2 \cdots a_r a_1)$, so the notation is determined up to a cyclic permutation.

Property *Disjoint cycles, i.e., cycles whose nontrivial orbits are disjoint, commute.*

Proposition 3.2

Every $\sigma \in S_n$, $\sigma \neq e$, can be written as a product of disjoint nontrivial cycles, in a unique way up to permutation of the factors.

Proof Every $\sigma \in S_n$ determines a partition into orbits under $\langle \sigma \rangle$, and $\langle \sigma \rangle$ has nontrivial orbits. As σ acts as cycles on each orbit, σ may be written as a product of cycles. The proof for uniqueness is omitted. ■

Definition 3.7 (Type)

*The **type** of $\sigma \in S_n$ is the partition of n given by the sizes of the orbits of the action of $\langle \sigma \rangle$ on $\{1, \cdots, n\}$.*

Example 3.1 Suppose $\sigma = (18632)(47) \in S_8$, then σ has type $[5, 2, 1]$.

Lemma 3.3

Let $\tau \in S_n$ and let $(a_1, \cdots, a_r)$ be a cycle. Then $\tau(a_1, \cdots, a_r)\tau^{-1} = (a_1\tau^{-1}, \cdots, a_r\tau^{-1})$, where $a_1\tau^{-1}$ denotes the right action of permutation τ^{-1} on a_1.

Proof For $1 \leq i < r$, $(a_i\tau^{-1})(\tau(a_1, \cdots, a_r)\tau^{-1}) = a_i(a_1, \cdots, a_r)\tau^{-1} = a_{i+1}\tau^{-1}$; and $(a_r\tau^{-1})(\tau(a_1, \cdots, a_r)\tau^{-1}) = a_1\tau^{-1}$ similarly. On the other hand, for $a' \notin \{a_i\tau^{-1}\}$, $a' = a\tau^{-1}$ for some $a \notin \{a_i\}$, so $a'(\tau(a_1, \cdots, a_r)\tau^{-1}) = a(a_1, \cdots, a_r)\tau^{-1} = a\tau^{-1} = a'$. ■

Remark This formula extends to the product of cycles, regardless whether they are disjoint or not, by inserting identity factors $\tau^{-1}\tau$. That is, $\tau(a_1 \cdots a_n)(b_1 \cdots b_m)\tau^{-1} = (a_1\tau^{-1} \cdots a_n\tau^{-1})(b_1\tau^{-1} \cdots b_m\tau^{-1})$.

Proposition 3.3

Two elements of S_n are conjugate in S_n if and only if they have the same type.

Proof The forward direction follows immediately from Lemma 3.3. Conversely, suppose σ and σ' have the same type, consider their cycle decomposition. For each cycle $(a_1 \cdots a_n)$ in σ, there is a corresponding cycle $(a'_1 \cdots a'_n)$ in σ'we define $\tau(a'_i) = a_i$. τ is well-defined and bijective because orbits form a partition. Then it is clear that $\tau\sigma\tau^{-1} = \sigma'$. ■

Corollary 3.2

The number of conjugacy classes in S_n equals the number of partitions of n. ♡

3.2.2 Transposition, Parity, Alternating Group

For $n \geq 1$, define the polynomial Δ_n by $\Delta_n = \prod_{1 \leq i \leq j \leq n}(x_i - x_j)$. We can acts with any σ on Δ_n, by permuting the indices according to σ:

$$\Delta_n\sigma = \prod_{1 \leq i \leq j \leq n} (x_{i\sigma} - x_{j\sigma}),$$

and $\Delta_n\sigma = \pm\Delta_n$.

Definition 3.8 (Transposition, Sign)

*A **transposition** is a cycle of length 2. The **sign** of a permutation $\sigma \in S_n$, denoted $(-1)^\sigma$, is determined by the action of σ on Δ_n: $\Delta_n\sigma = (-1)^\sigma\Delta_n$. We say σ is even if $(-1)^\sigma = +1$ and odd if $(-1)^\sigma = -1$.* ♣

Remark The sign function $\epsilon : S_n \to \{\pm 1\}$ defined by $\epsilon(\sigma) = (-1)^\sigma$ is a homomorphism since $\Delta_n(\sigma r) = (\Delta_n\sigma)r$ so that $(-1)^{\sigma r} = (-1)^\sigma(-1)^r$.

Lemma 3.4

Transpositions, namely cycles of length 2, generate S_n. ♡

Proof For all cycles $(a_1 \cdots a_n)$, $(a_1 \cdots a_n) = (a_1a_2)(a_1a_3)\cdots(a_1a_n)$, so the assertion follows immediately from Proposition 3.2. ■

Proposition 3.4

Let $\sigma = \tau_1 \cdots \tau_r$ be a product of transpositions. Then σ if even, resp., odd, according to whether r is even, resp., odd. ♠

Proof For each transposition τ, $\epsilon(\tau) = -1$. Suppose $\sigma = \tau_1 \cdots \tau_r$, the homomorphism implies that $(-1)^\sigma = \epsilon(\tau_1 \cdots \tau_r) = (-1)^r$. ■

Definition 3.9 (Alternating Groups)

*The **alternating group** on $\{1, \cdots, n\}$, denoted A_n, consists of all even permutation $\sigma \in S_n$.* ♣

Note *The alternating group A_n is a normal subgroup of S_n, and $[S_n : A_n] = 2$. Indeed, consider the sign function $\epsilon : S_n \to \{\pm 1\}$, the alternating group A_n is the kernel of ϵ.*

Note *The cycle is even, resp., odd, if it has odd, resp., even length. Then a permutation σ belongs to A_n if and only if n and the number of rows in the Young diagram have the same parity, namely n and $len(type(\sigma))$ have the same parity.*

3.2.3 Conjugacy, Simplicity, and Solvability

Denote by $[\sigma]_{S_n}$, resp., $[\sigma]_{A_n}$, the conjugacy class of an even permutation σ in S_n, resp., A_n.

Lemma 3.5

Let $n \geq 2$ and $\sigma \in A_n$. Then $[\sigma]_{A_n} = [\sigma]_{S_n}$ or the size of $[\sigma]_{A_n}$ is half the size of $[\sigma]_{S_n}$, according to whether the centralizer $Z_{S_n}(\sigma)$ is not or is contained in A_n.

Proof Suppose $Z_{S_n}(\sigma) \subset A_n$. Note that $Z_{S_n}(\sigma) = Z_{A_n}(\sigma)$, then $|[\sigma]_{S_n}| = [S_n : Z_{S_n}(\sigma)] = 2 \cdot [A_n : Z_{A_n}(\sigma)] = 2 \cdot |[\sigma]_{A_n}|$. Conversely, suppose $Z_{S_n}(\sigma) \cap (S_n \setminus A_n) \neq \varnothing$, let τ be such an element. Then for all $\varphi \notin A_n$, $\alpha\sigma\alpha^{-1} = (\varphi\tau)\sigma(\varphi\tau)^{-1} \in [\sigma]_{A_n}$, so $[\sigma]_{S_n} \subset [\sigma]_{A_n}$, it follows that $[\sigma]_{A_n} = [\sigma]_{S_n}$. ■

Remark Alternatively, by the second isomorphism theorem, $[Z_{S_n} : Z_{S_n} \cap A_n] = [A_n Z_{S_n} : A_n]$. Since $A_n Z_{S_n} \leq S_n$. Also note that $Z_{A_n} = Z_{S_n} \cap A_n$, then $[Z_{S_n} : Z_{A_n}] = [Z_{S_n} : Z_{S_n} \cap A_n]$ divides $[S_n : A_n] = 2$, so the index can only be 1 or 2. The index is one if and only if $Z_{S_n} \subset A_n$. Then the assertion follows from the orbit-stabilizer theorem, i.e., $|[\sigma]_{A_n}| = [A_n : Z_{A_n}]$ and $|[\sigma]_{S_n}| = [S_n : Z_{S_n}]$.

Conjugacy classes of even permutations either are preserved from S_n to A_n or they split into two distinct, equal-sized classes. The conjugacy class $[\sigma]_{S_n}$ splits into $[\sigma]_{A_n}$ and $[\sigma']_{A_n}$ if $\sigma' \notin [\sigma]_{A_n}$ and $\sigma' = \tau\sigma\tau^{-1}$ for some $\tau \notin A_n$.

Proposition 3.5

Let $\sigma \in A_n$, $n \geq 2$. Then the conjugacy class of σ in S_n splits into two conjugacy classes in A_n if and only if the type of σ consists of distinct odd numbers.

Proof It suffices to prove the type of σ contains distinct odd numbers if and only if $Z_{S_n}(\sigma) \subset A_n$, namely $\tau\sigma\tau^{-1} = \sigma$ implies that $\tau \in A_n$, by Lemma 3.5.

($\Rightarrow$) Suppose the type of σ contains distinct odd numbers and $\tau\sigma\tau^{-1} = \sigma$. Then every cycle $(a_1 \cdots a_m)$ in the cycle decomposition must preserved under σ. That is, σ must be a cyclic permutation on $(a_1 \cdots a_m)$, so σ contains $(a_1 \cdots a_m)^r$, which is clearly even given that m is odd. Thus, σ is even as a product of even permutations.

($\Leftarrow$) Conversely, suppose the type contains an even number, i.e., σ contains $(a_1 \cdots a_m)$ for some even m. Consider $\tau = (a_1 \cdots a_m)$ and identity elsewhere. Then $\tau\sigma\tau^{-1} = \sigma$ and τ is odd. On the other hand, suppose two cycles have the same odd length, i.e., $(a_1 \cdots a_m)$ and $(b_1 \cdots b_m)$. Consider τ defined by $\tau = (a_1 b_1)(a_2 b_2) \cdots (a_m b_m)$. Then $\tau\sigma\tau^{-1} = \sigma$ and τ is odd. ■

Corollary 3.3

*The alternating group A_5 is a **simple** (a group is simple if the only normal subgroups are trivial subgroup and itself) non-commutative group of order* 60.

♡

Proof The class formula for A_5 is $60 = 1 + 15 + 20 + 12 + 12$ (note that the conjugacy class splits for the type $[5]$). Consider subgroups of A_5, their order must be one of $2, 3, 4, 5, 6, 10, 12, 15, 20, 30$ by Lagrange theorem. Excluding the identity element, the subgroup has order of $1, 2, 3, 4, 5, 9, 11, 14, 19, 29$. We see that none can be written as the sum of orders of conjugacy classes, so they cannot be written as the union of conjugacy classes, so none of them are normal. It implies that A_5 is simple. ■

3.3 Sylow Theorems

3.3.1 Sylow Theorems

Theorem 3.1 (Cauchy's Theorem)

Let G be a finite group, and let p be a prime divisor of $|G|$. Then G contains an element of order p. ♡

Proof Proceed by induction on $|G|$. The case is trivial for $|G| = 1$. Suppose $|G| > 1$. Assume G is abelian, we let $H = \langle g \rangle$ for some $g \neq e_G$.

(1) If $p \,|\, |H|$, then $|g^{|H|/p}| = p$.

(2) If $p \nmid |H|$, then $p \,|\, |G/H|$ and G/H is a subgroup with order less than $|G|$. By inductive hypothesis, there exists $xH \in G/H$ such that $|xH| = p$. Note that $(xH)^{|x|} = H$, so $p \,|\, |x|$. Then $|x^{|x|/p}| = p$.

On the other hand, assume $|G|$ is not abelian, we therefore consider the class formula $|G| = |Z(G)| + \sum[G : G_a]$.

(1) If $p \,|\, |Z(G)|$, then the desired result follows immediately from the fact that $Z(G)$ is abelian.

(2) If $p \nmid |Z(G)|$, then $p \nmid [G : G_a]$ for some $a \in G$, so $p \,|\, |G_a|$. Note that $G_a \leq G$, so by inductive hypothesis, there exists $x \in G_a$ such that $|x| = p$.

Hence there exists $x \in G$ such that $|x| = p$. ■

Remark By the class formula, p divides the order of either (i) a stabilizer G_a or (ii) the center $Z(G)$. In the later case, we let $H := \langle g \rangle \trianglelefteq G$ for some $g \in Z(G)$. Since p divides $|H| \cdot |G/H| = |G|$, then p divides the order of (ii.1) H or (ii.2) G/H. In either cases, we may proceed by induction.

Proof Sketch of Alternative Proof: Let $H = \{(a_1, \cdots, a_p) \,|\, a_1 \cdots a_p = e\}$, then $|H| = |G|^{p-1}$ is is divisible by p^{p-1} because $a_1, \cdots a_{p-1}$ can be chosen arbitrarily. Consider $\mathbb{Z}/p\mathbb{Z}$ acts on H by left translation, it is well-defined because $a_k \cdots a_p a_1 \cdots a_{k-1} = e$ for all k. Note that $[H : H_x]$ is divisible by p since $|H_x|$ divides p, so then the class formula implies that $|Z(H)| \equiv |H| \equiv 0 \pmod{p}$, and Z is nonempty. Then Z is nontrivial, i.e., there exists $x \in G$ such that $(x, \cdots, x) \in Z$, and hence $|x| = p$. ■

Definition 3.10 (Simple Group)

*A group G is **simple** if its only normal subgroups are $\{e\}$ and G itself.* ♣

Definition 3.11 (p-Sylow group)

*Let p be a prime integer. A **p-Sylow subgroup** of a finite group G is a subgroup of order p^r where $|G| = p^r m$ and $\gcd(p, m) = 1$.* ♣

Theorem 3.2 (First Sylow Theorem)

Every finite group contains a p-Sylow subgroup, for all primes p. ♡

The first Sylow theorem follows from the stronger statement

Proposition 3.6

If p^k divides the order of G, then G has a subgroup of order p^k. ♠

Proof We may assume $p \,|\, |G|$ and $k \geq 1$. We proceed by induction on k. The $k = 1$ case follows immediately from Theorem 3.1. Suppose $k > 1$. Assume $p \,|\, Z(G)$, then there exists $x \in Z(G)$ such that $|x| = p$, so $N := \langle x \rangle$ is a normal subgroup that has order of p. Consider the quotient group G/N. Since $p^{k-1} \,|\, |G/N|$, the inductive hypothesis implies that there exists $H' \leq G/N$ such that $|H'| = p^{k-1}$. By the structure of subgroups of a quotient (Theorem 2.24), $H = H'/N$ for some $H \leq G$. Then $|H| = |H/N||N| = p^k$.

On the other hand, assume $p \nmid Z(G)$, the class formula implies that $p \nmid [G : G_a]$ for some $a \notin Z(G)$, so $p^k \,|\, |G_a|$. By inductive hypothesis, there exists a subgroup $H \leq G_a \leq G$ such that $|H| = p^k$. ■

Remark Suppose $|G| = p^r n$. If $p \,|\, Z(G)$, then $|G/N| = p^{r-1} n$ using quotient group by setting $N = \langle g \rangle$ for $p \mid |g|$. On the other hand, if $p \nmid Z(G)$, then $|G_a| = p^r m$ $(m < n)$ for some G_a, since $p \nmid [G : G_a]$ by class formula.

Theorem 3.3 (Second Sylow Theorem)

Let G be a finite group, let P be a p-Sylow subgroup, and let $H \subseteq G$ be a p-group. Then H is contained in a conjugate of P, i.e., there exists $g \in G$ such that $H \subseteq gPg^{-1}$. ♡

Proof Consider the left multiplication action by H on the left cosets G/P. Suppose $Z \subset G/P$ is the set of fixed points, then $|G/P| = |Z| + \sum [H : H_{gP}] \equiv |Z| \pmod{p}$ by Corollary 3.1. Since P is a p-Sylow subgroup, p does not divide $|G/P|$, so $|Z|$ is nonempty. Suppose $gP \in Z$, then $HgP = gP$, followed by $g^{-1}Hg \subset P$, hence $H \subset gPg^{-1}$. ■

Corollary 3.4 (Weaker Form of Theorem 3.3)

(a) All p-Sylow subgroups are conjugate of each other.

(b) Every maximal p-group in G is a p-Sylow subgroup. ♡

Remark The first Sylow theorem implies that some maximal p-group in G attains the largest size (i.e., p-Sylow subgroup), and the second Sylow theorem extends that every maximal p-group is a p-Sylow subgroup.

Proposition 3.7

Let H be a p-group contained in a finite group G. Then $[N_G(H) : H] \equiv [G : H] \pmod{p}$. ♠

Proof Consider the left multiplication action of H on G/H. Corollary 3.1 implies that $|G/H| = |Z| + \sum[H : H_{gH}] \equiv |Z| \pmod{p}$. Notice that $Z = \{gH \,|\, HgH = gH\} = \{gH \,|\, Hg = gH\} = N_G(H)/H$. Then $[G : H] \equiv |Z| = [N_G(H) : H] \pmod{p}$. ■

Proposition 3.8

Let H be a p-subgroup of a finite group G, and assume H is not a p-Sylow subgroup. Then there exists a p-subgroup H' of G containing H, such that $[H' : H] = p$ and H is normal in H'. ♠

Remark This proposition, combined with first and second Sylow theorem, implies that for every G such that $|G| = p^r m$ and every H, there exists a chain $\{e\} \subset H_1 \subset H_2 \cdots H_r$ containing H, and for which $|H_k| = p^k$ and $H_k \trianglelefteq H_{k+1}$ for all k.

Proof Since H is a p-subgroup which is not p-Sylow, p divides $[G : H]$ and thus divides $[N_G(H) : H]$ by above proposition, so there exists $gH \in N_G(H)/H$ such that $|gH| = p$ by Cauchy Theorem. The subgroup $\langle gH \rangle \leq N_G(H)/H$ is of order p, and $\langle gH \rangle = H'/H$ for some $H' \leq N_G(H)$ by the structure of quotient group. Then $[H' : H] = |\langle gH \rangle| = p$, and $H \trianglelefteq H'$ because $H' \subset N_G(H)$. ■

Theorem 3.4 (Third Sylow Theorem)

Let p be a prime integer, and let G be a finite group of order $|G| = p^r m$. Assume that p does not divide m. Then the number of p-Sylow subgroups of G divides m and is congruent to 1 modulo p. ♡

Proof Suppose K_p denotes the number of p-Sylow subgroups. According to second Sylow theorem (3.3), assume P is a p-Sylow subgroup, then Q is a p-Sylow subgroup if and only if it is conjugate to P, followed by K_p is precisely $[G : N_G(P)]$ by the orbit-stabilizer theorem.

It follows that $m = [G : P] = [G : N_G(P)][N_G(P) : P] = K_p[N_G(P) : P]$, so K_p divides m.

Indeed, $m = K_p[N_G(P) : P] \equiv K_p[G : P] = K_p m \pmod{p}$ by Proposition 3.7. Since $\gcd(m, p) = 1$, the cancellation law implies that $K_p \equiv 1 \pmod{p}$. ■

3.4 Products of Groups

3.4.1 Direct Product, Exact Sequence

Definition 3.12 (Commutator)

*The **commutator** $[A, B]$ of two subsets A, B of G is the subgroup generated by all commutators $[a, b] := aba^{-1}b^{-1}$.*

♣

Proposition 3.9

Let N, H be normal subgroups of a group G, then $[N, H] \subseteq N \cap H$.

♠

Proof It suffices to verify this on generators $[n, h]$: note that $[n, h] = (nhn^{-1})h^{-1} \in Hh^{-1} = H$ and $[n, h] = n(hn^{-1}h^{-1}) \in nN = N$, then $[n, h] \in N \cap H$. ■

Corollary 3.5

Let N, H be normal subgroups of a group G. If $N \cap H = \{e\}$, then N, H commute with each other: $nh = hn$ for every $n \in H$, $h \in H$.

♡

Proof It follows immediately from the above proposition that $[N, H] = \{e\}$, so $[n, h] = nhn^{-1}h^{-1} = e$, followed by $nh = hn$, for every $n \in H, h \in H$.

Proposition 3.10

Let N, H be normal subgroups of G, such that $N \cap H = \{e\}$, then $NH \cong N \times H$.

♠

Proof Consider $\varphi : N \times H \to NH$ defined by $\varphi(n, h) = nh$. It is a homomorphism because $\varphi((n_1, h_1)\cdot(n_2, h_2)) = \varphi(n_1n_2, h_1h_2) = n_1n_2h_1h_2 = n_1h_1n_2h_2 = \varphi(n_1, h_1)\varphi(n_2, h_2)$. φ is clearly surjective by the definition of NH; φ is injective since $\varphi(n, h) \in \ker\varphi$ if and only if $nh = e$, followed by $h = n^{-1} \in N \Rightarrow h \in N \cap H = \{e\} \Rightarrow h = e$, and $n = e$ without loss of generality. Hence φ is an isomorphism. ■

Definition 3.13 (Short Exact Sequence, Group Extension)

*A **(short) exact sequence** of groups is a sequence of groups and group homomorphisms*

$$1 \longrightarrow N \xrightarrow{\varphi} G \xrightarrow{\psi} H \longrightarrow 1$$

where φ is injective, ψ is surjective, and $\operatorname{im}\varphi = \ker\psi$. That is, the sequence is exact if $N \trianglelefteq G$ and ψ induces an isomorphism $G/N \to H$.

*Given an (short) exact sequence, we say that G is an **extension** of H by N.*

♣

Remark In the general case, a sequence $G_1 \xrightarrow{\varphi_1} G_2 \cdots \xrightarrow{\varphi_n} G_{n+1}$ is exact at G_i if $\mathrm{im}(\varphi_i) = \ker(\varphi_{i+1})$ by definition, and the sequence is an exact sequence if it is exact at every G_i.

In particular, consider the short sequence $1 \longrightarrow N \xrightarrow{\varphi} G \xrightarrow{\psi} H \longrightarrow 1$. Then the sequence is exact if and only if φ is injective, ψ is surjective, and $\mathrm{im}(\varphi) = \ker(\psi)$.

Hence every short exact sequence of groups is equivalent to a short exact sequence of the form $1 \longrightarrow \ker\varphi \hookrightarrow G \twoheadrightarrow G/\ker\varphi \longrightarrow 1$.

Example 3.2 For example, $1 \longrightarrow N \longrightarrow N \times H \longrightarrow H \longrightarrow 1$ is an exact sequence by defining $\varphi : n \to (n, e_H)$ and $\psi : (n, h) \to (e_N, h)$. However, G is not necessarily isomorphic to $N \times H$, for instance, $1 \longrightarrow C_3 \longrightarrow S_3 \longrightarrow C_2 \longrightarrow 1$ is an exact sequence, yet $S_3 \ncong C_3 \times C_2$. Indeed, in this case, there are two extensions of C_2 by C_3: $C_6 \cong C_3 \times C_2$ and S_3.

Definition 3.14 (Split Extension)

*An exact sequence of groups $1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1$ (or the corresponding extension) is said to **split** if H may be identified with a subgroup of G so that $N \cap H = \{e\}$.*

Lemma 3.6

Let N be a normal subgroup of a group G, and let H be a subgroup of G such that $G = HN$ and $N \cap H = \{e\}$. Then G is a split extension of H by N.

Proof By the second isomorphism theorem, $G/N = NH/N \cong H/(N \cap H) \cong H$, so G is an extension of H by N. Since H is a subgroup of G, the extension is a split extension. ■

3.4.2 Semdirect (Internal) Products

Suppose N is normal, then every subgroup H of G acts on N by conjugation, i.e., $\gamma : H \to \mathrm{Aut}_{\mathrm{GRP}}(N), h \mapsto \gamma_h$, where $\gamma_h(n) = hnh^{-1}$. The subgroup H and N commutes precisely when γ is trivial.

If the conditions in the above lemma are met, then the extension G of H by N may be reconstructed from the conjugation action: $n_1h_1n_2h_2 = (n_1(h_1n_2h_1^{-1}))(h_1h_2)$.

In the general discussion, suppose N, H are two groups, and θ is an arbitrary homomorphism $\theta : H \to \mathrm{Aut}_{\mathrm{GRP}}(N)$, $h \mapsto \theta_h$. Define the operation $\cdot_\theta$ on the set $N \times H$ as follows:

$$(n_1, h_1) \cdot_\theta (n_2, h_2) := (n_1, \theta(h_1, n_2), h_1h_2).$$

Note *The resulting structure $(N \times H, \cdot_\theta)$ is a group, with identity element (e_N, e_H).*

Definition 3.15 (Semidirect product)

*The group $(N \times H, \cdot_\theta)$ is a **semidirect product** of N and H and is denoted by $N \rtimes_\theta H$.*

Proposition 3.11

Let N, H be groups, and let $\theta : H \to Aut_{GRP}(N)$ be a homomorphism; let $G = N \rtimes_\theta H$ be the corresponding semidirect product. Then

(i) G contains isomorphic copies of N and H;

(ii) the natural projection $G \to H$ is a surjective homomorphism, with kernel N; thus N is normal in G, and the sequence $1 \longrightarrow N \longrightarrow N \rtimes_\theta H \longrightarrow H \longrightarrow 1$ is (split) exact.

(iii) $N \cap H = \{e_G\}$;

(iv) $G = NH$;

(v) the homomorphism θ is realized by conjugation in G; that is, for $h \in H$ and $n \in N$ we have $\theta_h(n) = hnh^{-1}$ in G.

Proof (i) Consider the inclusion function $i_N : N \to N \rtimes H$ defined by $i_N(n) = (n, e_H)$. i_N is obviously an injective homomorphism, so we may identifies N with $N \rtimes \{e\} \leq N \rtimes H$. The analogous statement holds for H.

(ii)-(iv) By identifying $N, H \leq G$, it is clear that $N \cap H = \{e_G\}$, and $G = NH$ since $(n, e_H) \cdot_\theta (e_N, h) = (n, h)$. Define the projection $\pi_H : G \to H$ by $(n, h) \mapsto h$. It is naturally a surjective homomorphism, and the kernel is given by $\ker \pi_H = N$. Therefore, $1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1$ is split exact.

(v) Note that $hnh^{-1} \leftrightarrow (e_N, h) \cdot_\theta (n, e_H) \cdot_\theta (e_N, h^{-1}) = (\theta_h(n)\theta_h(e_N), hh^{-1}) = (\theta_h(n), e_H) \leftrightarrow \theta_h(n)$, so θ is realized by conjugation. ■

Proposition 3.12

Let N, H be subgroups of a group G, with N normal in G. Assume that $N \cap H = \{e\}$, and $G = NH$. Let $\gamma : H \to Aut_{GRP}(N)$ be defined by conjugation: for $h \in H$, $n \in N$, $\gamma_h(n) = hnh^{-1}$. Then $G \cong N \rtimes_\gamma H$.

Proof Consider the function $\varphi : N \rtimes_\theta H \to G$ defined by $\varphi(n, h) = nh$. φ is clearly a bijection by definition, and it is a homomorphism since

$$\varphi((n_1, h_1)(n_2, h_2)) = \varphi(n_1\gamma_{h_1}(n_2), h_1h_2) = n_1(h_1n_2h_1^{-1})h_1h_2 = n_1h_1n_2h_2 = \varphi(n_1, h_1)\varphi(n_2, h_2).$$

Therefore, $N \rtimes_\gamma H \cong_\varphi G$. ■

Remark Proposition 3.11 implies that every (external) semi-direct product gives rise to a short exact sequence that splits, and Proposition 3.12 implies that a split extension can be realize through a (internal) semi-direct product.

3.5 Finite Abelian Groups

Note that we will denote the operation by "+", the identity by 0, and the direct product (direct sums) by $\oplus$.

Proposition 3.13

Let G be an abelian group, and let H, K be abelian subgroups such that $|H|$, $|K|$ are relatively prime. Then $H + K \cong H \oplus K$.

♠

Proof By Lagrange's theorem, $H \cap K = \{0\}$. The statement follows immediately from Proposition 3.10 since subgroups are normal in an abelian group. ■

Corollary 3.6

Every finite abelian group is the direct sum of its nontrivial Sylow subgroups.

♡

Proof Suppose $|G| = p_1^{r_1} \cdots p_n^{r_n}$. The Sylow theorems states that for each p_i, there is an unique p_i-Sylow subgroup H_i, i.e., $|H_i| = p_i^{r_i}$. The above proposition implies that $\bigoplus_{i=1}^n H_i \cong \sum_{i=1}^n H_i$. Since $|\bigoplus_{i=1}^n H_i| = |G|$ and $\bigoplus_{i=1}^n H_i \cong \sum_{i=1}^n H_i \subset G$, hence $G = H_1 \oplus \cdots \oplus H_n$. ■

Proposition 3.14

Let p be a prime integer and $r \geq 1$. Let G be a noncyclic abelian group of order p^{r+1}, and let $g \in G$ be an element of order p^r. Then there exists an element $h \in G$, $h \notin \langle g \rangle$ such that $|h| = p$.

♠

Proof Denote by $N = \langle g \rangle$. By Cauchy's theorem, there exists $hN = G/N$ such that $|hN| = p$, it is obvious that $h \notin N$ and $ph \in N$ so that $ph = m'g$. Notice that $|ph|$ divides pr and does not equal to pr because otherwise $G = \langle h \rangle$ is cyclic, thus we can write $ph = pmg$ for some m. Consider $h' = h - mg$, it is obvious that $h' \notin N$. Since $h - mg$ divides p since $p(h - mg) = 0$ and $|h - mg| \neq 1$, it follows that $|h'| = p$. ■

Proposition 3.15

Let G be an abelian p-group, and let $g \in G$ be an element of maximal order. Then the exact sequence $1 \longrightarrow \langle g \rangle \longrightarrow G \longrightarrow G/\langle g \rangle \longrightarrow 1$ splits.

♠

Remark In other words, there is a subgroup L of G such that $L \cong G/\langle g \rangle$ via canonical projection, that is, such that $\langle g \rangle \cap L = \{0\}$ and $\langle g \rangle + L = G$.

Proof We proceed by strong induction on $|G|$. The case $|G| = p^0 = 1$ is trivial. For nontrivial group G, assume the statement holds for every p-group smaller than G. Suppose $g \in G$ such that $|g| = p^r$ is the maximal order, consider $K = \langle g \rangle \trianglelefteq G$. The statement is obvious if $G = K$, so we therefore assume $G \neq K$. There is element in G/K of order p by Cauchy's theorem, it then generates G'/K for some $G' \leq G$ where $|G'| = p^{r+1}$. The previous proposition (3.14) implies that there exists $h \in G' \setminus K$ such that $|h| = p$. Let $H = \langle h \rangle$, then $G' = H \oplus K$ since $|hK| = p$.

Apply inductive hypothesis using the fact that $g + H$ has the maximal order in G/H, there is a split extension $0 \longrightarrow G'/H \longrightarrow G/H \longrightarrow L' \longrightarrow 0$ for some $L' \leq G/H$, and $L' = L/H$ for some $L \leq G$ by the structure of quotient group. In other words, $G'/H + L/H = G/H$ and $G'/H \cap L/H = \{H\}$. It is clear that $G'/H \cong K$. We want to prove $G = K \oplus L$ by verifying the following properties:

- Suppose $a \in G$, i.e., $a + H \in G/H$, then there exist $mg + H \in G'/H$ and $l + H \in L/H$ such that $a + H = mg + l + H$. Then $a \in mg + (l + H) \in K + L$. It follows that $G = K + L$.
- Suppose $a \in K \cap L$, then $a + H \in G'/H \cap L/H = \{H\}$, followed by $a \in H$. Then $a \in H \cap K$, forcing $a = 0$. That is, $K \cap L = \{0\}$.

Hence $G = K \oplus L$ as desired. ■

Corollary 3.7

Let G be a finite abelian group, Then G is a direct sum of cyclic groups, which may be assumed to be cyclic p-groups. ♡

Proof It suffices to prove every p-subgroup is a direct product of cyclic groups, then the desired statement follows immediately by Corollary 3.6. We proceed by induction on $|P|$. The case is trivial if P is trivial. Suppose P is a nontrivial p-group, let g be its element with maximal order. Proposition 3.15 implies that $P = \langle g \rangle + P'$ for some proper subgroup P'. P' is a direct sum of cyclic subgroups by inductive hypothesis, concluding the proof. ■

Theorem 3.5

Let G be a finite nontrivial abelian group. Then there exists prime integers $p_1, \cdots, p_r$ and positive integers $n_{i,j}$ such that $|G| = \prod_{i,j} p_i^{n_{i,j}}$ and

$$G \cong \bigoplus_{i,j} \mathbb{Z}/p^{n_{i,j}}\mathbb{Z}.$$

Equivalently, there exist positive integers $1 < d_1 \mid \cdots \mid d_s$ such that $|G| = d_1 \cdots d_s$ and

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \mathbb{Z}/d_s\mathbb{Z}.$$

Furthermore, these decompositions are uniquely determined by G. ♡

Remark The first form follows immediately from the above corollary. For the second form, the integers d_i are called ***invariant factors***. To obtain the invariant factors, collect the element divisors in a table, listing prime powers to increasing primes in the horizontal direction and decreasing exponents in the vertical direction, then the invariant factors are obtained as products of the factors in each row:

$d_r =$	$p_1^{n_{1,1}}$	$p_2^{n_{2,1}}$	$\cdots$
$d_{r-1} =$	$p_1^{n_{1,1}}$	$p_2^{n_{2,1}}$	$\cdots$
$d_{r-2} =$	$p_1^{n_{1,1}}$	$p_2^{n_{2,1}}$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\ddots$

Example 3.3 All abelian groups of order $360 = 2^3 \times 3^2 \times 5$ are

$$\mathbb{Z}/360\mathbb{Z}, \qquad \mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/180\mathbb{Z}, \qquad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z},$$
$$\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/6\mathbb{Z} \otimes \mathbb{Z}/30\mathbb{Z}, \qquad \mathbb{Z}/3\mathbb{Z} \otimes \mathbb{Z}/120\mathbb{Z}, \qquad \mathbb{Z}/6\mathbb{Z} \otimes \mathbb{Z}/60\mathbb{Z},$$

up to isomorphisms.