

# Algebraic Structure Notes

Instructor: Anton Bernshteyn  
Notes by: Lichen Zhang  
Carnegie Mellon University  
21-373 Algebraic Structure

March 14, 2020

## Contents

<b>1</b>	<b>Sets, Functions and Equivalence Relations</b>	<b>3</b>
1.1	Basic definitions . . . . .	3
1.2	Higher-order functions . . . . .	5
1.3	Equivalence relations & quotients . . . . .	6
<b>2</b>	<b>Functors</b>	<b>8</b>
2.1	Covariant functors . . . . .	8
2.2	Universal elements . . . . .	10
2.3	Contravariant functors . . . . .	12
<b>3</b>	<b>Groups</b>	<b>13</b>
3.1	Concrete groups . . . . .	13
3.2	Abstract groups . . . . .	17
3.3	Abelian groups, subgroups, homomorphisms . . . . .	21
3.4	Actions, cosets, orbits . . . . .	23
3.5	Orbit-stabilizer theorem . . . . .	28
3.6	Normal subgroups and kernels . . . . .	32
3.7	Groups and counting . . . . .	34
<b>4</b>	<b>Category</b>	<b>36</b>
4.1	Basic definitions & examples . . . . .	36
4.2	Monomorphism, epimorphism . . . . .	38
<b>5</b>	<b>Advanced topics on Groups</b>	<b>41</b>
5.1	Product & coproduct of groups . . . . .	41
5.2	Free groups . . . . .	43
5.3	Structure of finite groups . . . . .	51

<b>6</b>	<b>Rings and Modules</b>	<b>55</b>
6.1	Basic definitions . . . . .	55
6.2	Free modules, independent, spanning, and basis . . . . .	57
6.3	Commutative rings and IBN . . . . .	60
6.4	Polynomials . . . . .	66

# 1 Sets, Functions and Equivalence Relations

## 1.1 Basic definitions

We start this notes by reminding readers some basic definitions of sets, functions and equivalence relations, which, though fundamental, are critical in the study of various algebraic structures. Given two sets  $A, B$ , except for the standard notation  $A \cup B, A \cap B, A \setminus B, A \subseteq B, A \subset B$ , we introduce *symmetric difference* of two sets.

**Definition 1.1.** The *symmetric difference* of two sets  $A, B$ , denoted by  $A \triangle B$ , is defined as  $(A \setminus B) \cup (B \setminus A)$ .

**Definition 1.2.** The set of all functions  $f : A \rightarrow B$  is denoted as  $B^A$ .

**Exercise 1.3.** If both  $A, B$  are finite, show that  $|B^A| = |B|^{|A|}$ .

*Proof.* To count all functions from  $A$  to  $B$ , it is useful to think of it in a *bucket-item* manner: each element of  $A$  can be viewed as a *bucket*, while each element of  $B$  is *item*, count the number of functions is just counting the number of ways to put items into buckets. For each bucket, there are  $|B|$  items we can put into, moreover, these items can be put into as many buckets as we want, so there are  $\underbrace{|B||B| \dots |B|}_{|A| \text{ times}} = |B|^{|A|}$  functions in total.  $\square$

**Definition 1.4.** Let  $f : A \rightarrow B$  be a function.

- $f$  is *injective*, if for  $a_1, a_2 \in A, a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$ .
- $f$  is *surjective*, if for any  $b \in B, b \in \text{im}(f)$ , or equivalently,  $B = \text{im}(f)$ .
- $f$  is *bijective* if it is both injective and surjective.

**Definition 1.5.** Two functions  $f, g$  are *equal*, if  $\text{dom}(f) = \text{dom}(g)$ , and for any  $x \in \text{dom}(f), f(x) = g(x)$ .

**Example 1.6.** 1. Let  $A$  be a set,  $\{0\}$  be a 1-element set, what is  $A^{\{0\}}$ ? It's the set of all functions from  $\{0\}$ . It is clear that there is a bijection between  $A^{\{0\}}$  and  $A$  by  $f \mapsto f(0)$ . In such scenario, we say  $A$  is *isomorphic* to  $A^{\{0\}}$ .

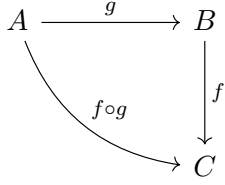
**Definition 1.7.** Given two sets  $A, B$ , we say  $A$  is *isomorphic* to  $B$ , denoted by  $A \cong B$ , if there exists a bijection from  $A$  to  $B$ .

2.  $A^{\{0,1\}} \cong A \times A$ , the bijection is given by  $f \mapsto (f(0), f(1))$ .
3. What is  $A^\emptyset, \emptyset^A$ ? They are different as long as  $A \neq \emptyset$ .
4.  $\{0,1\}^A \cong \mathcal{P}(A)$ , the bijection is  $f \mapsto \{a \in A : f(a) = 1\}$ .

**Definition 1.8.** Given three sets  $A, B, C$ , two functions  $f : B \rightarrow C, g : A \rightarrow B$ , define *composition* of functions  $f, g$ , denoted by  $f \circ g$ , as follows:

- $\text{dom}(f \circ g) = \{x \in \text{dom}(g) : g(x) \in \text{dom}(f)\}$ .

- For  $x \in \text{dom}(f \circ g)$ , define  $(f \circ g)(x) = f(g(x))$ .



**Exercise 1.9** (Important). Verify function composition is associative, i.e., given  $f, g, h$  three functions with well-behaved domains & codomains, verify  $f \circ (g \circ h) = (f \circ g) \circ h$ .

**Example 1.10.** Applying a function to an element can be “encoded” as a composition operation: let  $f : A \rightarrow B$  be our function, consider  $f(a)$ , we can replace  $a$  by function  $g : \{0\} \rightarrow A$  by  $0 \mapsto a$ , then  $f \circ g : \{0\} \rightarrow B : 0 \mapsto f(a)$ .

**Definition 1.11.** Given a set  $A$ , the *identity functions* on  $A$ , denoted by  $\text{id}_A : A \rightarrow A$ , is the function  $a \mapsto a$ .

**Exercise 1.12.** Let  $f : A \rightarrow B$ , then  $f \circ \text{id}_A = \text{id}_B \circ f = f$ .

**Definition 1.13.** Let  $f : A \rightarrow B, g : B \rightarrow A$ , if  $f \circ g = \text{id}_B$ , then  $f$  is a *left inverse* of  $g$  and  $g$  is a *right inverse* of  $f$ . If  $f$  is both left and right inverse of  $g$ , then  $f$  is a *two-sided inverse* of  $g$ .

**Exercise 1.14.** Give an example such that  $f$  is a left inverse, but not a right inverse of  $g$ .

**Exercise 1.15.** Let  $A \neq \emptyset, B$  be two sets and  $f : A \rightarrow B, g : B \rightarrow A$ . Prove the following:

1.  $f$  has a left inverse  $g$  if and only if  $f$  is injective.
2.  $f$  has a right inverse  $g$  if and only if  $f$  is surjective.

The proof is not hard, for the first part, one simply choose  $g$  to send everything to its preimage under  $f$ . For the second part,  $g$  can simply send element to one of its preimage under  $f$ .

**Definition 1.16.** Given  $f : A \rightarrow B$ , the followings are equivalent:

1.  $f$  is bijective.
2.  $f$  has a right and left inverse.
3.  $f$  has a two-sided inverse.

In this case, we denote (two-sided) inverse of  $f$  as  $f^{-1}$ . Also,  $f^{-1}$  is a bijection from  $B$  to  $A$  and  $(f^{-1})^{-1} = f$ .

**Exercise 1.17.** Suppose  $f : A \rightarrow B, g : B \rightarrow A$  are both bijective, then  $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ .

## 1.2 Higher-order functions

In this section, we study *higher-order functions*, which take functions as inputs and spits out functions. This idea has been heavily exploited in functional programming and the study of programming language. We motivate with an example.

**Example 1.18.** Let  $X, Y, A$  be sets, then we claim  $A^{X \times Y} \cong (A^X)^Y$ .

Given  $f \in A^{X \times Y}$ , i.e.,  $f : X \times Y \rightarrow A$ , we associate  $f$  to the function  $F : Y \rightarrow A^X$  as follows: for any  $y \in Y, x \in X$ ,  $(F(y))(x) := f(x, y)$ . This is called *function currying*.

The inverse of this operation is as follows: to each  $F \in (A^X)^Y$ , assign  $f : X \times Y \rightarrow A$  by  $f(x, y) := (F(y))(x)$ .

**Definition 1.19.** Let  $X, Y, A$  be sets, to each function  $f : X \rightarrow Y$ , corresponds a function  $f^A : X^A \rightarrow Y^A$ , given by  $f^A(g) := f \circ g$ .

$$\begin{array}{ccc} A & \xrightarrow{g} & X \\ & \searrow f^A(g) & \downarrow f \\ & = f \circ g & Y \end{array}$$

**Proposition 1.20.** Let  $X, Y, Z$  be sets and  $f : X \rightarrow Y, g : Y \rightarrow Z$ , then  $(g \circ f)^A = g^A \circ f^A$ .

*Proof.* First, let's compare the domains.

- $g \circ f : X \rightarrow Z$ , so  $(g \circ f)^A : X^A \rightarrow Z^A$
- $g^A : Y^A \rightarrow Z^A, f^A : X^A \rightarrow Y^A$ , so  $g^A \circ f^A : X^A \rightarrow Z^A$

Take and  $h \in X^A$ , let's do some computations.

- $(g \circ f)^A(h) = (g \circ f) \circ h$
- $g^A \circ f^A(h) = g^A(f \circ h) = g \circ (f \circ h)$

By 1.9, we know that function composition is associative, therefore, they are equal.  $\square$

**Definition 1.21.** Let  $X, Y, A$  be sets, to each function  $f : X \rightarrow Y$ , corresponds a function  $A^f : A^Y \rightarrow A^X$  by  $(A^f)(g) = g \circ f$ .

$$\begin{array}{ccc} X & \xrightarrow{A^f(g)} & Y \\ & \searrow f & \downarrow g \\ & & A \end{array}$$

**Exercise 1.22.** Let  $X, Y, Z$  be sets and  $f : X \rightarrow Y, g : Y \rightarrow Z$ , then  $A^{g \circ f} = A^f \circ A^g$ .

### 1.3 Equivalence relations & quotients

**Definition 1.23.** A (binary) relation on a set  $X$  is a subset  $R \subseteq X \times X$ , usually, we write  $xRy$  instead of  $(x, y) \in R$ .

**Definition 1.24.** An equivalence relation  $E$  on set  $X$  is a relation such that

1.  $E$  is reflexive.
2.  $E$  is symmetric.
3.  $E$  is transitive.

**Example 1.25.** Consider the following relation on  $\mathbb{Z}$ :

- $xEy \Leftrightarrow x - y \in \mathbb{Z}$ , this is an equivalence relation.
- $xEy \Leftrightarrow x + y \in \mathbb{Z}$ , this is not an equivalence relation, transitivity does not hold.

**Definition 1.26.** Given function  $f : X \rightarrow Y$ , the equivalence kernel of  $f$  is the relation  $E_f$  on  $X$ , given by  $xE_fy \Leftrightarrow f(x) = f(y)$ , this  $E_f$  is an equivalence relation.

Conversely, given an equivalence relation  $E$  on  $X$ , for  $x \in X$ , let  $[x]_E := \{y \in X : xEy\}$ , defined as the equivalence class of  $x$ .

Let  $X/E := \{[x]_E : x \in X\}$  be the quotient of  $X$  by  $E$ , the map  $p_E : X \rightarrow X/E : x \mapsto [x]_E$  is called the quotient map.

**Proposition 1.27.** Let  $E$  be an equivalence relation on  $X$ , then  $p_E : X \rightarrow X/E$  is a surjection, with equivalence kernel  $E$ .

*Proof.* The first part is clear, any equivalence class  $[x]_E$  has at least one canonical representation, namely  $x$  in it, this is given by  $E$  is reflexive. To see the second part, consider the following chain of equivalence:  $xEy \Leftrightarrow [x]_E = [y]_E \Leftrightarrow p_E(x) = p_E(y)$ .  $\square$

**Definition 1.28.** Let  $E$  be an equivalence relation on set  $X$ , a function  $f : X \rightarrow Y$  is  $E$ -invariant if  $xEy \Rightarrow f(x) = f(y)$ , i.e.,  $f$  is constant on equivalence classes.

**Theorem 1.29.** Let  $E$  be an equivalence relation on  $X$ , if  $f : X \rightarrow Y$  is  $E$ -invariant, then there is a unique function  $g : X/E \rightarrow Y$  such that  $f = g \circ p_E$ .

*Proof.* The theorem is equivalent to the following diagram:

$$\begin{array}{ccc} X & \xrightarrow{p_E} & X/E \\ & \searrow f & \downarrow \exists! g \\ & & Y \end{array}$$

Define function  $g$  as follows: for each  $C \in X/E$ , let  $g(C) := f(x)$ , for any  $x \in C$ . Since  $f$  is  $E$ -invariant, this does not depend on the choice of  $x \in C$ , so  $g$  is well-defined.

Moreover,  $(g \circ p_E)(x) = g(p_E(x)) = g([x]_E) = f(x)$ , this proves the existence of such an  $g$ .

To see uniqueness, if  $f = g \circ p_E$ , then for any  $x$ ,  $(g \circ p_E)(x) = g([x]_E) = f(x)$ , therefore, it's unique.  $\square$

**Exercise 1.30.** Based on the construction of  $g$  above, prove the following:

1.  $g$  is injective if and only if the equivalence kernel of  $f$  is  $E$ .
2.  $g$  is surjective if and only if  $f$  is surjective.
3. If  $E_f = E$  and  $\text{im}(f) = Y$ , then  $g$  is a bijection.

**Corollary 1.31** (Canonical decomposition theorem). *Let  $f : X \rightarrow Y$ , then  $f$  can be decomposed*

as follows:

$$\begin{array}{ccccc}
 X & \xrightarrow{p} & X/E_f & \xhookrightarrow{b} & \text{im}(f) \\
 & \searrow f & & \nearrow i & \\
 & & Y & & 
 \end{array}$$

where:

- $p$  is the quotient map  $p_E$ , which is surjective.
- $i$  is the inclusion map, which is injective.
- $b$  is a bijective map, which is  $g$  from 1.29.

## 2 Functors

In this section, we study the first algebraic structure in this course, which operates on sets and functions.

### 2.1 Covariant functors

**Definition 2.1.** A *functor* (on sets to sets) is a rule  $\mathcal{F}$  that assigns each set  $S$  a set  $\mathcal{F}(S)$  and to each function  $f : S \rightarrow T$  a function  $\mathcal{F}(f) : \mathcal{F}(S) \rightarrow \mathcal{F}(T)$  such that

1. For each set  $S$ ,  $\mathcal{F}(\text{id}_S) := \text{id}_{\mathcal{F}(S)}$ .
2. For any  $f : S \rightarrow T$ ,  $g : R \rightarrow S$ , we have  $\mathcal{F}(f \circ g) = \mathcal{F}(f) \circ \mathcal{F}(g)$ .

One can think of a functor  $\mathcal{F}$  consists of

- an “object map”:  $\mathcal{F}_O : \text{sets} \rightarrow \text{sets}$ .
- a “mapping map”:  $\mathcal{F}_M : \text{functions} \rightarrow \text{functions}$ .

Let’s look at some examples of functors to form a better sense of the definition.

**Example 2.2.** 1. The identity functor, given by  $\text{Id}(S) = S, \text{Id}(f) = f$ .  
 2. Fix a set  $A$ , let  $\mathcal{F}(S) := A$ , for any set  $S$ , and let  $\mathcal{F}(f) := \text{id}_A$ , for any  $f$ .

**Exercise 2.3.** Are there any other functors with  $\mathcal{F}(S)$ , for any set  $S$ ?

3. The powerset functor, given by  $\mathcal{F}(S) = \mathcal{P}(S)$ , and for function  $f : S \rightarrow T$ , we need to have  $\mathcal{F}(f) : \mathcal{P}(S) \rightarrow \mathcal{P}(T)$ . For any subset  $A \subseteq S$ , let  $(\mathcal{F}(f))(A) := \{f(a) : a \in A\}$ , i.e., the image of  $A$  under  $f$ , or  $f(A)$ . Let’s verify it’s a functor.

*Proof.* Notice  $\mathcal{F}(\text{id}_S)(A) = \text{id}_S(A) = A$ , and  $\text{id}_{\mathcal{F}(S)}(A) = A$ , so they are equal. For composition, we use  $f_*$  as a shorthand notation for  $\mathcal{F}(f)$ , then

- $(f \circ g)_*(A) = \{(f \circ g)(a) : a \in A\} = (f \circ g)(A) = f(g(A))$
- $f_* \circ g_*(A) = f_*(g_*(A)) = f_*(g(A)) = f(g(A))$

Again, the composition is preserved. □

4. Fix a set  $A$ , define the functor to raise sets and functions to the power of  $A$ :  $S \mapsto S^A, f \mapsto f^A$ . This defines a functor, since in 1.20, we have shown that  $(f \circ g)^A = f^A \circ g^A$ . Identity is easy to verify.
5. For each set  $S$ , let  $[S]^{<\infty}$  be the set of all *finite* subsets of  $S$ , define a functor as follows: for each set  $S$ ,  $\mathcal{F}(S) := [S]^{<\infty}$ , and for each function  $f : S \rightarrow T$ ,  $\mathcal{F}(f) : \mathcal{F}(S) \rightarrow \mathcal{F}(T)$ , given by  $(\mathcal{F}(f))(A) := \{f(a) : a \in A\}$ . Since input subset  $A$  is finite, output is also finite, so this functor is well-defined.

**Definition 2.4.** A functor  $\mathcal{G}$  is called a *subfunctor* of  $\mathcal{F}$  if for any set  $S$ ,  $\mathcal{G}(S) \subseteq \mathcal{F}(S)$ , and for any  $f : S \rightarrow T$ ,  $\mathcal{G}(f) = (\mathcal{F}(f))|_{\mathcal{G}(S)}$ .



A quick observation: suppose  $\mathcal{F}$  is a functor and let  $\mathcal{G}_0$  be a mapping that assigns each set  $S$  a subset  $\mathcal{G}_0(S) \subseteq \mathcal{F}(S)$ , then there is a unique subfunctor  $\mathcal{G}$  of  $\mathcal{F}$  whose object map is  $\mathcal{G}_0$  if and only if  $\text{im}(\mathcal{F}(f)|_{\mathcal{G}_0(S)}) \subseteq \mathcal{G}_0(T)$ , for any  $f : S \rightarrow T$ .

**Example 2.5.** Fix a set  $A$ , let  $\mathcal{F}$  be the functor given by  $\mathcal{F}(S) := S^A$ , and for each  $f : S \rightarrow T$ , define  $\mathcal{F}(f) := f^A$ . Let  $E$  be an equivalence relation on  $A$ , let  $\mathcal{G}_0(S) := \{E\text{-invariant functions } f : A \rightarrow S\}$ . This gives rise to a subfunctor of  $\mathcal{F}$ : first, it's clear that for any set  $S$ , we have  $\mathcal{G}_0(S) \subseteq S^A$ , our goal is to show that  $f^A|_{\mathcal{G}_0(S)} : \mathcal{G}_0(S) \rightarrow \mathcal{G}_0(T)$  is well-defined and well-behaved, i.e.,  $f^A|_{\mathcal{G}_0(S)}(g) = f \circ g$ , is this function  $E$ -invariant? Notice that by definition,  $g$  is  $E$ -invariant, so if  $a_1 E a_2 \Rightarrow g(a_1) = g(a_2) \Rightarrow f(g(a_1)) = f(g(a_2))$ .

## 2.2 Universal elements

**Definition 2.6.** A *universal element* for a functor  $\mathcal{F}$  is a pair  $(R, u)$ , where  $R$  is a set,  $u \in \mathcal{F}(R)$  such that for any set  $S$  and each  $s \in \mathcal{F}(S)$ , there exists a unique function  $h : R \rightarrow S$ , satisfying  $(\mathcal{F}(h))(u) = s$ .

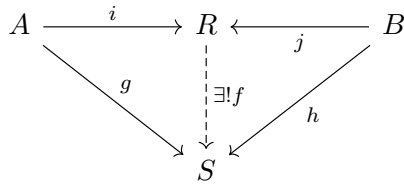
**Example 2.7.** Fix a set  $A$  and an equivalence relation  $E$ , we have a functor  $\mathcal{F}$  that maps  $S$  to  $\mathcal{F}(S) = \{E\text{-invariant functions } g : A \rightarrow S\}$ , and each  $f : S \rightarrow T$  to  $\mathcal{F}(f)$  by  $g \mapsto f \circ g$ .

What is the universal element of this functor? We need a set  $R$ , and  $u \in \mathcal{F}(R)$ , where  $u$  is an  $E$ -invariant function from  $A$  to  $R$ , our goal is to satisfy the *universal property*, i.e., for all set  $S$  and  $s : A \rightarrow S$  which is  $E$ -invariant, there is a unique function  $h : R \rightarrow S$  such that  $\mathcal{F}(h)(u) = h \circ u = s$ . Let's set  $R = A/E$ , and  $u = p_E$ , set  $h([x]_E) = s(x)$ , given such  $u$ ,  $h$  must be unique, so  $(A/E, p_E)$  is a universal element of functor  $\mathcal{F}$ .

**Example 2.8.** Fix sets  $A, B$ , define  $\mathcal{F}(S) = S^A \times S^B$ , given  $f : S \rightarrow T$ , define  $\mathcal{F}(f)$  by  $(g, h) = (f \circ g, f \circ h)$ .

**Exercise 2.9.** Prove it's a functor.

What is the universal element? It's called *disjoint union* of  $A$  and  $B$ . Let  $R$  be our target set,  $u \in \mathcal{F}(R) = R^A \times R^B = (i, j)$ , for set  $S$  and  $s \in \mathcal{F}(s) = (g, h)$ , there is a unique function  $f : R \rightarrow S$  such that  $\mathcal{F}(f)(i, j) = (g, h) = (f \circ i, f \circ j)$ .



If  $A \cap B = \emptyset$ , then we can simply set  $R = A \cup B$  and  $i, j$  be inclusion maps. Set

$$f(x) = \begin{cases} g(x), & \text{if } x \in A \\ h(x), & \text{if } x \in B \end{cases}$$

On the other hand, if  $A \cap B \neq \emptyset$ , then let  $A', B'$  be  $A' := A \times \{0\}$ ,  $B' = B \times \{1\}$ , and  $i, j$  maps element with an extra bit. By this bit,  $f$  has the ability to decode the input. Set

$$f(x) = \begin{cases} g(i^{-1}(x)), & \text{if } x \in A' \\ h(j^{-1}(x)), & \text{if } x \in B' \end{cases}$$

This construction is referred as the *disjoint union* of  $A$  and  $B$ .

**Proposition 2.10.** Let  $(R, u)$  be a universal element of  $\mathcal{F}$ , suppose  $b : R \rightarrow R'$  is a bijection, then  $(R', u')$  is also a universal element, where  $u' = \mathcal{F}(b)(u)$ .

*Proof.* Take any set  $S$  and  $s \in \mathcal{F}(S)$ , we need to show that there exists a unique  $h' : R' \rightarrow S$  such that  $\mathcal{F}(h')(u') = s$ . We separately show the existence and uniqueness.

**Existence:** since  $(R, u)$  is universal, there exists a unique  $h : R \rightarrow S$  with  $\mathcal{F}(h)(u) = s$ . Define

$h' = h \circ b^{-1}$ , then

$$\begin{aligned}
\mathcal{F}(h')(u') &= \mathcal{F}(h')(\mathcal{F}(b)(u)) \\
&= \mathcal{F}(h') \circ \mathcal{F}(b)(u) \\
&= \mathcal{F}(h' \circ b)(u) \\
&= \mathcal{F}(h \circ b^{-1} \circ b)(u) \\
&= \mathcal{F}(h)(u) \\
&= s
\end{aligned}$$

**Uniqueness:** Notice that we must have  $\mathcal{F}(h' \circ b)(u) = \mathcal{F}(h)(u)$ , by uniqueness of  $h$ , we must have  $h' \circ b = h$ , the only choice for  $h'$  is  $h \circ b^{-1}$ .  $\square$

Next theorem is the converse of above proposition.

**Theorem 2.11** (Uniqueness of universal element). *Let  $\mathcal{F}$  be a functor, if  $(R, u), (R', u')$  are universal for  $\mathcal{F}$ , then there exists a unique  $b : R \rightarrow R'$  such that  $u' = \mathcal{F}(b)(u)$ .*

*Proof.* Since  $(R, u)$  is universal, there exists a unique  $b : R \rightarrow R'$  such that  $\mathcal{F}(b)(u) = u'$ . Similarly,  $(R', u')$  is universal, so there exists a unique  $b' : R' \rightarrow R$  such that  $\mathcal{F}(b')(u') = u$ . It suffices to show  $b$  is a bijection, and  $b'$  is its inverse, i.e.,  $b \circ b' = \text{id}_{R'}$ ,  $b' \circ b = \text{id}_R$ .

$$\begin{aligned}
\mathcal{F}(b' \circ b)(u) &= \mathcal{F}(b') \circ \mathcal{F}(b)(u) \\
&= \mathcal{F}(b')(u') \\
&= u
\end{aligned}$$

Apply universal property on  $u$  itself, there exists a unique  $h : R \rightarrow R$  such that  $\mathcal{F}(h)(u) = u$ . First observe that  $\text{id}_{\mathcal{F}(R)}(u) = u$ , and  $\mathcal{F}(\text{id}_R) = \text{id}_{\mathcal{F}(R)}$ ,  $h$  must be  $\text{id}_R$ . On the other hand,  $\mathcal{F}(b \circ b')(u) = u$ , which implies  $b \circ b' = h = \text{id}_R$ . The other identity is similar.  $\square$

### 2.3 Contravariant functors

**Definition 2.12.** A *contravariant functor*  $\mathbb{C}$  assigns to each set  $S$  a  $\mathbb{C}(S)$  and to each  $f : S \rightarrow T$  a function  $\mathbb{C}(f) : \mathbb{C}(T) \rightarrow \mathbb{C}(S)$  such that

- $\mathbb{C}(\text{id}_S) = \text{id}_{\mathbb{C}(S)}$
- If  $f : S \rightarrow T, g : R \rightarrow S$ , then  $\mathbb{C}(f \circ g) = \mathbb{C}(g) \circ \mathbb{C}(f)$

**Example 2.13** (Contravariant powerset functor). Define  $\mathbb{C}$  as follows:  $S \mapsto \mathcal{P}(S)$ ,  $f \mapsto f_*$  by  $f_* : \mathcal{P}(T) \rightarrow \mathcal{P}(S)$ , for each set  $B \subseteq T$ ,  $f_*(B) = \{a \in S : f(a) \in B\}$ , i.e., the *preimage* of  $B$  under  $f$ .

**Exercise 2.14.** Check it's a contravariant functor.

**Example 2.15.** Fix a set  $A$ , the following is contravariant:  $S \mapsto A^S$ ,  $f \mapsto A^f$ , i.e.,  $f : S \rightarrow T$ ,  $A^f : A^T \rightarrow A^S$ , and  $A^f(g) = g \circ f$ .

**Definition 2.16.** Let  $\mathbb{C}$  be a contravariant functor, a *universal element* for  $\mathbb{C}$  is a pair  $(R, u)$ , where  $R$  is a set and  $u \in \mathbb{C}(R)$ , such that for any  $S$  and  $s \in \mathbb{C}(S)$ , there exists a unique  $h : S \rightarrow R$  such that  $\mathbb{C}(h)(u) = s$ .

Universal element for contravariant functors is very similar to universal element for covariant functors, except for the function  $h$ , now its domain is  $S$  and codomain is  $R$ .

**Example 2.17.** Fix sets  $A, B$ , define a contravariant functor  $\mathbb{C}$  as follows:  $\mathbb{C}(S) := A^S \times B^S$ , for  $f : S \rightarrow T$ , define  $\mathbb{C}(f) : \mathbb{C}(T) \rightarrow \mathbb{C}(S)$  by  $\mathbb{C}(f)(g, h) := (g \circ f, h \circ f)$ .

What is the universal element? We want  $(R, u)$ ,  $u \in \mathbb{C}(R)$ , so  $u = (p, q) \in A^R \times B^R$ , for any  $S$  and  $s = (g, h) \in \mathbb{C}(S)$ , there exists a unique  $f : S \rightarrow R$  such that  $s = \mathbb{C}(f)(p, q) = (p \circ f, q \circ f) = (g, h)$ . Set  $R = A \times B$ ,  $p(a, b) = a$ ,  $q(a, b) = b$ , and  $f(x) = (g(x), h(x))$ . It's not hard to check this is a universal element.

Similar to covariant functor, contravariant functor also has a uniqueness theorem for universal element.

**Theorem 2.18.** If  $(R, u), (R', u')$  are universal elements for contravariant functor  $\mathbb{C}$ , then there exists a unique bijection  $b' : R' \rightarrow R$  such that  $u' = \mathbb{C}(b')(u)$ .

### 3 Groups

In this section, we study group, one of the most famous algebraic structures, with a simple definition but surprisingly complicated dynamics.

#### 3.1 Concrete groups

**Definition 3.1.** A *concrete group* on a set  $X$  is a set  $G$  of bijections  $X \rightarrow X$ , such that

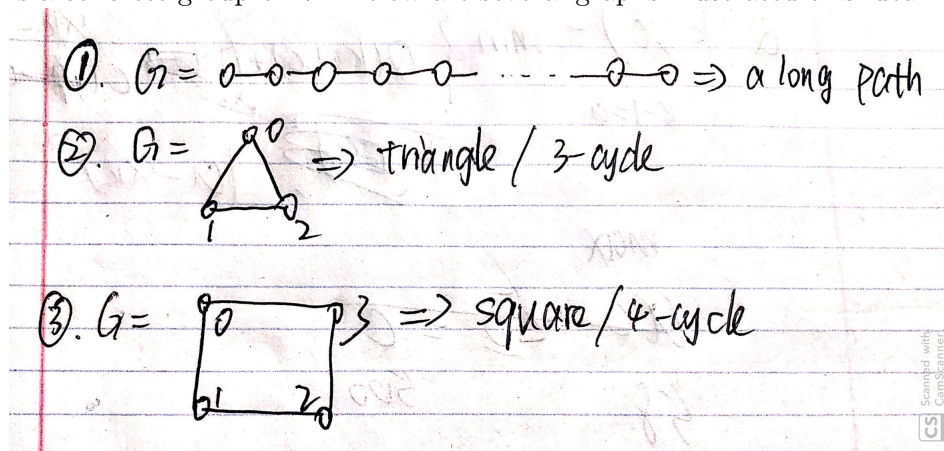
1.  $\text{id}_X \in G$
2. if  $f \in G$ , then  $f^{-1} \in G$
3. if  $f, g \in G$ , then  $f \circ g \in G$

**Example 3.2.** 1. The set  $\{f \in X^X : f \text{ is a bijection}\}$  is a concrete group on  $X$ , we call it *symmetric group* on  $X$ , denoted by  $\text{Sym}(X)$ . The elements of  $\text{Sym}(X)$  are called *permutations*.

2.  $\{\text{id}_X\}$  is a concrete group.
3.  $I = \{f \in \text{Sym}(\mathbb{R}) : \forall x, y \in \mathbb{R}, x < y \Rightarrow f(x) < f(y)\}$  is a concrete group on  $\mathbb{R}$ .
  - (a)  $\text{id}_{\mathbb{R}} \in I$
  - (b)  $f \in I \Rightarrow f^{-1} \in I$ . Take  $x, y \in \mathbb{R}$  with  $x < y$ , our goal is to show that  $f^{-1}(x) < f^{-1}(y)$ . Suppose not, then  $f^{-1}(x) > f^{-1}(y)$ , but  $f$  is increasing, so  $f(f^{-1}(x)) > f(f^{-1}(y)) \Rightarrow x > y$ , contradicts  $x < y$ .
  - (c)  $f, g \in I \Rightarrow f \circ g \in I$ , take  $x, y \in \mathbb{R}$  with  $x < y$ , then  $g(x) < g(y)$ , so  $f(g(x)) < f(g(y))$ .
4. Let  $X \subseteq \mathbb{R}^n$ , a bijection  $f : X \rightarrow X$  is an *isometry* if for all  $x, y \in X$ ,  $\|x - y\|_2 = \|f(x) - f(y)\|_2$ .  $\text{Iso}(X) := \{f \in \text{Sym}(X) : f \text{ is an isometry}\}$  is a concrete group.
5. Let  $X \subseteq \mathbb{R}^n$ , a bijection  $f : X \rightarrow X$  is a *homeomorphism* if  $f$  and  $f^{-1}$  are continuous.  $\text{Homeo}(X) := \{f \in \text{Sym}(X) : f \text{ is a homeomorphism}\}$  is a concrete group on  $X$ .

**Exercise 3.3.** Show that  $\{f \in \text{Sym}(X) : f \text{ is continuous}\}$  might not be a concrete group.

6. Graphs: Let  $G = (V, E)$ , an *automorphism* of  $G$  is a bijection  $f : V \rightarrow V$ , such that for any  $x, y \in V$  with  $\{x, y\} \in E \Leftrightarrow \{f(x), f(y)\} \in E$ .  $\text{Aut}(G) := \{f \in \text{Sym}(V) : f \text{ is an automorphism}\}$  is a concrete group on  $V$ . Below are several graphs illustrated this idea:



The first graph is just a long path, there are only two automorphisms, namely, the identity and flip the entire path, notice no matter the length of this path, there are only these two kinds of automorphisms.

The second graph is a triangle, and  $\text{Aut}(G) = \text{Sym}(\{0, 1, 2\})$ . Why? No matter how we permute the three vertices, it remains an automorphism, thus, the automorphisms are exactly all permutations.

The last one is a 4-cycle, and  $|\text{Aut}(G)| = 8$ . To do the counting, we can first put vertex 0: 4 positions to put. Then there are 2 ways to put 1. After that, everything is fixed, so in total  $4 \times 2 = 8$  automorphisms.

Two quick definitions:  $C_n :=$  cycle of length  $n$ , and  $D_{2n} := C_n$ . Perhaps another name for  $D_{2n}$  is much more famous: it is the *dihedral group* of order  $2n$ , and  $|\text{Aut}(G)| = 2n$ , we typically use  $|D_{2n}|$  to denote this number.

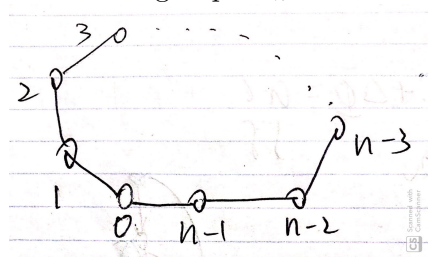
7. Let  $G$  be a concrete group on a set  $X$ , a function  $f \in \text{Sym}(G)$  is an *automorphism* of  $G$  if for any  $g, h \in G$ ,  $f(g \circ h) = f(g) \circ f(h)$ . It is not hard to show that if  $f$  is an automorphism of  $G$ , then  $f(\text{id}_X) = \text{id}_X$ , therefore,  $\text{Aut}(G) := \{f \in \text{Sym}(G) : f \text{ is an automorphism of } G\}$  is a concrete group on  $G$ .
8. Let  $X$  be a set and  $f \in \text{Sym}(X)$ , for  $n \in \mathbb{N}$ , we write  $f^n := \underbrace{f \circ f \circ \dots \circ f}_n$ ,  $f^0 := \text{id}_X$ ,  $f^{n+1} := f \circ f^n$ . Also, let  $f^{-n} := (f^{-1})^n$ .

**Exercise 3.4.** For any  $n, m \in \mathbb{Z}$ , show that:

- (a)  $f^{-n} = (f^n)^{-1}$
- (b)  $(f^n)^m = f^{nm}$
- (c)  $f^n \circ f^m = f^{n+m}$

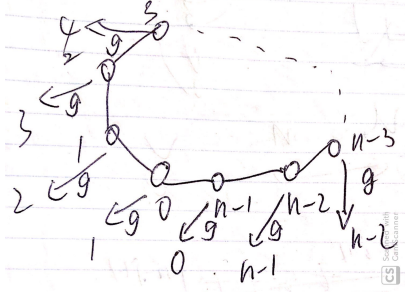
From this, it follows that  $\langle f \rangle := \{f^n : n \in \mathbb{Z}\}$  is a concrete group on  $X$ , this group is called the *cyclic group* generated by  $f$ .

Now let's dive deeper into the study of dihedral group. It is useful to keep the following picture of dihedral group  $D_{2n}$  in mind:



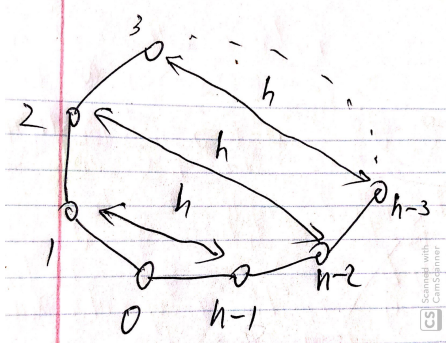
$D_{2n}$  is just all automorphisms on the cycle of length  $n$ , and for  $n \geq 3$ , we have  $|D_{2n}| = 2n$ . Consider the following 2 elements of  $D_{2n}$ :

- $g :=$



i.e.,  $g$  rotates the cycle to the left, by 1.

•  $h :=$



i.e.,  $h$  flips the cycle along the fixed 0 axis.

**Proposition 3.5.** Elements of  $D_{2n}$  are  $\text{id} = g^0, g^1, g^2, \dots, g^{n-1}$ , and  $h = g^0 \circ h, g^1 \circ h, g^2 \circ h, \dots, g^{n-1} \circ h$ .

*Proof.* Take any  $f \in D_{2n}$ , let  $k := f(0)$ , we wish to express  $f$  either as  $g^k$  or  $g^k \circ h$ , let  $f' := g^{-k} \circ f$ , clearly,  $f'(0) = g^{-k} \circ f(0) = g^{-k}(k) = 0$ , so  $f'$  is either  $\text{id}$  or  $h$ . Moreover, we can write  $f$  as  $g^k \circ f'$ , this completes the proof.  $\square$

**Exercise 3.6.** For each  $k, \ell$ , compute  $(g^k \circ h^\ell)(0)$  and  $(g^k \circ h^\ell)(1)$ , and conclude that  $2n$  functions listed in the claim are distinct.

*Proof Sketch.* For different  $k$ ,  $(g^k \circ h^\ell)(0)$  must be different. For fixed  $k$ ,  $g^k(1) \neq g^k \circ h(1)$ .  $\square$

Observe that  $D_{2n}$  is the smallest group containing  $g, h$ . Indeed, if  $G$  is a group containing  $g, h$ , then for any  $k, \ell$ ,  $g^k \circ h^\ell \in G$ , so  $D_{2n} \subseteq G$ . We say that  $D_{2n}$  is *generated* by  $g, h$ .

**Lemma 3.7.** Let  $X$  be a set,  $\mathcal{G}$  be a set of concrete groups of  $G$ , define  $\bigcap \mathcal{G} := \{f \in \text{Sym}(X) : \forall G \in \mathcal{G}, f \in G\}$ . Then  $\bigcap \mathcal{G}$  is also a concrete group.

*Proof.* 1.  $\text{id}_X \in \bigcap \mathcal{G}$ , since for any  $G$ ,  $\text{id}_X \in G$ .

2. if  $f \in \bigcap \mathcal{G}$ , then  $f^{-1} \in \bigcap \mathcal{G}$ , to see this, notice that for any  $G$ ,  $f \in G$ , and  $G$  is a concrete group, so for any  $G$ ,  $f^{-1} \in G \Rightarrow f^{-1} \in \bigcap \mathcal{G}$ .

3. if  $f, g \in \bigcap \mathcal{G}$ , then apply the same argument,  $f \circ g \in \bigcap \mathcal{G}$ .  $\square$

**Definition 3.8.** If  $S \subseteq \text{Sym}(X)$ , then  $\langle S \rangle := \bigcap \{G : G \text{ is a concrete group on } X \text{ such that } S \subseteq G\}$  is a concrete group by 3.7, furthermore,  $S \subseteq \langle S \rangle$ , so  $\langle S \rangle$  is the smallest group containing  $S$  as a subset.  $\langle S \rangle$  is called the *group generated by*  $S$ .

For example, if  $f \in \text{Sym}(X)$ , then  $\langle f \rangle = \langle \{f\} \rangle$ , and more generally, we write  $\langle \{f_1, f_2, \dots, f_n\} \rangle$  as  $\langle f_1, f_2, \dots, f_n \rangle$ , e.g., with  $g, h \in D_{2n}$ , we have  $D_{2n} = \langle g, h \rangle$ .

The next proposition will show that, we can write elements of  $\langle S \rangle$  in a more structured way.

**Proposition 3.9.** *Let  $X$  be a set,  $S \subseteq \text{Sym}(X)$ , then*

$$\langle S \rangle = \{g_1^{\epsilon_1} \circ g_2^{\epsilon_2} \circ \dots \circ g_k^{\epsilon_k} : k \in \mathbb{N}, g_1, \dots, g_k \in S, \epsilon_1, \dots, \epsilon_k \in \{-1, 1\}\}$$

*Proof.* Let  $H$  denote the set on RHS, clearly,  $H \subseteq \langle S \rangle$ , and also,  $S \subseteq H$ . So to argue for the other inclusion, it suffices to show  $H$  is a group, then we will have  $\langle S \rangle \subseteq H$  automatically.

- Take  $k = 0$ , we have  $g_0 = \text{id}_X \in H$ .
- Suppose  $f \in H = g_1^{\epsilon_1} \circ \dots \circ g_k^{\epsilon_k}$ , then  $f^{-1} = g_k^{-\epsilon_k} \circ g_{k-1}^{-\epsilon_{k-1}} \circ \dots \circ g_1^{-\epsilon_1} \in H$ .
- If  $f, g \in H$ , then it's clear  $f \circ g \in H$ : we just express it by adding a  $\circ$  between the representation of  $f$  and  $g$ .

□

Let's look at some examples of groups generated by a set of elements.

**Example 3.10.** 1. Rubik's cube: let  $X$  be a set of cardinality 48, and  $S :=$  set of 6 individual rotations, viewed as permutations on  $X$ . The Rubik's group is  $\langle S \rangle$ .

2. The *lamplighter group* is defined as follows:  $X = \{0, 1\}^{\mathbb{Z}} \times \mathbb{Z}$ , and there are two functions:

- $g$  : move to the next light, i.e.,  $g(x, n) := (x, n + 1)$ .
- $h$  : switch the light the person is currently standing by, i.e.,  $h(x, n) := (x', n)$ , where 
$$x'_i = \begin{cases} 1 - x_i, & \text{if } i = n \\ x_i, & \text{otherwise} \end{cases}$$

We use  $\langle g, h \rangle$  to denote the lamplighter group.



### 3.2 Abstract groups

**Definition 3.11.** A *binary operation* on a set  $S$  is a function  $\star : S \times S \rightarrow S$ .

**Example 3.12.** 1. If  $G$  is a concrete group on  $X$ , then  $\circ : G \times G \rightarrow G$  is a binary operation, where  $\circ(f, g) = f \circ g$ . Note:  $\star$  is always written as an infix operator.

2. There are tons of binary operations on  $\mathbb{Z}$ :  $+$  on  $\mathbb{Z}$ ,  $*$  on  $\mathbb{Z}$ , and  $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} : (n, m) \mapsto n$ .

**Definition 3.13.** A binary operation  $\star : S \times S \rightarrow S$  is *associative* if  $\forall a, b, c \in S : (a \star b) \star c = a \star (b \star c)$ .

**Definition 3.14.** Let  $\star$  be a binary operation on  $S$ , then an element  $e \in S$  is an *identity* for  $\star$  if for all  $a \in S$ ,  $a \star e = e \star a = a$ .

**Lemma 3.15.** Let  $\star$  be a binary operation on  $S$ , then  $\star$  has at most one identity.

*Proof.* Suppose both  $e$  and  $e'$  are identities for  $\star$ , then  $e \star e' = e = e'$ . □

**Definition 3.16.** Let  $\star$  be a binary operation with identity element  $e$  on  $S$ , an *inverse* of an element  $a$  is an element  $b \in S$  such that  $a \star b = b \star a = e$ .

**Exercise 3.17.** Given an example of a binary operation  $\star$  with identity such that there is an element with more than one inverse.

You can intentionally assign two elements as inverse to some element, then force those two elements to be different from each other.

**Lemma 3.18.** If  $\star$  is associative, with identity  $e$ , then for any  $a \in S$ , if it has inverse, then it has at most one inverse.

*Proof.* Suppose  $b, b'$  are inverses of  $a$ , then compute  $b \star a \star b' = (b \star a) \star b' = e \star b' = b'$ , on the other hand,  $b \star a \star b' = b \star (a \star b') = b \star e = b$ , by associativity, we have  $b = b'$ . □

After setting up enough definitions, we are ready to define abstract groups.

**Definition 3.19.** An *abstract group*, or *group* for short, is a set  $G$  with a binary operation  $\star$  such that

- $\star$  is associative.
- $\star$  has an identity.
- each  $a \in G$  has an inverse with respect to  $\star$ .

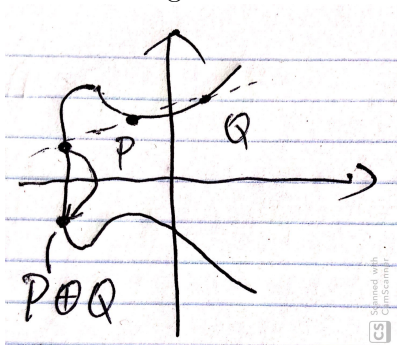
The main example: if  $G$  is a concrete group on  $X$ , then  $(G, \circ)$  is a group.  
Some quick examples:  $(\mathbb{N}, +)$  is not a group, but  $(\mathbb{Z}, +)$  is a group.  $(\mathbb{R}, *)$  is not a group, but  $(\mathbb{R} \setminus \{0\}, *)$  is a group.

**Exercise 3.20.** Let  $X$  be a set, recall  $\Delta$  is the symmetric difference operation on two sets, then  $(\mathcal{P}(X), \Delta)$  is a group.

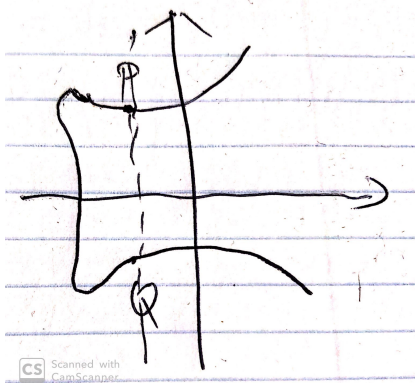
Some more examples of groups:

**Example 3.21.** 1.  $\mathbb{Z}/n\mathbb{Z}$ : let  $n \geq 2$  be an integer, and  $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ ,  $+_n$  : addition modulo  $n$ , i.e., for  $x, y \in \mathbb{Z}_n$ , define  $x +_n y$  to be the remainder of  $x + y$  after divided by  $n$ . Then,  $(\mathbb{Z}_n, +_n)$  is a group. Please verify this. The nasty part is to verify that  $+_n$  is associative.

2. Elliptic curves: An elliptic curve is the set of points  $(x, y) \in \mathbb{R}^2$ , satisfying an equation of the form  $y^2 = x^3 + ax + b$ , for example,  $y^2 = x^3 - x + 1$ . We denote the set by  $E$ . Let's illustrate this with diagram:



Let  $*$  be an extra element not in  $E$ , define an operation  $\oplus$  on  $E \cup \{*\}$  as follows:  $P \oplus Q \Rightarrow$  take tangent of the line  $PQ$ , find its third intersection with  $E$ , then flip that point with respect to  $x$  axis. What if  $PQ$  intersects  $E$  only on  $P$  and  $Q$ ? For example, consider



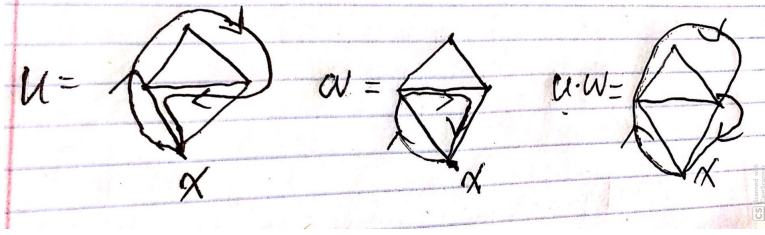
Then define  $P \oplus Q = *$ . For all  $P \in E$ , define  $* \oplus P = P \oplus * = P$ , and  $* \oplus * = *$ , i.e.,  $*$  is the identity element. This turns  $E \cup \{*\}$  into a group.

3. Let  $G$  be a connected graph, fix a vertex  $x \in V(G)$ , define  $\Pi_1(G, x)$ , the *homotopy group* of  $G$ , as follows:

$$\Pi_1(G, x) := \{\text{all non-backtracking closed walks in } G, \text{ start and end at } x\}$$

Here, non-backtracking just means if you have used edge  $(u, v)$ , you cannot immediately take the edge  $(v, u)$ .

Given two walks  $u$  and  $w$ ,  $u \cdot w$  is the walk obtained from  $u$  and  $w$  by concatenating them and removing all backtrack edges. For example,



This defines a group.

**Theorem 3.22** (Cayley). *Every abstract group is isomorphic to a concrete group, i.e., for all groups  $(G, \star)$ , there exists a set  $X$ , a concrete group  $H$  on  $X$ , and a bijection  $\varphi : G \rightarrow H$ , such that for all  $f, g \in G$ , we have  $\varphi(f \star g) = \varphi(f) \circ \varphi(g)$ .*

*Proof.* Take  $X = G$ . For each  $g \in G$ , let  $\varphi(g) : G \rightarrow G$  be the function given by  $\varphi(g)(h) := g \star h$ . We prove a sequence of propositions, to show that this  $\varphi$  gives us the desired result.

**Proposition 3.23** (Closure of  $\varphi$ ). *For all  $f, g \in G$ ,  $\varphi(f \star g) = \varphi(f) \circ \varphi(g)$ .*

*Proof of Closure.* Take  $h \in G$ .  $\varphi(f \star g)(h) = (f \star g) \star h$ , while  $\varphi(f) \circ \varphi(g)(h) = \varphi(f)(g \star h) = f \star (g \star h)$ . By associativity of  $\star$ , the identity holds.  $\square$

The next part will focus on proving  $\varphi$  is an isomorphism, i.e., it is a bijection. By 3.23, we need to show the following:

**Proposition 3.24.** *Let  $e$  be the identity of  $G$ , then  $\varphi(e) = \text{id}_G$ .*

*Proof of identity.* Take  $h \in G$ ,  $\varphi(e)(h) = e \star h = h$ , for all  $h$ , so  $\varphi(e) = \text{id}_G$ .  $\square$

The next proposition will be useful in finding our concrete group  $H$ .

**Proposition 3.25.** *For all  $g \in G$ ,  $\varphi(g)$  is a bijection.*

*Proof of  $\varphi(g)$  bijectivity.* We claim that the inverse of  $\varphi(g)$  is  $\varphi(g^{-1})$ .

$$\varphi(g) \circ \varphi(g^{-1}) = \varphi(g \star g^{-1}) = \varphi(e) = \text{id}_G$$

$$\varphi(g^{-1}) \circ \varphi(g) = \varphi(g^{-1} \star g) = \varphi(e) = \text{id}_G$$

$\square$

So we can view  $\varphi$  as a function from  $G$  to  $\text{Sym}(G)$ , where  $H := \text{im}(\varphi) = \{\varphi(g) : g \in G\}$ .

**Proposition 3.26.**  *$H$  is a concrete group on  $G$ .*

*Proof of  $H$  is a concrete group.* •  $\text{id}_G \in H$ , since  $e \in G$ ,  $\varphi(e) \in H$ .

- If  $f \in H$ , then  $f^{-1} \in H$ : suppose  $f = \varphi(g)$  for some  $g \in G$ , then  $f^{-1} = \varphi(g^{-1}) \in H$ .
- If  $f_1, f_2 \in H$ , then  $f_1 \circ f_2 \in H$ : since  $\varphi(g_1) \circ \varphi(g_2) = \varphi(g_1 \star g_2) \in H$ .

$\square$

Finally, we are ready to show  $\varphi$  is a bijection.

**Proposition 3.27.**  *$\varphi : G \rightarrow H$  is a bijection.*

*Proof.* Surjectivity comes from definition of  $H$ : it is  $\text{im}(\varphi)$ . What about injectivity? If  $\varphi(g_1) = \varphi(g_2)$ , then  $\varphi(g_1)(e) = g_1 \star e = g_1 = \varphi(g_2)(e) = g_2 \star e = g_2$ .  $\square$

This completes the proof of Cayley's theorem.  $\square$

Let's examine 3.22 on Dihedral group. Recall  $D_{2n} = \langle g, h \rangle$ , where  $g$  is rotate by 1, and  $h$  is flip with respect to 0 axis. What is  $\varphi(g)$ ? If we apply it to other elements, the result will be further shifted by 1. What about  $\varphi(h)$ ? It will flip all elements.

### 3.3 Abelian groups, subgroups, homomorphisms

In this section, we extend more on structures of abstract groups. We introduce three important concepts, that will be used across all later sections.

We first introduce some conventions, to simplify the notation. Often, we just say “ $G$  is a group” without mentioning the operation. In such case, the operation is called “multiplication” and denoted by  $a \cdot b$  or simply,  $ab$ . There’s a notable exception, i.e., groups with addition, such as  $(\mathbb{Z}, +)$ .

**Definition 3.28.** A binary operation  $\star$  on set  $S$  is *commutative* if order does not matter, i.e.,  $a \star b = b \star a$ , for any  $a, b \in S$ .

**Definition 3.29.** If  $(G, \star)$  is a group and  $\star$  is commutative, we say that  $(G, \star)$  is an *abelian group*. In this case, often the operation is denoted by “ $+$ ”. We write  $-x$  for  $x^{-1}$ , and  $0$  as identity. Also,  $nx$  is used to denote  $x^n$ .

An exception to the above convention:  $(\mathbb{Q} \setminus \{0\}, \cdot)$  is abelian.

**Definition 3.30.** Let  $(G, \star)$ ,  $(H, \cdot)$  be groups, a function  $\varphi : G \rightarrow H$  is a *homomorphism* if  $\varphi(g \star h) = \varphi(g) \cdot \varphi(h)$ .

**Exercise 3.31.** If  $\varphi : G \rightarrow H$  is a homomorphism, where  $G, H$  are groups with identities  $e_G, e_H$ , then  $\varphi(e_G) = e_H$ , and for all  $g \in G$ ,  $\varphi(g^{-1}) = (\varphi(g))^{-1}$ .

It’s not hard to see that, for any  $g \in G$ ,  $\varphi(g) = \varphi(g \cdot e_G) = \varphi(g) \cdot \varphi(e_G)$ , so  $\varphi(e_G) = e_H$ . A similar argument can be used to show the inverse part.

Given the definition of homomorphism, it is natural to ask: if we have two groups  $G, H$ , does there exist a homomorphism from  $G$  to  $H$ ? The answer is yes. Simply map every element of  $G$  to  $e_H$ , then this is a valid homomorphism. Remarkably, one can show that this is the only valid homomorphism between certain groups.

**Exercise 3.32.** Consider  $(\mathbb{Z}_n, +)$  as a group, show that there is no non-trivial homomorphism from  $\mathbb{Z}_4$  to  $\mathbb{Z}_7$ .

We have seen the definition of isomorphism between two sets before, here we extend it to groups.

**Definition 3.33.** A bijective homomorphism from  $G$  to  $H$  is called an *isomorphism*. If an isomorphism from  $G$  to  $H$  exists, we say that  $G$  and  $H$  are *isomorphic*, denoted by  $G \cong H$ .

**Exercise 3.34.** Show that the inverse of an isomorphism from  $G$  to  $H$  is an isomorphism from  $H$  to  $G$ .

Recall that in 3.22, our argument has showed that the map from  $G$  to  $\text{Sym}(G)$  by  $g \mapsto (h \mapsto gh)$  is an injective homomorphism. We abstract this intuition further.

**Definition 3.35.** Let  $(G, \star)$  be a group. Given a subset  $S \subseteq G$ , define  $\star_S : S \times S \rightarrow G$  by  $a \star_S b = a \star b$ . If  $\star_S$  is a binary operation on  $S$ , i.e.,  $\text{im}(\star_S) \subseteq S$ , and  $(S, \star_S)$  is a group, then  $(S, \star_S)$  or  $S$  is called a *subgroup* of  $G$ , denoted by  $S \leq G$ .

**Lemma 3.36.** Let  $G$  be a group,  $S \subseteq G$ , then  $S \leq G$  if and only if the following conditions hold:

1.  $e \in S$

2. if  $g \in S$ , then  $g^{-1} \in S$
3. if  $g, h \in S$ , then  $gh \in S$

In particular, a concrete group on set  $X$  is the same as a subgroup of  $\text{Sym}(X)$ .

*Proof.* ( $\Leftarrow$ ) : By the three conditions,  $S$  is a group, and  $S$  is closed under group operation, so  $S \leq G$ .

( $\Rightarrow$ ) : Suppose  $S \leq G$ , condition 3 holds by definition, it suffices to show the other two conditions.

1. We need to show  $e_S = e$ . The first observation is, for any element  $g \in G$ , if  $g^2 = g$ , then  $g = e$ . Why? Given  $g^2 = g$ , we can multiply both sides by  $g^{-1}$ , get  $g = e$ . Indeed,  $e_S^2 = e_S$ , so  $e_S = e$ .
2. We need to show that, if  $g \in S$  and  $h$  is the inverse of  $g$  in  $S$ , then  $h = g^{-1}$ . Indeed,  $gh = hg = e_S = e$ , and  $h = g^{-1}$ , as desired.  $\square$

**Proposition 3.37.** Suppose  $\varphi : G \rightarrow H$  is a homomorphism, then  $\text{im}(\varphi) \leq H$ .

*Proof.* It suffices to check three conditions in 3.36.

- Since  $\varphi(e_G) = e_H$ , we have  $e_H \in \text{im}(\varphi)$ .
- Suppose  $h \in \text{im}(\varphi)$ , then there exists some  $g \in G$  such that  $\varphi(g) = h$ . Since  $(\varphi(g))^{-1} = \varphi(g^{-1})$ ,  $h^{-1} \in \text{im}(\varphi)$ .
- Suppose  $h_1, h_2 \in \text{im}(\varphi)$ , then there exists  $g_1, g_2 \in G$  being mapped to them by  $\varphi$ . Since  $\varphi$  is a homomorphism, we have  $h_1 h_2 = \varphi(g_1 g_2)$ , so  $h_1 h_2 \in \text{im}(\varphi)$ .  $\square$

Observe that if  $\varphi$  is injective, then trivially, we have  $G \cong \text{im}(\varphi)$ .

### 3.4 Actions, cosets, orbits

Groups are interesting structures with nice property we can leverage. Can we extend it to arbitrary set? We do so by defining *action*.

**Definition 3.38.** Let  $G$  be a group, an *action* on a set  $X$  is a homomorphism  $\alpha : G \rightarrow \text{Sym}(X)$ .

For notations, we usually denote domain and codomain of  $\alpha$  as  $\alpha : G \curvearrowright X$ , and often, instead of  $\alpha(g)(x)$ , we write  $g \cdot_\alpha x$  or  $g \cdot x$  if  $\alpha$  is clear from context.

**Example 3.39.** 1. Consider  $\alpha : G \curvearrowright G$  given by  $g \cdot h = gh$ , this is called the *left multiplication action*.

2.  $\alpha : G \curvearrowright G$  given by  $g \cdot h = hg^{-1}$ , this is called the *right multiplication action*. Let's verify it is an action. Suppose  $g_1, g_2, h \in G$ , then  $(g_1 g_2) \cdot h = h(g_1 g_2)^{-1} = hg_2^{-1} g_1^{-1} = g_1 \cdot (hg_2^{-1}) = g_1 \cdot g_2 \cdot h$ .

Moreover, the map  $G \rightarrow G : h \mapsto hg^{-1}$  is a bijection, we left to reader to check this.

3. The trivial action:  $G \curvearrowright X : g \cdot x = x$ , for all  $g \in G, x \in X$ .

**Definition 3.40.** A *right action* of  $G$  on  $X$  is a function  $\beta : G \rightarrow \text{Sym}(X)$ , such that for all  $g_1, g_2 \in G$ ,  $\beta(g_1 g_2) = \beta(g_2) \circ \beta(g_1)$ . We usually write it as  $\beta : X \curvearrowleft G$ , and  $x \cdot_\beta g$  or  $x \cdot g$  for  $\beta(g)(x)$ . With this notation, the requirement of  $\beta$  can be written as  $(x \cdot g_1) \cdot g_2 = x \cdot (g_1 g_2)$ .

So we can define *right multiplication action* via  $h \cdot g = hg$ , also,  $h \cdot g = g^{-1}h$ .

**Definition 3.41.** The *shift action*  $\sigma : G \curvearrowright \mathcal{P}(G)$ , defined as  $g \cdot S := gS := \{gh : h \in S\}$ .

Notice that  $\mathcal{P}(G) \cong \{0, 1\}^G$ , so we can view this action as  $G \curvearrowright \{0, 1\}^G$ . More generally, there is a shift action  $G \curvearrowright X^G$  for any set  $G$ : take  $g \in G$ ,  $f \in X^G$ , then  $g \cdot f \in X^G$  is a function  $G \rightarrow X$ , given by  $(g \cdot f)(h) := f(g^{-1}h)$ , for all  $h \in G$ . It is instrumental for the reader to verify this is in fact an action.

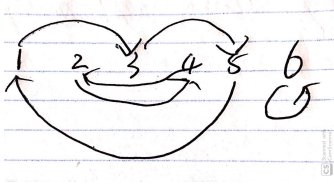
Even more generally, given any action  $G \curvearrowright Y$ , we can “lift” it to an action  $G \curvearrowright X^Y$ : for  $f \in X^Y$ , define  $g \cdot f : y \mapsto f(g^{-1} \cdot y)$ .

An important type of action to study is actions of  $(\mathbb{Z}, +)$ . What does this kind of actions look like? Let  $\alpha : \mathbb{Z} \curvearrowright X$ , then  $\alpha(0) = \text{id}_X$ , suppose  $\alpha(1) := f \in \text{Sym}(X)$ , then  $\alpha(n) = f^n$ , for all  $n \in \mathbb{Z}$ . This is true, since we can view  $\mathbb{Z}$  as generated by 1, since  $\alpha$  is a homomorphism, it must preserve such a structure. Thus, there is a natural bijection between  $\{\text{actions of } \mathbb{Z} \curvearrowright X\}$  and  $\text{Sym}(X)$ , given by  $\alpha \mapsto \alpha(1)$ .

**Example 3.42.** Consider  $\alpha : \mathbb{Z} \curvearrowright [6]$ , given by  $\alpha(1) = \begin{bmatrix} 3 \\ 4 \\ 5 \\ 2 \\ 1 \\ 6 \end{bmatrix}$ . We write in a vector form, since

essentially,  $\text{Sym}([6])$  are permutations, so we just need to specify where does each number go. The

following diagram illustrates this action:



**Definition 3.43.** Let  $\alpha : G \curvearrowright X, x \in X$ . The *orbit* of  $x$  under  $\alpha$  is the set  $G \cdot_\alpha x = G \cdot x := \{g \cdot x : g \in G\}$ .

**Definition 3.44.** The *orbit equivalence relation*,  $E_\alpha$ , is the binary relation on set  $X$ , given by  $x E_\alpha y \Leftrightarrow y \in G \cdot_\alpha x$ .

**Exercise 3.45.** Verify this is an equivalence relation.

**Exercise 3.46.** For actions of  $(\mathbb{Z}, +)$ , orbits are the following type: single element orbit, two elements orbit, three elements orbit, etc., and another type: a long chain that does not end.

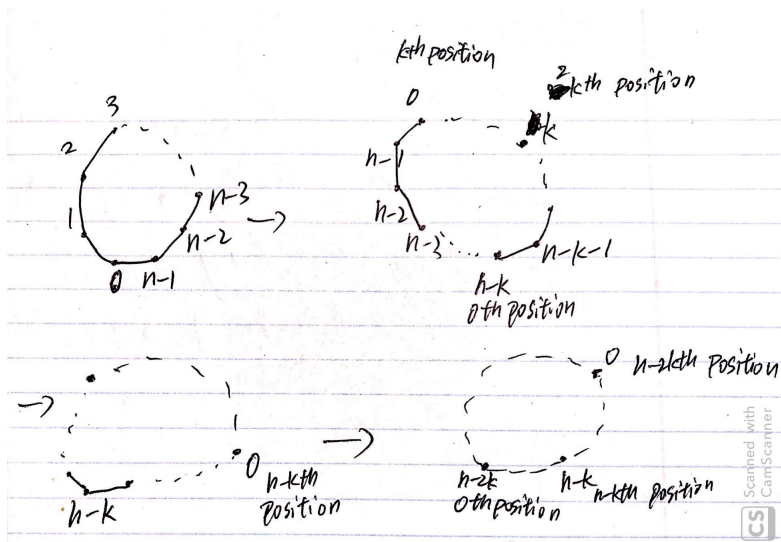
The next example introduces an important type of action, which plays a major role in a bunch of concepts in abstract groups.

**Example 3.47.** The *conjugation action*,  $\alpha_{conj} : G \curvearrowright G : g \cdot h := ghg^{-1}$ . Let's verify it is a homomorphism:  $\alpha_{conj}(g_1 g_2)(h) = g_1 g_2 h (g_1 g_2)^{-1} = g_1 g_2 h g_2^{-1} g_1^{-1} = g_1 \alpha_{conj}(g_2)(h) g_1^{-1} = \alpha_{conj}(g_1) \circ \alpha_{conj}(g_2)(h)$ . Recall that  $\text{Aut}(G) = \{\text{automorphisms of } G\} \leq \text{Sym}(G)$ , and definition of automorphism can be found in 7, i.e., functions that preserve compositions of elements. We can effectively view  $\alpha_{conj} : G \rightarrow \text{Aut}(G)$ . What we need to argue is: for all  $g \in G$ ,  $\alpha_{conj}(g) : G \rightarrow G$  is a homomorphism, i.e., for any  $h_1, h_2 \in G$ ,  $\alpha_{conj}(g)(h_1 h_2) = \alpha_{conj}(g)(h_1) \alpha_{conj}(g)(h_2)$ .

$$\begin{aligned} \alpha_{conj}(g)(h_1 h_2) &= gh_1 h_2 g^{-1} \\ &= gh_1 g^{-1} g h_2 g^{-1} \\ &= (gh_1 g^{-1})(gh_2 g^{-1}) \\ &= \alpha_{conj}(g)(h_1) \alpha_{conj}(g)(h_2) \end{aligned}$$

Let's examine conjugation action on dihedral group,  $D_{2n}$ . What is the orbit of  $h$  under conjugation? Clearly,  $hhh = h$ , and for any rotation  $g^k$ ,  $g^k h g^{-k}$  is as follows: first rotate 0 to  $k$ , and  $n - k$  to 0, then flips it with respect to fixed 0 axis, which results in  $k$  goes to  $n - k$ , which can be viewed as the original 0 goes to  $n - k$ . Finally,  $g^{-k}$  rotates  $n - k$  to  $n - 2k$  and  $k$  to 0. It is a bit abstract to talk in this way, the following diagram illustrates the behavior:





One can view this as flip with respect to  $n - k$  axis.

Similar to  $E_\alpha$ , we use  $E_{conj}$  to denote the orbit equivalence relation under conjugation action, i.e.,  $g$  and  $h$  are conjugate if and only if  $gE_{conj}h$ .

A quick observation on abelian group:  $G$  is abelian if and only if the conjugation action is trivial.

For forward implication, notice that  $\alpha(g)(h) = ghg^{-1} = gg^{-1}h = h$ . For converse,  $ghg^{-1} = h \rightarrow gh = hg$ .

**Definition 3.48.** Let  $\text{Sub}(G) := \{H \subseteq G : H \leq G\}$ , instead of conjugating elements, we can extend the definition by conjugating the entire subgroup, i.e.,  $\alpha_{conj} : G \curvearrowright \text{Sub}(G)$  by  $g \cdot H = gHg^{-1} := \{ghg^{-1} : h \in H\}$ . Moreover,  $g \cdot H$  is actually a subgroup of  $G$ , so we can further extend  $E_{conj} :=$  the orbit equivalence relation on  $\text{Sub}(G)$ . We say two subgroups  $H_1, H_2$  are *conjugate*, if  $H_1E_{conj}H_2 \Rightarrow gH_1g^{-1} = H_2$ , for some  $g \in G$ . This even gives an isomorphism between this two subgroups, the mapping is  $h_1 \mapsto gh_1g^{-1}$ , so  $H_1E_{conj}H_2 \Rightarrow H_1 \cong H_2$ .

**Definition 3.49.** A subgroup  $H \leq G$  is *normal* if  $G \cdot_{conj} H = \{H\}$ , notation:  $H \trianglelefteq G$ .

**Example 3.50.** 1.  $\{e\}$ , the trivial subgroup.

2. If  $G$  is abelian, then every subgroup is normal.

3.  $G = D_{2n}$ , the dihedral group.  $\langle h \rangle = \{h, e\}$  is not a normal subgroup of  $D_{2n}$ , define  $h_i :=$  flip with respect to axis  $i$ , then  $h$  is conjugate to  $h_i$  by  $g^i$ . So  $\langle h \rangle$  is conjugate to  $\langle h_i \rangle$ , but they are not equal if  $i \neq 0$ .

On the other hand,  $\langle g \rangle \trianglelefteq D_{2n}$  is a normal subgroup: any  $g^k$  act on it results in the same group, and  $h \cdot g^i = g^{n-i}$ .

**Definition 3.51.** Let  $\alpha : G \curvearrowright X, \beta : G \curvearrowright Y$ , a *homomorphism* from  $\alpha$  to  $\beta$  is a function  $\varphi : X \rightarrow Y$  such that for any  $g \in G, x \in X$ , we have  $\varphi(g \cdot_\alpha x) = g \cdot_\beta \varphi(x)$ . Another term to describe  $\varphi$  is, it is  $G$ -equivalent. A diagram:

$$\begin{array}{ccc}
X & \xrightarrow{\alpha(g)} & X \\
\downarrow \varphi & & \downarrow \varphi \\
Y & \xrightarrow{\beta(g)} & Y
\end{array}$$

If  $\varphi$  is bijective, then  $\varphi$  is an *isomorphism*.

**Example 3.52.** Consider the following two  $\mathbb{Z}$  actions on  $[5]$ , i.e., permutations on  $[5]$ :  $\begin{bmatrix} 3 \\ 4 \\ 5 \\ 2 \\ 1 \end{bmatrix}$  and

$\begin{bmatrix} 2 \\ 1 \\ 4 \\ 5 \\ 3 \end{bmatrix}$ , these two  $\mathbb{Z}$  actions are isomorphic. How to figure it out? Notice in the first action, there are

two orbits:  $1 - 3 - 5$  and  $2 - 4$ , while in the second action, there are also two orbits:  $1 - 2$  and  $3 - 4 - 5$ , so we can build a bijection between this two orbits. More generally,  $\alpha, \beta$  are isomorphic  $\Leftrightarrow$  there exists a bijection  $b : X/E_\alpha \rightarrow Y/E_\beta$ , such that the type of each orbit in  $O \in X/E_\alpha$  is the same type, or size of  $b(O)$ , i.e.,  $|O| = |b(O)|$ . Generalize this idea further, instead of saying the size of the orbit is the same, we formalize it using action: if there exists a bijection  $b : X/E_\alpha \rightarrow Y/E_\beta$  such that for each orbit  $O \in X/E_\alpha$ , the induced actions  $G \curvearrowright O$  and  $G \curvearrowright b(O)$  are isomorphic.

This helps to reduce the problem to studying actions with just one orbit, and such actions are called *transitive*.

In the next part, it is useful to recall 1.31, the canonical decomposition. Let  $\alpha : G \curvearrowright X$  be an action, pick  $x \in X$ , define  $f_x : G \rightarrow X : g \mapsto g \cdot x$ . Apply 1.31 on  $f_x$ , we get the following diagram:

$$\begin{array}{ccccc}
G & \twoheadrightarrow & X/E_{f_x} & \xrightarrow{\cong} & \text{im}(f_x) \\
& \searrow f_x & & \nearrow & \\
& & X & & 
\end{array}$$

Where  $E_{f_x}$  is the equivalence kernel of  $f_x$ : 1.26, i.e.,  $g_1 E_{f_x} g_2 \Leftrightarrow f_x(g_1) = f_x(g_2) \Leftrightarrow g_1 \cdot x = g_2 \cdot x \Leftrightarrow (g_2^{-1} g_1) \cdot x = x$ . Let's leverage this special structure by defining stabilizer of  $x$ .

**Definition 3.53.** The *stabilizer* of  $x$  is  $\text{Stab}(x) := \{g \in G : g \cdot x = x\}$ .

**Proposition 3.54.**  $\text{Stab}(x) \leq G$ .

*Proof.* Let's check three properties in 3.36.

- First,  $e \cdot x = x$ . To see this, notice any action is an homomorphism, so  $\alpha(e) = \text{id}_X$ , therefore,  $e \cdot x = x$ .
- If  $g \cdot x = x$ , then by property of homomorphism,  $g \cdot g^{-1} \cdot x = g^{-1} \cdot g \cdot x = g^{-1} \cdot x = x$ , so  $g^{-1} \in \text{Stab}(x)$ .

- If  $g, h$  are all fix points, then  $(gh) \cdot x = g \cdot h \cdot x = g \cdot x = x$ , so  $gh \in \text{Stab}(x)$ .  $\square$

**Definition 3.55.** Let  $H \leq G$ , the *left coset equivalence relation* of  $H$ , denoted by  $LC_H$  on  $G$ , is given by  $g_1 LC_H g_2 \Leftrightarrow g_2^{-1} g_1 \in H$ .

$LC_H$  is in fact an equivalence relation, and  $H$  is the orbit equivalence relation under the right action:  $G \curvearrowright H : g \cdot h = gh$ . The orbits of this action are called *left-cosets*. We say that  $g_1 \in \text{orbit of } g_2 \Leftrightarrow g_2^{-1} g_1 \in H \Leftrightarrow g_1 \in g_2 H$ . Consider  $G/LC_H = \{gH : g \in G\}$ , we use  $G/H$  as a shorthand notation for  $G/LC_H$ .

Similarly, *right-cosets* of  $H$  are the orbits of left action  $H \curvearrowright G$  by  $h \cdot g = hg$ , notation:  $H \backslash G = G/RC_H = \{Hg : g \in G\}$ .

With this definition, we can write  $G/E_{f_x}$  as  $G/\text{Stab}(x)$ . The next part in the diagram is  $\text{im}(f_x)$ . What is  $\text{im}(f_x)$ ?  $\text{im}(f_x) = \{f_x(g) : g \in G\} = \{g \cdot x : g \in G\} = G \cdot x$ , i.e., orbit of  $x$ . So we can complete the diagram as follows:

$$\begin{array}{ccccc}
 G & \xrightarrow{\quad} & X/\text{Stab}(x) & \xleftarrow{\quad \cong \quad} & G \cdot x \\
 & \searrow f_x & & \nearrow & \\
 & & X & & 
 \end{array}$$

This is the *orbit-stabilizer theorem*.

### 3.5 Orbit-stabilizer theorem

**Theorem 3.56** (Orbit-Stabilizer Theorem). *Let  $G$  be a group,  $G \curvearrowright X$  be an action, fix  $x \in X$ , let  $f_x : G \rightarrow X : g \mapsto g \cdot x$ . The following diagram holds:*

$$\begin{array}{ccccc} G & \xrightarrow{\quad} & X/\text{Stab}(x) & \xleftarrow{\quad \cong \quad} & G \cdot x \\ & \searrow f_x & & \nearrow & \\ & & X & & \end{array}$$

*Proof.* Direct application of canonical decomposition theorem, with  $E_{f_x} = \text{Stab}(x)$  and  $\text{im}(f_x) = G \cdot x$ .  $\square$

Let's further explore this diagram. Suppose our action is transitive, i.e., there is only one orbit, then  $G \cdot x = X$ . By orbit-stabilizer, it is isomorphic to  $G/\text{Stab}(x)$ , i.e.,  $G$  quotient a subgroup of  $G$ . This observation leads to the following theorem:

**Theorem 3.57.** *Let  $\alpha : G \curvearrowright X$  be a transitive action, then  $\alpha$  is isomorphic to an action  $\beta : G \curvearrowright G/H$ , for a subgroup  $H \leq G$ .*

*Proof.* The action we consider is given by  $g \mapsto (H \mapsto gH)$ , it is clearly an action:  $(g_1 g_2) \cdot_\beta H = g_1 g_2 H = g_1 \cdot_\beta g_2 H = g_1 \cdot_\beta g_2 \cdot_\beta H$ .

Since  $\alpha$  is transitive,  $G \cdot_\alpha x = X$ , and by 3.56,  $G \cdot_\alpha x \cong G/\text{Stab}(x)$ . Let's fix an  $x \in X$ , set  $H = \text{Stab}(x)$ , define  $\varphi : G/H \rightarrow X : gH \mapsto g \cdot_\alpha x$ . We will show  $\varphi$  is an isomorphism by showing it's a homomorphism and a bijection. But first of all, let's show  $\varphi$  is a well-defined function.

- Suppose  $g_1 H = g_2 H$ , we need to show that  $g_1 \cdot_\alpha x = g_2 \cdot_\alpha x$ . Since  $g_1 H = g_2 H$ , we have  $g_2^{-1} g_1 H = H$ , this means  $g_2^{-1} g_1 \in H$ . Why? Let's prove a lemma for this.

**Lemma 3.58.** *Let  $H$  be a subgroup of  $G$ , and  $g \in G$ , then  $gH = H \Rightarrow g \in H$ .*

*Proof of Lemma.* Let's do the contrapositive: if  $g \notin H$ , then  $gH \neq H$ . This is clear: since  $H$  is a subgroup,  $e \in H$ , so  $ge = g \in gH$ , but  $g \notin H$ , so  $gH \neq H$ .  $\square$

So  $g_2^{-1} g_1 \in H$ , recall that  $H = \text{Stab}(x)$ , which means  $(g_2^{-1} g_1) \cdot_\alpha x = x \Rightarrow g_1 \cdot_\alpha x = g_2 \cdot_\alpha x$ .

- Homomorphism: Let  $y \in X$ , our goal:  $\varphi(g_1 \cdot_\beta g_2 H) = g_1 \cdot_\alpha \varphi(g_2 H)$ . LHS is just  $\varphi(g_1 g_2 H) = (g_1 g_2) \cdot_\alpha x$ , while RHS is  $g_1 \cdot_\alpha g_2 \cdot_\alpha x$ , since  $\alpha$  is an action, the identity holds.
- Bijection: Define  $\phi : X \rightarrow G/H$  by  $y \mapsto gH$ , where  $g \cdot_\alpha x = y$ . This is well-defined, since if  $g_1 \cdot_\alpha x = g_2 \cdot_\alpha x = y$ , then  $g_2^{-1} g_1 \cdot_\alpha x = x$ , which means  $g_2^{-1} g_1 \in \text{Stab}(x)$ , so  $g_1 \in g_2 H$ . Similarly,  $g_2 \in g_1 H$ , this shows the mapping is well-defined. Moreover, it is clear that  $\phi$  is the inverse of  $\varphi$ , so  $\varphi$  is a bijection.  $\square$

**Theorem 3.59.** *Given 2 subgroups  $H_1, H_2 \leq G$ , the actions  $G \curvearrowright G/H_1, G \curvearrowright G/H_2$  given by  $g \mapsto (H \mapsto gH)$  are isomorphic, if and only if  $H_1, H_2$  are conjugate to each other.*

*Proof.* Exercise.  $\square$




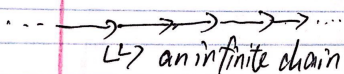
Combine 3.57 and 3.59, we obtain a 1-to-1 correspondence between

$\{\text{isomorphism classes of transitive actions of } G\}$

and

$\{\text{conjugacy classes of subgroup of } G\}$

**Example 3.60.** Consider  $G = (\mathbb{Z}, +)$ . In 3.46, we have studied orbits of  $(\mathbb{Z}, +)$ , now let's establish connections between isomorphic classes of transitive actions or “the shape of orbits” and conjugacy classes of subgroups of  $\mathbb{Z}$ .

isomorphic classes of transitive action	conjugacy classes of subgroup of $\mathbb{Z}$
	$\mathbb{Z}$
	$2\mathbb{Z}$
	$3\mathbb{Z}$
$\vdots$	$\vdots$
 $\hookrightarrow$ an infinite chain	$\{0\}$

One way to think of this is actions of  $\mathbb{Z}$  is determined by  $\alpha(1) = f$ , and corresponding subgroup we choose is  $\text{Stab}(x)$ , i.e., the integer power  $k$  such that  $f^k(x) = x$ . If the orbit only contains one element, then any  $f^k$  has the property that  $f^k(x) = x$ , so  $\text{Stab}(x) = \mathbb{Z}$ . Similarly, if orbits contain 2 elements, then  $f^{2k}(x) = x$ , so all even powers work. If orbit is an infinite chain, then any  $f^k$  for  $k \neq 0$  will not become  $\text{id}_X$ , so only  $\{0\}$  works.

**Exercise 3.61.** Recall: a group  $G$  is cyclic if  $G = \langle g \rangle$  for some  $g \in G$ , i.e.,  $G$  is generated by a single element. Show that every subgroup is cyclic.

For this exercise, pick the least positive integer power of  $g$ , prove it generates the entire subgroup. Next, we talk about some important applications and corollaries of orbit-stabilizer.

1. Let  $H \leq G$ ,  $H \curvearrowright G$  by left multiplication:  $h \cdot g := hg$ . Take some  $g \in G$ , consider the diagram:

$$\begin{array}{ccccc}
 H & \xrightarrow{\quad} & H/\text{Stab}(g) & \xrightarrow{\cong} & H \cdot g \\
 & \searrow & & \swarrow & \\
 & & G & & 
 \end{array}$$

The orbit  $H \cdot g$  is the right-coset of  $H$  corresponding to  $g$ :  $Hg$ .  $\text{Stab}(g) = \{h \in H : hg = g\} = \{e\}$ , so we further have  $Hg \cong H/\text{Stab}(g) \cong H$ , i.e., every right-coset of  $H$  is in bijection with  $H$ .

**Theorem 3.62** (Lagrange). *If  $G$  is a finite group,  $H \leq G$ , then  $|G| = |H||G/H|$ , where we usually use  $|G : H|$  to denote  $|G/H|$ , called the index of  $H$  in  $G$ .*

*Proof.* By our above observation, each coset of  $H$  is in bijection with  $H$ , which means they all have cardinality  $|H|$ . Moreover, either left-coset or right-coset partitions  $G$ , and there are  $|G/H|$  or  $|HG|$  such cosets in total, so  $|G| = |H||G/H|$ .  $\square$

**Corollary 3.63.**  $|H| \mid |G|$ .

*Proof.* By 3.62,  $|G| = |H||G/H|$ , and  $|G/H|$  is a positive integer.  $\square$

For instance, if  $|G|$  is prime, then subgroups of  $G$  are either  $\{e\}$  or  $G$ .

**Exercise 3.64.** Show that the only group of size  $p$  a prime, up to isomorphism, is  $\mathbb{Z}_p$ .

One can show such group must be cyclic: suppose not, then you can construct another subgroup of size smaller than  $p$ , contradicts 3.62.

**Corollary 3.65.** *Let  $G$  be a finite group,  $g \in G$ .*

- (a)  $\{n \in \mathbb{N}^+ : g^n = e\} \neq \emptyset$
- (b) Let  $|g| := \min\{n \in \mathbb{N}^+ : g^n = e\}$ , called the order of  $g$ , then  $g^n = e$  if and only if  $|g| \mid n$ .
- (c)  $|g| \mid |G|$ , i.e.,  $g^{|G|} = e$ .

*Proof.* (a) Since  $G$  is finite, we cannot keep generating new elements by keep powering  $g$ , so there must exists some positive  $i, j \in \mathbb{N}^+$  with  $j > i$ , such that  $g^j = g^i \Rightarrow g^{j-i} = e$ .

(b)  $(\Leftarrow)$  : If  $|g| \mid n$ , then  $n = k|g|$  for some positive integer  $k$ , so  $g^n = g^{k|g|} = (g^{|g|})^k = e^k = e$ .  
 $(\Rightarrow)$  : Use division algorithm. Suppose  $|g| \nmid n$ , so  $n = k|g| + r$ , for some  $0 < r < |g|$ , so  $g^n = g^{k|g|+r} = g^{k|g|}g^r = eg^r = g^r = e$ , however,  $r < |g|$ , so contradicts the definition of order.

(c) Consider the subgroup  $\langle g \rangle$ , it has size  $|g|$ : every element in  $\langle g \rangle$  can be expressed as  $g^k$ , for  $0 \leq k < |g|$ . By 3.63,  $|g| \mid |G|$ , as desired.  $\square$

**Exercise 3.66.** Let  $p$  be a prime number, consider  $G = (\mathbb{Z}_p, \cdot)$ .

- (a) Show this is an abelian group.
- (b) Conclude that for every  $a \in \mathbb{Z}$ ,  $a^p = a \pmod p$ , this is *Fermat's little theorem*.

The first part is a little bit painstaking to show. The second part is just apply 3.65 to  $G$ .

2. Let  $\varphi : G \rightarrow H$  be a group homomorphism, it gives rise to an action  $\alpha_\varphi : G \curvearrowright H$ , given by  $(\alpha_\varphi(g))(h) := \varphi(g)(h)$ . Let  $e_H$  be the identity of  $H$ , the orbit of  $e_H$  is  $\text{im}(\varphi)$ , since  $G \cdot_\alpha e_H = \{\varphi(g) : g \in G\}$ .  $\text{Stab}(e_H) = \{g \in G : \varphi(g)(e_H) = e_H\} = \{g \in G : \varphi(g) = e_H\} = \text{preim}(\varphi(e_H))$ , we call it *kernel* of  $\varphi$ .

**Theorem 3.67** (First Isomorphism Theorem). *Let  $\varphi : G \rightarrow H$  be a group homomorphism, then  $\text{im}(\varphi) \cong G/\ker(\varphi)$ .*

*Proof.* Apply orbit-stabilizer, with element  $e_H$ , so  $\text{Stab}(e_H) = \ker(\varphi)$ , and  $G \cdot e_H = \text{im}(\varphi)$ .  $\square$

### 3.6 Normal subgroups and kernels

In this part we focus on normal subgroup and kernel of homomorphisms. Let  $\varphi : G \rightarrow H$  be a homomorphism, recall 3.67, combine with 3.56, we have the following diagram:

$$\begin{array}{ccccc} G & \twoheadrightarrow & G/\ker(\varphi) & \xrightarrow{\cong} & \text{im}(\varphi) \\ & \searrow \varphi & & \swarrow & \\ & & H & & \end{array}$$

In this diagram,  $\text{im}(\varphi)$  is a subgroup of  $H$ , by the isomorphism between  $G/\ker(\varphi)$  and  $\text{im}(\varphi)$ , we can “copy” the group structure and operation to  $G/\ker(\varphi)$ . This makes all the arrows in the diagram group homomorphisms. Let  $K := \ker(\varphi)$ , what is the group structure of  $G/K$ ? For each choice  $C_1, C_2 \in G/K$ , let's do the most natural thing. Let  $C_1 = g_1K, C_2 = g_2K$ , then define  $C_1C_2 := (g_1K)(g_2K) = (g_1g_2)K$ . So the group operation on  $G/K$  is denoted by  $(g_1K)(g_2K) = (g_1g_2)K$ .

**Theorem 3.68.** *Let  $K \leq G$ , then there is a group operation on  $G/K$  defined by  $(g_1K)(g_2K) = (g_1g_2)K$  if and only if  $K$  is a **normal** subgroup.*

*Proof.* ( $\Leftarrow$ ): Assume  $K$  is normal, we need to check that the group operation is well-defined, i.e., if  $g_1K = g'_1K, g_2K = g'_2K$ , then  $(g_1g_2)K = (g'_1g'_2)K$ . Since  $g_1K = g'_1K$ , we have  $g_1^{-1}g'_1K = K$ , so  $g_1^{-1}g'_1 \in K$ , similarly,  $g_2^{-1}g'_2 \in K$ , and  $g_1^{-1}g'_1g'_2g_2^{-1} \in K$ . Since  $K$  is normal,  $K = g_2Kg_2^{-1}$ , so  $g_1^{-1}g'_1g'_2g_2^{-1} \in g_2Kg_2^{-1} \Rightarrow g_2^{-1}g_1^{-1}g'_1g'_2 \in K$ , which means  $(g_1g_2)^{-1}(g'_1g'_2) \in K$ , therefore,  $(g_1g_2)^{-1}(g'_1g'_2)K = K \Rightarrow (g_1g_2)K = (g'_1g'_2)K$ , as desired.

( $\Rightarrow$ ): Suppose  $G/K$  is a group, we want to show that  $K \trianglelefteq G$ , this means for any  $g \in G, K = gKg^{-1}$ . Take  $g \in G$ .

( $\subseteq$ ): We can reuse some arguments in the converse part, i.e., suppose  $g_1K = g'_1K, g_2K = g'_2K$ , then  $(g_1g_2)K = (g'_1g'_2)K$ , this means that  $K = (g_1g_2)^{-1}(g'_1g'_2)K = g_2^{-1}g_1^{-1}g'_1g'_2K$ , so  $g_2^{-1}g_1^{-1}g'_1g'_2 \in K$ ,  $g_1^{-1}g'_1g'_2g_2^{-1} \in g_2Kg_2^{-1}$ . Moreover, if we have  $g_1^{-1}g'_1 \in K, g'_2g_2^{-1} \in K$ , then we show  $K \subseteq gKg^{-1}$ . Now, let's take  $g_2 = g$ , for any  $k \in K$ , we can write  $k$  as  $e^{-1}kgg^{-1}$ , clearly,  $e^{-1}k \in K, gg^{-1} = e \in K$ , so we have  $k \in gKg^{-1}$ .

( $\supseteq$ ): Since  $K \leq G, K \subseteq gKg^{-1}$ , we have  $Kg \subseteq gK \Rightarrow g^{-1}Kg \subseteq K$ . Set  $h = g^{-1}$ , so we have  $hKh^{-1} \subseteq K$ , as desired.  $\square$

We abstract the argument in  $\supseteq$  part into a Lemma:

**Lemma 3.69.** *If  $K \leq G$  satisfies  $K \subseteq gKg^{-1}$ , then  $K$  is normal.*

In fact, if  $\alpha : G \curvearrowright X$  and  $Y \subseteq X$  such that  $Y \subseteq g \cdot_\alpha Y$ , then  $g \cdot_\alpha Y = Y$ .

**Corollary 3.70.** *A subgroup  $K \leq G$  is a kernel of some homomorphism if and only if  $K$  is normal in  $G$ .*

*Proof.* ( $\Rightarrow$ ): Let  $K = \ker(\varphi)$  with  $\varphi : G \rightarrow H$ , by 3.67,  $G/K \cong \text{im}(\varphi)$  as group. By 3.68,  $K \trianglelefteq G$ . ( $\Leftarrow$ ): Suppose  $K$  is normal, by 3.68,  $G/K$  is a group and  $G \twoheadrightarrow G/K$ , the quotient map, is a homomorphism, we claim the kernel is  $K$ . What is the identity of  $G/K$ ? It is  $K$ , since  $(gK)(eK) = (ge)K = gK$ . Moreover, what elements  $g \in G$  satisfy  $gK = K$ ? Exactly the elements in  $K$ .  $\square$



Let  $\{*\}$  be an one-element trivial group, if  $K \trianglelefteq G$ , consider the following sequence:

$$\{*\} \longrightarrow K \hookrightarrow G \twoheadrightarrow G/K \longrightarrow \{*\}$$

In this sequence, the image of every homomorphism is equal to the kernel of next.

- $\text{im}(\{*\} \rightarrow K) = \{e_K\}$ ,  $\ker(K \hookrightarrow G) = \{e_K\}$
- $\text{im}(K \hookrightarrow G) = K$ ,  $\ker(G \twoheadrightarrow G/K) = K$

**Definition 3.71.** The sequence with above property is called *exact* sequence.

**Exercise 3.72.** Let  $K, G, H$  be groups, suppose we have a sequence of homomorphisms which is exact:

$$\{*\} \longrightarrow K \longrightarrow G \longrightarrow H \longrightarrow \{*\}$$

Show that  $K \cong K' \trianglelefteq G, H \cong G/K'$ .

**Exercise 3.73** (important). Suppose  $\varphi : G \rightarrow H$  is a homomorphism, then

1.  $\varphi$  is surjective  $\Leftrightarrow \text{im}(\varphi) = H$
2.  $\varphi$  is injective  $\Leftrightarrow \ker(\varphi) = \{e_G\}$

Both parts are not hard to show, but the result is very useful.

**Definition 3.74.** A group  $G$  is *simple* if the only normal subgroups of  $G$  are  $G$  and  $\{e\}$ .

**Exercise 3.75.**  $(\mathbb{Z}_n, +_n)$  is simple if and only if  $n$  is prime.

Notice  $(\mathbb{Z}_n, +_n)$  is abelian, so every subgroup is normal. If  $n$  is not prime, then it has subgroups other than  $G$  and  $\{e\}$ , so it's not simple.

### 3.7 Groups and counting

In this section, we use structure of groups to facilitate counting, especially, we study the famous necklace problem.

**Lemma 3.76** (Burnside). *Let  $\alpha : G \curvearrowright X$  be an action of a finite group  $G$ , on a finite set  $X$ . Then*

$$\underbrace{|X/E_\alpha|}_{\text{number of orbits}} = \frac{1}{|G|} \sum_{g \in G} \underbrace{|\{x \in X : g \cdot x = x\}|}_{\text{points fixed by } g}$$

Before proving lemma, let's first look at an example.

**Example 3.77.** Suppose  $\alpha : G \curvearrowright X$  is an action such that for any  $x \in X$ ,  $\text{Stab}(x) = \{e\}$ , such actions are called *free*. By orbit-stabilizer, every orbit is isomorphic to  $G/\text{Stab}(x) \cong G$ , so every orbit has size  $|G|$ , there are  $\frac{|X|}{|G|}$  orbits in total. For each  $g \in G$ ,  $|\{x \in X : g \cdot x = x\}| = \begin{cases} 0, & \text{if } g \neq e \\ |X|, & \text{if } g = e \end{cases}$ , so RHS is also  $\frac{|X|}{|G|}$ .

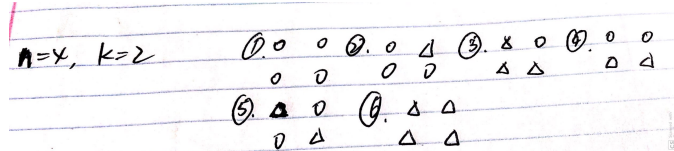
*Proof.* Let's do some calculations.

$$\begin{aligned} |X/E_\alpha| &= \sum_{O \in X/E_\alpha} 1 \\ &= \sum_{O \in X/E_\alpha} \sum_{x \in O} \frac{1}{|O|} \\ &= \sum_{x \in X} \frac{1}{|G \cdot x|} \quad \text{orbits partition } X \end{aligned}$$

By orbit-stabilizer,  $G \cdot x \cong G/\text{Stab}(x)$ , so  $|G \cdot x| = |G/\text{Stab}(x)| = |G|/|\text{Stab}(x)|$ , where the last equality is due to 3.62, so we can write  $|X/E_\alpha|$  as:

$$\begin{aligned} |X/E_\alpha| &= \sum_{x \in X} \frac{1}{|G \cdot x|} \\ &= \sum_{x \in X} \frac{|\text{Stab}(x)|}{|G|} \\ &= \frac{1}{|G|} \sum_{x \in X} |\text{Stab}(x)| \\ &= \frac{1}{|G|} \sum_{x \in X} \sum_{g \in G} \delta(g \cdot x = x) \quad \delta(\cdot) \text{ is the indicator function} \\ &= \frac{1}{|G|} \sum_{g \in G} \sum_{x \in X} \delta(g \cdot x = x) \\ &= \frac{1}{|G|} \sum_{g \in G} |\{x \in X : g \cdot x = x\}| \quad \square \end{aligned}$$

**Example 3.78.** How many different types of necklaces with  $n$  gems of  $k$  kinds are there, if the necklaces are the same up to rotation? Let's first look at  $n = 4, k = 2$ :



Let  $G$  : all rotations,  $X$  :  $k^n$  configurations of necklaces, so the problem reduces to count the number of orbits of the action  $G \curvearrowright X$  by rotating one configuration.

In this setting,  $|G| = n$ : we can rotate one configuration clockwise up to  $n - 1$  steps.  $|X| = k^n$ , so in general, number of orbits =  $\frac{1}{n} \sum_{s \in \mathbb{Z}_n} |\{x \in X : s \cdot x = x\}|$ . Let's examine our  $n = 4, k = 2$  case.

- For  $s = 0$ , all  $2^4 = 16$  configurations are fixed.
- For  $s = 1$ , only 2 configurations, namely, all squares or all triangles are fix points.
- For  $s = 2$ , diagonals must be the same, so 4 configurations.
- For  $s = 3$ , only 2 configurations.

By 3.76, the count is  $\frac{1}{4} (16 + 2 + 4 + 2) = 6$ .

**Exercise 3.79.** Show that  $|\{x \in X : s \cdot x = x\}| = k^{\gcd(n,s)}$ .

**Exercise 3.80.** What is the count, if you can flip the necklace?

For the second exercise, choose  $G = D_{2n}$ .

**Corollary 3.81** (Polya). *Let  $G$  be a finite group,  $X, Y$  finite sets, and  $\alpha : G \curvearrowright X$  be an action. For each  $g \in G$ , let  $c(g)$  be the number of cycles in the permutation  $\alpha(g)$  on  $X$ , i.e., the number of orbits in the action  $\mathbb{Z} \curvearrowright X : 1 \mapsto \alpha(g)$ . The action  $\alpha$  gives rises to an action  $G \curvearrowright Y^X$  by  $(g \cdot f)(x) := f(g^{-1} \cdot x)$ , i.e., the shift action. Then the number of orbits of this action is equal to  $\frac{1}{|G|} \sum_{g \in G} |Y|^{c(g)}$ .*

*Proof.*

$$\begin{aligned}
 \text{number of orbits} &= \frac{1}{|G|} \sum_{g \in G} |\{f \in Y^X : g \cdot f = f\}| \\
 &= \frac{1}{|G|} \sum_{g \in G} |\{f \in Y^X : f(x) = f(g^{-1} \cdot x), \forall x \in X\}| \quad \text{this means } f \text{ is constant on cycles in } \alpha(g) \\
 &= \frac{1}{|G|} \sum_{g \in G} |Y|^{c(g)} \quad \square
 \end{aligned}$$

## 4 Category

Category is a more abstract definition of “collections” of objects. Category is useful because *the same definition* can work in several categories.

### 4.1 Basic definitions & examples

**Definition 4.1.** A *category*  $\mathbb{C}$  consists of

- a class  $\text{Obj}(\mathbb{C})$  of *objects*
- for all  $A, B \in \text{Obj}(\mathbb{C})$ , a set  $\text{Hom}_{\mathbb{C}}(A, B)$ , or simply  $\text{Hom}(A, B)$  of *morphisms* from  $A$  to  $B$
- for all  $A, B, C \in \text{Obj}(\mathbb{C})$ , a function  $\circ : \text{Hom}(B, C) \times \text{Hom}(A, B) \rightarrow \text{Hom}(A, C)$ , called *composition*, such that:
  1. composition is associative: Let  $A, B, C, D \in \text{Obj}(\mathbb{C})$ ,  $f \in \text{Hom}(A, B)$ ,  $g \in \text{Hom}(B, C)$ ,  $h \in \text{Hom}(C, D)$ , then

$$h \circ (g \circ f) = (h \circ g) \circ f$$

2. identities: For each  $A \in \text{Obj}(\mathbb{C})$ , there is a  $1_A \in \text{Hom}(A, A)$ , such that for all  $B \in \text{Obj}(\mathbb{C})$ ,  $f \in \text{Hom}(A, B)$ ,  $g \in \text{Hom}(B, A)$ :

$$f \circ 1_A = f, 1_A \circ g = g$$

Notice for fixed  $A$ ,  $1_A$  is unique: duplicate the argument that proves identity of a binary operation is unique.

**Example 4.2.** 1. The most basic example is the category Set of sets:

- $\text{Obj}(\underline{\text{Set}}) = \text{all sets}$
- $\text{Hom}_{\underline{\text{Set}}}(A, B) = \text{functions from } A \text{ to } B$
- $\circ = \text{composition of functions}$

2. One can obtain different categories by taking fewer morphisms:

- (a)
  - $\text{Obj} = \text{all sets}$
  - $\text{Hom}(A, B) = \text{bijections from } A \text{ to } B$
  - $\circ = \text{composition}$
- (b)
  - $\text{Obj} = \text{all sets}$
  - $\text{Hom}(A, B) = \begin{cases} \emptyset, & \text{if } A \not\subseteq B \\ \{\text{the inclusion map } A \hookrightarrow B\} & \text{if } A \subseteq B \end{cases}$
  - $\circ = \text{composition}$

3.  $\text{Obj} = \mathbb{Z}, \text{Hom}(n, m) = \begin{cases} \emptyset, & \text{if } n > m \\ \text{one element set } \{f_{nm}\}, & \text{if } n \leq m \end{cases}$

For composition, we need  $\circ : \text{Hom}(n, m) \times \text{Hom}(k, n) \rightarrow \text{Hom}(k, m)$ .

- If  $k \leq n \leq m$ ,  $f_{nm} \circ f_{kn} := f_{km}$ .

- Otherwise, there's nothing to define: simply  $\emptyset$ .
4. The category of graphs, Graph:
- $\text{Obj}(\text{Graph}) = \{\text{all graphs}\}$
  - $\text{Hom}(G, H) = \{\text{all homomorphisms from } G \text{ to } H\}$ . Let's recall the definition of homomorphism of graphs: it is a function  $f : V(G) \rightarrow V(H)$  such that if  $\{x, y\} \in E(G)$ , then  $\{f(x), f(y)\} \in E(H)$ .
  - $\circ = \text{composition}$
5. The category of groups, Grp:
- $\text{Obj}(\text{Grp}) = \{\text{all groups}\}$
  - $\text{Hom}(G, H) = \{\text{all group homomorphisms from } G \text{ to } H\}$
  - $\circ = \text{composition}$

## 4.2 Monomorphism, epimorphism

In this section, we introduce some general concepts for different categories, which are useful in understanding more about groups.

**Definition 4.3.** Let  $\mathbb{C}$  be a category, and  $A, B \in \text{Obj}(\mathbb{C})$ .

- $f \in \text{Hom}(A, B)$  is a *monomorphism* if for all  $C \in \text{Obj}(\mathbb{C})$  and  $g, h \in \text{Hom}(C, A)$ ,

$$f \circ g = f \circ h \Rightarrow g = h$$

- Similarly,  $f$  is an *epimorphism* if for all  $C \in \text{Obj}(\mathbb{C})$  and  $g, h \in \text{Hom}(B, C)$ ,

$$g \circ f = h \circ f \Rightarrow g = h$$

In the category Set, it is not hard to show that

- monomorphism  $\Leftrightarrow$  injective
- epimorphism  $\Leftrightarrow$  surjective

What about in Grp? Clearly, injectivity implies monomorphism. What about monomorphism implies injectivity?

*Proof.* Suppose  $f : A \rightarrow B$  is a group homomorphism, take  $a, a' \in A$  with  $f(a) = f(a')$ . Then there are homomorphisms  $g, h : \mathbb{Z} \rightarrow A$  given by  $g(n) := a^n, h(n) := (a')^n$ . Let's verify  $f$  and  $g, h$  satisfy the monomorphism condition:

$$\begin{aligned} (f \circ g)(n) &= f(g(n)) \\ &= f(a^n) \\ &= f(a)^n && \text{since } f \text{ is a homomorphism} \\ &= f(a')^n \\ &= f((a')^n) \\ &= f(h(n)) \\ &= (f \circ h)(n) \end{aligned}$$

So  $f \circ g = f \circ h$ , combined with  $f$  is a monomorphism, we have  $g = h \Rightarrow g(1) = h(1) \Rightarrow a = a'$ , therefore,  $f$  is injective.  $\square$

So indeed, monomorphism in Grp  $\Leftrightarrow$  injective.

Note: in this proof, we have used the property of integers: for every group  $A$  and  $a \in A$ . there is a unique homomorphism:  $\mathbb{Z} \rightarrow A$  sending 1 to  $a$ .

What about epimorphisms? Surjectivity implies epimorphisms. How about the converse? In the category of Grp, the converse is true, however, it is a non-trivial task to show.

**Theorem 4.4** (Schreier). *If a group homomorphism  $\varphi : H \rightarrow G$  is an epimorphism in the category Grp, then  $\varphi$  is surjective.*

Notice it is not true in every category.

**Example 4.5.** Consider the category of subsets of  $\mathbb{R}^n$ ,  $n \in \mathbb{N}$ , with continuous functions as morphisms. The embedding  $\iota : \mathbb{Q} \hookrightarrow \mathbb{R}$  is, surprisingly an epimorphism. Given  $g, h : \mathbb{R} \rightarrow \mathbb{R}^n$  as continuous functions, if  $g \circ \iota = h \circ \iota$ , since  $\mathbb{Q}$  is dense in  $\mathbb{R}$ , so a continuous function on  $\mathbb{R}$  is determined by its values on rational points. Therefore,  $g = h$ , and  $\iota$  is an epimorphism. But clearly,  $\iota$  is not surjective.

*Proof of Schreier.* We can first decompose  $\varphi$  into the following diagram:

$$\begin{array}{ccc} H & \xrightarrow{\quad} & \text{im}(\varphi) \\ & \searrow \varphi & \downarrow \iota \\ & & G \end{array}$$

The claim is, if  $\varphi$  is an epimorphism, then so is  $\iota$ . Let  $g, h : G \rightarrow K$  be group homomorphisms, if  $g \circ \iota = h \circ \iota$ , then  $g \circ \varphi = h \circ \varphi$ : for any  $h \in H$ , let  $t = \varphi(h)$ , since so  $g \circ \iota(t) = h \circ \iota(t) \Rightarrow g \circ \iota \circ \varphi(h) = h \circ \iota \circ \varphi(h) \Rightarrow g \circ \varphi = h \circ \varphi$ . So  $g = h$  since  $\varphi$  is an epimorphism. Therefore, it suffices to consider the case where  $H \leq G$ , and  $\varphi : H \hookrightarrow G$  is the inclusion map. Since  $\varphi$  is the inclusion map,  $\varphi$  is surjective if and only if  $H = G$ , and we will show this.

**Lemma 4.6.** *If  $H$  is normal in  $G$ , then  $H = G$ .*

*Proof of Lemma.* Consider the two homomorphisms from  $G$  to  $G/H$ :

- the quotient homomorphism  $q : G \twoheadrightarrow G/H$
- the trivial homomorphism  $t : G \rightarrow G/H : g \mapsto H$

The claim is  $q \circ \varphi = t \circ \varphi$ , since for all  $h \in H$ , we have  $(q \circ \varphi)(h) = q(h) = H$ , and  $(t \circ \varphi)(h) = t(h) = H$ . Since  $\varphi$  is an epimorphism, we have  $q = t$ , i.e., the quotient map is nothing but the trivial map, this means  $G/H = \{H\}$ , i.e.,  $G = H$ , as desired.  $\square$

**Corollary 4.7.** *In such scenario, we can assume  $|G/H| \geq 3$ .*

*Proof of Corollary.* If  $|G/H| = 1$ , then  $G = H$ . Otherwise, if  $|G/H| = 2$ , then there are exactly two cosets:  $H$  and  $gH$ , for some  $g \in G$ . Suppose  $H$  is not normal, i.e., there is some  $a \in G$  such that  $aHa^{-1} \neq H$ , which means there is some  $h \in H$ , with  $aha^{-1} \notin H$ . Clearly,  $a \notin H$ , so we can write  $a = g\ell$ , for some  $\ell \in H$ , and  $aha^{-1} \notin H$  implies that  $aha^{-1} = gh'$ , for some  $h' \in H$ . Multiply both sides by  $g^{-1}$ , we get  $g^{-1}aha^{-1} = h' \Rightarrow g^{-1}g\ell h\ell^{-1}g^{-1} = h' \Rightarrow \ell h\ell^{-1}g^{-1} = h'$ , since  $\ell, h, h' \in H$ , it must be the case that  $g^{-1} \in H \Rightarrow g \in H$ , contradicts that  $gH$  and  $H$  partitions  $G$ . Thus,  $H$  must be normal.  $\square$

Towards a contradiction, let's assume  $H \neq G$ , so  $H$  cannot be normal, by above corollary, it's safe to say  $|G/H| \geq 3$ . We will show that in this case, it's possible to construct two homomorphisms  $\alpha, \beta : G \rightarrow \text{Sym}(G)$ , such that  $\alpha \circ \varphi = \beta \circ \varphi$ , but  $\alpha \neq \beta$ , which contradicts  $\varphi$  is an epimorphism. Define  $\alpha =$  left multiplication action, and  $\beta = \alpha$  conjugated by “swapping” two of cosets of  $H$ . More specifically, since  $|G/H| \geq 3$ , there are two elements  $u, v \in G$  such that  $H, Hu, Hv$  are all distinct. Let  $\pi : G \rightarrow G$  be the bijection such that

$$\pi(g) := \begin{cases} hv, & \text{if } g = hu \text{ for some } h \in H \\ hu, & \text{if } g = hv \text{ for some } h \in H \\ g, & \text{if } g \notin H_u \cup H_v \end{cases}$$

Define an action  $\beta : G \curvearrowright G$  by  $\beta(g) := \pi \circ \alpha(g) \circ \pi^{-1} = \pi \circ \alpha(g) \circ \pi$ . We need to check  $\alpha, \beta$  agree on  $H$ . Take  $h, h' \in H$ , then

- $\alpha(h)(h') = hh', \beta(h)(h') = \pi \circ \alpha(h) \circ \pi(h') = \pi \circ \alpha(h)(h') = \pi(hh') = hh'$
- $\alpha(h)(h'u) = hh'u, \beta(h)(h'u) = \pi \circ \alpha(h) \circ \pi(h'u) = \pi \circ \alpha(h)(h'u) = \pi(hh'u) = hh'u$
- $\alpha(h)(h'v) = hh'v, \beta(h)(h'v) = \pi \circ \alpha(h) \circ \pi(h'v) = \pi \circ \alpha(h)(h'u) = \pi(hh'u) = hh'v$

Thus,  $\alpha|_H = \beta|_H \Rightarrow \alpha \circ \varphi = \beta \circ \varphi$ , but  $\alpha \neq \beta$ , in particular,  $\alpha(u) \neq \beta(u) : \alpha(u)(e) = u, \beta(u)(e) = v$ . This completes the contradiction, and thus completes the proof of the theorem.  $\square$



## 5 Advanced topics on Groups

In this section, we study more advanced topics on groups, including products & coproducts, free groups, and Sylow groups.

### 5.1 Product & coproduct of groups

Before studying products & coproducts of groups, let's first recall them on Sets. It is best to illustrate the definitions of products & coproducts with diagrams. The first is what we need for product of sets:

$$\begin{array}{ccc}
 X \times Y & \xrightarrow{p} & X \\
 \downarrow q & \nwarrow \exists! h & \uparrow f \\
 Y & \xleftarrow{g} & A
 \end{array}$$

The second one is what we need for coproduct of sets, and coproduct is sometimes called *disjoint union*:

$$\begin{array}{ccc}
 X \sqcup Y & \xleftarrow{i} & X \\
 \uparrow j & \searrow \exists! h & \downarrow f \\
 Y & \xrightarrow{g} & A
 \end{array}$$

In Grp: Given groups  $G, H$ , we want a group  $G \times H$  and homomorphisms  $p : G \times H \rightarrow G, q : G \times H \rightarrow H$ , such that

$$\begin{array}{ccc}
 G \times H & \xrightarrow{p} & G \\
 \downarrow q & \nwarrow \exists! \xi & \uparrow \varphi \\
 H & \xleftarrow{\psi} & F
 \end{array}$$

As a set,  $G \times H$  is just the Cartesian product of  $G$  and  $H$ , where operations are defined as  $(g_1, h_1) \cdot (g_2, h_2) := (g_1 g_2, h_1 h_2)$ , i.e., pointwise multiplication. Define homomorphisms  $p, q$  as  $p(g, h) = g, q(g, h) = h$ . Given homomorphisms  $\varphi : F \rightarrow G, \psi : F \rightarrow H$ , there exists a unique  $\xi : F \rightarrow G \times H$ , such that  $p \circ \xi = \varphi, q \circ \xi = \psi$ , by  $\xi(f) = (\varphi(f), \psi(f))$ .

**Definition 5.1.**  $G \times H$  is called *direct product* of  $G$  and  $H$ .

**Example 5.2.** 1.  $G \times \text{trivial group} \cong G$

2.  $\mathbb{Z} \times \mathbb{Z} = \mathbb{Z}^2$

3.  $\mathbb{Z}_3 \times \mathbb{Z}_7 \cong \mathbb{Z}_{21}$

**Exercise 5.3.** Show that if  $n, m \geq 2, \gcd(m, n) = 1$ , then  $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$ .

However, if  $\gcd(m, n) \neq 1$ , we cannot say anything about  $\mathbb{Z}_n \times \mathbb{Z}_m$ : for example,  $\mathbb{Z}_2 \times \mathbb{Z}_2 \not\cong \mathbb{Z}_4$ , since  $\mathbb{Z}_4$  is cyclic but the former is not.

Now let's switch the gear to look at coproducts. In Grp, what we want is:

$$\begin{array}{ccc}
 G * H & \xleftarrow{i} & G \\
 \uparrow j & \searrow \exists! \xi & \downarrow \varphi \\
 H & \xrightarrow{\psi} & F
 \end{array}$$

Recall that in Sets: 2.8, we have shown that if  $\text{im}(i) \cap \text{im}(j) = \emptyset$ , then we can simply take the union of  $G$  and  $H$ . However,  $\text{im}(i) \cap \text{im}(j) \neq \emptyset$ , since  $i(e_G) = j(e_H)$ . The question is, is there any group  $K$  such that there are homomorphisms  $i : G \rightarrow K, j : H \rightarrow K$ ,  $i, j$  are injective, and  $\text{im}(i) \cap \text{im}(j) = \{e_K\}$ ? Consider  $K = G \times H$ , and  $i : g \mapsto (g, e_H), j : h \mapsto (e_G, h)$ .

**Proposition 5.4.** *In the category Ab, a.k.a. abelian groups,  $G \times H$  is the coproduct of  $G$  and  $H$ .*

*Proof.* Take abelian group  $F$  with homomorphisms  $\varphi : G \rightarrow F, \psi : H \rightarrow F$ , we want to show there exists a unique  $\xi : G \times H \rightarrow F$  such that the diagram holds. Simply define  $\xi(g, h) := \varphi(g) + \psi(h)$ , this is a homomorphism, since

$$\begin{aligned}
 \xi((g_1, h_1) + (g_2, h_2)) &= \xi(g_1 + g_2, h_1 + h_2) \\
 &= \varphi(g_1 + g_2) + \psi(h_1 + h_2) \\
 &= \varphi(g_1) + \varphi(g_2) + \psi(h_1) + \psi(h_2) \\
 &= \varphi(g_1) + \psi(h_1) + \varphi(g_2) + \psi(h_2) \\
 &= \xi(g_1, h_1) + \xi(g_2, h_2)
 \end{aligned}$$

We leave uniqueness part as an exercise to the reader. □

So in abelian groups, we call coproduct *direct sums*.  
What about Grp? We need to introduce the notion of *free groups*.

## 5.2 Free groups

What is free groups? We use a diagram to introduce the idea. Let  $X$  be a set and  $G$  be a group, then free group  $\mathbb{F}_X$  is the group that satisfies the following diagram:

$$\begin{array}{ccc} X & \xrightarrow{\quad} & \mathbb{F}_X \\ & \searrow f & \downarrow \exists! \varphi \\ & & G \end{array}$$

Let's first do the easy case, say  $X = \{x\}$ , then we claim  $\mathbb{F}_X \cong \mathbb{Z}$ , and  $\varphi : \mathbb{Z} \rightarrow G : n \mapsto (f(x))^n$ , and for the map from  $\{x\}$  to  $\mathbb{F}_X$ , we simply map  $x$  to 1. Given such setting,  $\varphi$  is clearly unique, and is also a homomorphism.

What if  $X = \{x, y\}$ , in such scenario, what should  $\mathbb{F}_{\{x,y\}}$  look like? To address this problem, we need to introduce the concept of *reduced words*.

**Definition 5.5.** Let  $X$  be a set (generators), define

$$X' = \{x' : x \in X \text{ is associated with } x', \text{ serve as } \textit{inverse}\}$$

The *words* over  $X \cup X'$  is simply  $(X \cup X')^*$ , where  $A^*$  is the *kleene star*, i.e., all words over alphabet  $A$  with finite length. The *reduced words* is a subset of words over  $X \cup X'$ , with no  $x$  and  $x'$  adjacent to each other.

**Definition 5.6.** The *free group* over a set  $X$ , denoted by  $\mathbb{F}_X$  is defined as {all reduced words over  $X \cup X'$ }. The group operation is concatenation+reduction, i.e., for two reduced words  $w_1, w_2$ , we first concatenate them, then cancel out all adjacent  $x$  and  $x'$ .

**Exercise 5.7.** Show that such operation is associative. In other words, the result of reducing a word is independent of orders of reductions.

For simplicity, we write  $x^{-1}$  for  $x'$ .

Whenever  $G$  is a group,  $f : X \rightarrow G$ , then there exists a unique homomorphism  $\varphi : \mathbb{F}_X \rightarrow G$  that completes the diagram in 5.2: let  $w = x_1 x_2 \dots x_n$  be a reduced word, define  $\varphi(w) = f(x_1) f(x_2) \dots f(x_n)$ , and define  $f(x^{-1}) := (f(x))^{-1}$ .

What is the coproduct  $\mathbb{Z} * \mathbb{Z}$ ?

$$\begin{array}{ccc} \mathbb{Z} * \mathbb{Z} \cong \mathbb{F}_{\{x,y\}} & \xleftarrow{1 \mapsto x} & \mathbb{Z} \\ \uparrow 1 \mapsto y & \searrow \exists! \xi & \downarrow 1 \mapsto a \\ \mathbb{Z} & \xrightarrow{1 \mapsto b} & G \end{array}$$

Since  $\varphi : \mathbb{Z} \rightarrow G, \psi : \mathbb{Z} \rightarrow G$ , we can abstract them as  $1 \mapsto a, 1 \mapsto b$ , so  $\xi$  is defined as  $\xi(x) = \varphi(1) = a, \xi(y) = \psi(1) = b$ .

**Example 5.8.** Consider the dihedral group,  $D_{2n} = \langle g, h \rangle$ , where  $g^n = e, h^2 = e, hghg = e$ .

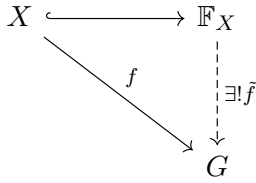
**Proposition 5.9.** Suppose  $G$  is a group,  $x, y \in G$  such that  $x^n = y^2 = yxyx = e$ , then there exists a unique homomorphism:  $\varphi : D_{2n} \rightarrow G$ , such that  $\varphi(g) = x, \varphi(h) = y$ .

*Proof.* Since  $D_{2n}$  is generated by  $g, h$ , every element of  $D_{2n}$  is of the form  $g^{m_1}h^{\ell_1} \dots g^{m_k}h^{\ell_k}$ , where  $m_i, \ell_i \in \mathbb{Z}$ . Then  $\varphi(g^{m_1}h^{\ell_1} \dots g^{m_k}h^{\ell_k}) = x^{m_1}y^{\ell_1} \dots x^{m_k}y^{\ell_k}$ , this proves uniqueness. We need to show  $\varphi$  is in fact a function, and it suffices to check if  $g^{m_1}h^{\ell_1} \dots g^{m_k}h^{\ell_k} = e_{D_{2n}}$ , then  $x^{m_1}y^{\ell_1} \dots x^{m_k}y^{\ell_k} = e_G$ . We proceed by cleaning up the exponents.

1. Get rid of negative powers of  $g$  by  $g^{n-1} = g^{-1}, x^{n-1} = x^{-1}$
2. Get rid of negative powers of  $h$  by  $h^{-1} = h, y^{-1} = y$
3.  $hghg = e \Rightarrow ghg = h \Rightarrow hg = g^{n-1}h, yx = x^{n-1}y$ , so we can move all  $g$  in front of  $h$ , and all  $x$  in front of  $y$

This results in a form of  $g^m h^\ell$ , where  $0 \leq m < n, 0 \leq \ell \leq 1$ , and we have  $x^m y^\ell$  as well, since  $g^m h^\ell = e_{D_{2n}}$ , we must have  $m = \ell = 0 \Rightarrow x^0 y^0 = e_G$ , as desired.  $\square$

If  $w = x_1 \dots x_n$  is a word, let  $\tilde{f}(w) := f(x_1) \dots f(x_n)$ , so our diagram becomes:



**Definition 5.10.** Let  $R$  be a set of reduced words over  $X$ , i.e.,  $R \subseteq \mathbb{F}_X$ , call the elements of  $R$  *relations*. Given a group  $G$  and  $f : X \rightarrow G$ , say  $(G, f)$  *satisfies*  $R$  if  $\tilde{f}(w) = e_G$ , for all  $w \in R$ .

**Example 5.11.** Let  $X = \{x, y\}, G = D_{2n}, f : X \rightarrow D_{2n} : (x \mapsto g, y \mapsto h)$ , then  $(D_{2n}, f)$  satisfies  $\{x^n, y^2, xyxy\}$ .

Note that, if  $(G, f)$  satisfies  $R$  and  $\varphi : G \rightarrow H$  is a homomorphism, then  $(H, \varphi \circ f)$  also satisfies  $R$ , since  $\widetilde{\varphi \circ f}(w) = \varphi(\tilde{f}(w)) = \varphi(e_G) = e_H$ .

**Definition 5.12.** Let  $G$  be a group,  $X$  be a set,  $f : X \rightarrow G, R \subseteq \mathbb{F}_X$ , we write  $(G, f) \cong \langle X \mid R \rangle$ , if

1.  $(G, f)$  satisfies  $R$ .
2. If there exists other  $(H, g)$  satisfies  $R$ , then there exists a unique homomorphism  $\varphi : G \rightarrow H$ , such that  $g = \varphi \circ f$ .

We call  $\langle X \mid R \rangle$  a *presentation* of  $G$ .

**Exercise 5.13.** If  $(G, f), (H, g) \cong \langle X \mid R \rangle$ , show that there exists a unique isomorphism  $\varphi : G \rightarrow H$ , such that  $g = \varphi \circ f$ .

As a hint, use the homomorphism given by definition of  $(G, f) \cong \langle X \mid R \rangle$ , and show the homomorphism given by  $(H, g) \cong \langle X \mid R \rangle$  is its inverse.

**Example 5.14.** 1.  $\mathbb{F}_X \cong \langle X \mid \emptyset \rangle = \langle X \mid \rangle$

2.  $\langle \{x\} \mid \{x^n\} \rangle = \langle x \mid x^n \rangle \cong \mathbb{Z}_n$

**Exercise 5.15.** If  $(G, f) \cong \langle X \mid R \rangle$ , then  $G = \langle \{f(x) : x \in X\} \rangle$ .

3. As a shorthand notation, below we will write  $G \cong \langle X \mid R \rangle$  to denote that there exists  $f : X \rightarrow G$  such that  $(G, f) \cong \langle X \mid R \rangle$ . With this notation, we have  $D_{2n} \cong \langle x, y \mid x^n, y^2, xyxy \rangle$ .
4. Free abelian group over  $X$ :  $\langle x \mid \{x^{-1}y^{-1}xy : x, y \in X\} \rangle$ .
5. Let  $G$  be an arbitrary group,  $X = G$ ,  $\text{id}_G : G \rightarrow G$ , then  $(G, \text{id}_G) \cong \langle G \mid R_G \rangle$ , where

$$R_G = \{ \text{all reduced words } w \in \mathbb{F}_G \text{ that are satisfied in } (G, \text{id}_G), \text{ i.e., } w = g_1 \dots g_n \text{ such that } g_1 \dots g_n = e_G \}$$

**Corollary 5.16.** *If  $G$  is finite, then  $G$  is finitely represented, i.e., it has a presentation with finitely many relations.*

*Proof.* Since  $G$  is finite, there are only finitely many elements that can be  $e_G$ , using  $G \cong \langle G \mid R_G \rangle$  gives us the desired result.  $\square$

**Theorem 5.17.** *Let  $X$  be a set,  $R \subseteq \mathbb{F}_X$ , then there exists a group  $G$  with a function  $f : X \rightarrow G$  such that  $(G, f) \cong \langle X \mid R \rangle$ .*

We need a Lemma/definition in order to prove this theorem.

**Lemma 5.18.** *Let  $G$  be a group,  $R \subseteq G$ , then define  $N(R) := \bigcap \{H \trianglelefteq G : R \subseteq H\}$ , it is a normal subgroup of  $G$ , called the normal closure of  $R$ .  $N(R)$  is the smallest normal subgroup of  $G$  containing  $R$ .*

*Proof.* Take  $g \in G$ , we want to show that  $N(R)$  is normal, i.e.,  $gN(R)g^{-1} = N(R)$ . Take  $h \in N(R)$ , then  $ghg^{-1} \in N(R)$ , since  $h$  is in every normal group that contains  $R$ . This proves  $gN(R)g^{-1} \subseteq N(R)$ . Recall in 3.69, we have shown that one side of containment suffices to show a group is normal. Thus,  $N(R)$  is normal, as desired.  $\square$

**Exercise 5.19.** Let  $G$  be a group,  $R \subseteq G$ , show that  $N(R) = \langle \{grg^{-1} : g \in G, r \in R\} \rangle$ .

**Lemma 5.20.** *Let  $G, H_1, H_2$  be groups,  $\varphi_1 : G \rightarrow H_1, \varphi_2 : G \rightarrow H_2$  be homomorphisms such that  $\text{im}(\varphi_1) = H_1$  and  $\ker(\varphi_1) \subseteq \ker(\varphi_2)$ , then there exists a unique homomorphism  $\psi : H_1 \rightarrow H_2$  such that  $\psi \circ \varphi_1 = \varphi_2$ .*

*Proof.* Let  $K_1 := \ker(\varphi_1), K_2 := \ker(\varphi_2)$ , by 3.67,  $\text{im}(\varphi_1) \cong G/K_1$ , since  $\text{im}(\varphi_1) = H_1$ , we can assume  $H_1 = G/K_1$ , so one can view  $\varphi_1$  as a homomorphism from  $G$  to  $G/K_1$ , i.e., the quotient map. Define  $\psi : G/K_1 \rightarrow H_2$  by  $\psi(gK_1) = \psi(\varphi_1(g)) = \varphi_2(g)$ , we need to check that  $\psi$  is well-defined, i.e., if  $gK_1 = g'K_1$ , then  $\varphi_2(g) = \varphi_2(g')$ . Notice that

$$\begin{aligned} gK_1 &= g'K_1 \\ \Rightarrow g^{-1}g'K_1 &= K_1 \\ \Rightarrow g^{-1}g' &\in K_1 \\ \Rightarrow g^{-1}g' &\in K_2 && \text{since } K_1 \subseteq K_2 \\ \Rightarrow \varphi_2(g^{-1}g') &= e_{H_2} \\ \Rightarrow \varphi_2(g) &= \varphi_2(g') \end{aligned}$$

Uniqueness is left as an exercise to the reader. This gives us the following diagram:

$$\begin{array}{ccc} G & \xrightarrow{\varphi_1} & H_1 \cong G/\ker(\varphi_1) \\ & \searrow \varphi_2 & \downarrow \exists! \psi \\ & & H_2 \end{array}$$

□

Now we are ready to prove the theorem.

*Proof of Theorem.* Take  $G := \mathbb{F}_X/N(R)$ , consider the following diagram:

$$\begin{array}{ccccc} X & \hookrightarrow & \mathbb{F}_X & \xrightarrow{p} & \mathbb{F}_X/N(R) \\ & \searrow f & \downarrow \tilde{f} & \swarrow \exists! \varphi & \\ & & H & & \end{array}$$

where  $(H, f)$  satisfies  $R$ . What we need to show is two things: 1).  $G$  satisfies  $R$ , and 2). there exists a unique homomorphism from  $G$  to  $H$ . For the first part, notice that  $R \subseteq N(R)$ , if we let  $\iota$  denote the embedding of  $X$  into  $\mathbb{F}_X$ , then  $p \circ \iota$  will satisfy  $R$ . For the second part, we apply 5.20 to  $\mathbb{F}_X - \mathbb{F}_X/N(R) - H$ , where we need to check that  $p$  is surjective, and  $\ker(p) \subseteq \ker(\tilde{f})$ . The first part is clear, since  $p$  is the quotient map, for the second part, notice  $\ker(p) = N(R)$ . By our assumption,  $(H, f)$  satisfies  $R$ , so  $R \subseteq \ker(\tilde{f})$ , and due to 3.70,  $\ker(\tilde{f})$  is normal, so  $N(R) \subseteq \ker(\tilde{f})$ . Thus, by 5.20, there exists a unique homomorphism  $\varphi : \mathbb{F}_X/N(R) \rightarrow H$ , as desired. □

**Example 5.21.** Coproducts of groups. Let  $G_1, G_2$  be groups, say  $G_1 \cong \langle X_1 \mid R_1 \rangle, G_2 \cong \langle X_2 \mid R_2 \rangle$ , assume  $X_1 \cap X_2 = \emptyset$ .

**Proposition 5.22.**  $\langle X_1 \cup X_2 \mid R_1 \cup R_2 \rangle = G_1 * G_2$  is a coproduct of  $G_1$  and  $G_2$ , it is also called the free product.

*Proof.* Consider the following diagram:

$$\begin{array}{ccccc} X_1 & \hookrightarrow & X_1 \cup X_2 & \hookleftarrow & X_2 \\ \downarrow & & \downarrow & & \downarrow \\ G_1 & \longrightarrow & G_1 * G_2 & \longleftarrow & G_2 \\ & \searrow & \downarrow \exists! & \swarrow & \\ & & H & & \end{array}$$

By 5.2,  $H$  both satisfies  $R_1$  and  $R_2$ , so there exists a unique homomorphism from  $G_1 * G_2$  to  $H$ . □

This has some interesting dynamics: consider  $\mathbb{Z}_2 * \mathbb{Z}_2$ , we can represent the first with  $\langle x \mid x^2 \rangle$  and the second with  $\langle y \mid y^2 \rangle$ , by 5.22, we have  $\mathbb{Z}_2 * \mathbb{Z}_2 = \langle x, y \mid x^2, y^2 \rangle$ , this is an infinite group: we can repeatedly form  $xy, xyxy, xyxyxy, \dots$ , i.e.,  $(xy)^*$ .

**Example 5.23.** Consider  $\langle x, y \mid x^n, y^2, x^{-1}y^{-1}x^2y \rangle$ , where the last relation can be interpreted as  $x^2y = yx$ , by this relation, we can swap all  $x$  in front of  $y$ , so every element can be written  $x^m y^\ell$ , for  $0 \leq m < n, 0 \leq \ell \leq 1$ . The size of this group is thus at most  $2n$ .

Let's do some more computations.

$$\begin{aligned} x &= y^2 x \\ &= y x^2 y \\ &= x^2 y x y \\ &= x^4 y^2 \\ &= x^4 \end{aligned}$$

So  $x^3 = e$ . If  $\gcd(n, 3) = 1$ , then  $x^n = x^3 = e \Rightarrow x = e$ , the group is then  $\{e, y\} \cong \mathbb{Z}_2$ .

**Exercise 5.24.** What if  $n$  is divisible by 3?

**Example 5.25.** A famous computational problem, the *word* problem: given a finite presentation  $\langle X \mid R \rangle$  and  $w \in \mathbb{F}_X$ , is  $w$  the identity in  $\langle X \mid R \rangle$ ? Though seems the problem is not so hard to solve, but it is in fact *undecidable*.

Let's try to understand more structures about free groups.

$\mathbb{F}_0$  is the trivial group,  $\mathbb{F}_1 \cong \mathbb{Z}$ ,  $\mathbb{F}_2 \cong 2d$  tree, we know that  $\mathbb{F}_1 \not\cong \mathbb{F}_2$ , since  $\mathbb{F}_1$  is abelian, but  $\mathbb{F}_2$  is not. One can prove  $\mathbb{F}_3 \not\cong \mathbb{F}_2$  via *abelianization* or some counting argument on homomorphisms, but it is not obvious. Moreover,  $\mathbb{F}_3$  is isomorphic to a subgroup of  $\mathbb{F}_3$ , making the structure even more mysterious. Even more, there exists an injective homomorphism from  $\mathbb{F}_\infty$  to  $\mathbb{F}_2$ . Still, something can be said as “general property” for free groups.

**Theorem 5.26** (Nelsen-Schreir). *Every subgroup of a free group is free.*

The type of argument we are gonna use is new to this course, it comes from a specific field called *geometric group theory*, one can view it as a general type of graphs, where multi-edges and self-loops are allowed, and for each edge, we think of it as two arcs with different orientations. We formally re-define the notion of graph we are gonna use.

**Definition 5.27.** A graph  $G$  consists of the followings:

- a set  $V$  of vertices
- a set  $E$  of edges
- a pair of functions,  $start, end : E \rightarrow V$
- a bijection  $flip : E \rightarrow E$ , such that

- $flip(flip(e)) = e$
- $start(flip(e)) = end(e)$
- $end(flip(e)) = start(e)$

**Definition 5.28.** For  $x, y \in V$ , an  $x$ - $y$  walk is a sequence of edges  $e_k e_{k-1} \dots e_2 e_1$  (possibly empty), where:

- $start(e_{i+1}) = end(e_i)$
- $start(e_1) = x, end(e_k) = y$

Given a graph  $G$ , we form a subset  $E^+ \subseteq E$  by picking an arbitrary edge from each pair  $\{e, flip(e)\}$ . Let  $E^- := E \setminus E^+$ .

For an  $xy$ -walk  $p$  and a  $yz$ -walk  $q$ , one can define an  $xz$ -walk  $qp$  by concatenating the sequences, this gives rise to a category:

- Objects are vertices
- Morphisms from  $x$  to  $y$ :  $xy$ -walks
- Composition: concatenation of walks

**Definition 5.29.** A walk  $e_k e_{k-1} \dots e_1$  is *reduced* if there is no  $i$  such that  $e_{i+1} = flip(e_i)$ .

For every  $xy$ -walk  $p$ , if  $p$  is *not* reduced, say there exists some  $i$  with  $e_{i+1} = flip(e_i)$ , then we can apply a reduction operation to  $p$ , by removing both  $e_i$  and  $e_{i+1}$  from the sequence. After finitely many reductions, we have a reduced walk, denoted by  $Red(p)$ . Define an operation on reduced walk  $p$  from  $x$  to  $y$ , reduced walk  $q$  from  $y$  to  $z$ , by  $qp := Red(concat(qp))$ .

**Proposition 5.30.** 1. *Reduced walk  $Red(p)$  does not depend on the order of reductions taken.*

2. *If  $p$  is a reduced  $xy$ -walk,  $q$  is a reduced  $yz$ -walk,  $r$  is a reduced  $zw$ -walk, then  $(rq)p = r(qp)$ .*

*Proof.* Consider the free group  $\mathbb{F}_{E^+}$ . Notice walks are directly relating to words over  $E^+ \cup E^-$ , and reduced walks are essentially a subset of reduced words. Concatenation with reduction of reduced walks coincides with multiplication in  $\mathbb{F}_{E^+}$ . By using the property of  $\mathbb{F}_{E^+}$ , we have completed the proof of the proposition.  $\square$

This gives rise to a new category:

- Objects are vertices
- Morphisms from  $x$  to  $y$ : reduced  $xy$ -walks
- Composition: free group multiplication

In this category, every morphism has an inverse: let  $p$  be a walk from  $x$  to  $y$ , then flip all edges along  $p$  gives  $p^{-1}$ , a walk from  $y$  to  $x$ .

For  $x \in V$ , let  $\pi(x, G)$  be the group of all reduced  $xx$ -walks. Notice  $\pi(x, G) \leq \mathbb{F}_{E^+}$ .

**Proposition 5.31.** *If  $G$  is connected, then  $\pi(x, G) \cong \pi(y, G)$ , for any  $x, y \in V$ . So we can write  $\pi(G)$  without mentioning any vertex, this group is called the fundamental group of  $G$ .*

*Proof.* Since  $G$  is connected, there exists a walk  $p$  from  $x$  to  $y$ . Define the isomorphism as follows: given an  $xx$ -walk  $q$ , maps it to  $pqp^{-1}$ , i.e., first travels from  $y$  to  $x$ , take an  $xx$ -walk, then travel back to  $y$ . To see this is a homomorphism, observe that  $pq_1q_2p^{-1} = pq_1p^{-1}pq_2p^{-1}$ , and the inverse of this mapping is, given a  $yy$ -walk  $o$ , map it to  $p^{-1}op$ .  $\square$

**Theorem 5.32.** *Let  $X$  be a set,  $\mathbb{F}_X$  be the free group on  $X$ , and  $H \leq \mathbb{F}_X$ , then  $H = \pi(G)$  for some graph  $G$ .*



*Proof.* Look at  $\mathbb{F}_X/H$ . Let  $\alpha : \mathbb{F}_X \curvearrowright \mathbb{F}_X/H$  be the left multiplication action. Define a graph  $G$  as follows:  $V = \mathbb{F}_X/H$ ,  $E = \{(C, x) : C \in \mathbb{F}_X/H, x \in X\}$ , i.e., vertices are cosets of  $\mathbb{F}_X/H$ , and edges compromise two bits of information: the start of the edge,  $C$ , and the end point  $xC$ . So  $flip(C, x) = (xC, x^{-1})$ ,  $flip(C, x^{-1}) = (x^{-1}C, x)$ ,  $start(C, x) = C$ ,  $end(C, x) = xC$ . Now our goal is to show  $\pi(G) \cong H$ . First,  $\pi(G) \cong \pi(H, G)$ , what are elements of  $\pi(H, G)$ ? That's all reduced  $HH$ -walks, i.e., sequences  $(C_k, x_k) \dots (C_2, x_2)(C_1, x_1)$ , where  $x_1, \dots, x_k \in X \cup X^{-1}$ ,  $C_1 = C_k = H$ , and  $C_{i+1} = x_i C_i$ , so we can write the sequence as  $x_k x_{k-1} \dots x_2 x_1 H = H \Rightarrow x_k \dots x_2 x_1 \in H$ , a.k.a., each reduced word corresponds to exactly one reduced-walk in  $\pi(G, H)$ . This completes the proof.  $\square$

**Definition 5.33.** Let  $G$  be a graph,  $e = \{u, v\}$  be an edge, the *edge contraction of  $e$*  is the operation that removes  $e$  from  $E$ , and make one super vertex  $w$ , connects all neighbors of  $u$  and  $v$  to  $w$ . Notice edge contraction might yield a graph with self-loops, if the original graph admits multi-edges. We use  $G/e$  as a notation for  $G$  contracts edge  $e$ .

**Proposition 5.34.** *If  $e \in E(G)$  and  $e$  is not a self-loop, then  $\pi(G) \cong \pi(G/e)$ .*

*Proof.* Let  $e = \{u, v\}$ , and let  $w$  be the super vertex of  $u$  and  $v$ , after contraction. We will show  $\pi(u, G) \cong \pi(w, G/e)$ . We classify  $uu$ -walks as follows:

Type 1 Walks that do not use edge  $e$ . For this kind of walk, we simply map it to the same sequence of edges in  $G/e$ , with all  $u$  and  $v$  substituted by  $w$ .

Type 2 Walks that use edge  $e$ . This means at some time of the walk, it takes edge  $e$  to go from  $u$  to  $v$ , since this is essentially a  $uu$ -walk, it then must take some walk  $p$  to go from  $v$  to  $u$ , so it is safe to simply remove all occurrences of edge  $e$  in the original walk, the result is still a  $w$ -walk, and it is not hard to see that this mapping is bijective.

Thus,  $\pi(u, G) \cong \pi(w, G/e)$ .  $\square$

**Definition 5.35.** A *spanning tree* in a connected graph  $G$  is a set  $T \subseteq E$  such that

1. for all  $e \in T$ ,  $flip(e) \in T$
2. for all  $x, y \in V$ , there is an  $xy$ -walk with edges in  $T$
3. there are no non-trivial reduced closed walks in  $T$ , i.e.,  $T$  does not contain cycles

**Proposition 5.36.** *If  $G$  is a connected graph, then  $G$  has a spanning tree.*

*Proof.* A simple procedure will work: keep adding edges that do not form a cycle, until all vertices have been covered.  $\square$

**Exercise 5.37.** If  $T \subseteq E$  is a spanning tree in  $G$ , then for all  $x, y \in V$ , there is a unique reduced  $xy$ -walk in  $T$ .

*Proof.* Suppose it's not the case, i.e., there are at least two reduced  $xy$ -walk in  $T$ , then one can use the first walk to travel from  $x$  to  $y$ , and use the second to travel back from  $y$  to  $x$ : this is doable since by definition of spanning tree, both  $e$  and  $flip(e)$  are in  $T$ . This gives us a non-trivial closed walk, contradicts the definition of spanning tree.  $\square$

**Theorem 5.38.** *For every connected graph  $G$ ,  $\pi(G)$  is a free group.*

*Proof.* Pick a vertex  $x \in V$ , let  $T \subseteq E$  be a spanning tree in  $G$ . We claim that  $\pi(G) \cong \mathbb{F}_{E+\backslash T}$ , where we interpret  $flip(e)$  as  $e^{-1}$ . First of all, it is clear that  $\pi(x, G) \subseteq \mathbb{F}_{E+}$ , define an embedding

$\varphi : \mathbb{F}_{E+} \rightarrow \mathbb{F}_{E+\backslash T}$ , by  $e \mapsto \begin{cases} e, & \text{if } e \notin T \\ \text{id}, & \text{otherwise} \end{cases}$  The goal is to show  $\varphi|_{\pi(x, G)}$  is an isomorphism

from  $\pi(x, G)$  to  $\mathbb{F}_{E+\backslash T}$ , i.e., for every  $e_k \dots e_2 e_1 \in \mathbb{F}_{E+\backslash T}$ , there is a unique  $p \in \pi(x, G)$  such that  $\varphi(p) = e_k \dots e_1$ . Let's say we write  $p = p_k e_k p_{k-1} e_{k-1} \dots p_2 e_2 p_1 e_1 p_0$ , where  $p_0, p_1, \dots, p_k$  are walks using tree edges from  $T$ . Notice that  $p_0$  is a  $(x, start(e_1))$ -walk, for each  $1 \leq i < k$ ,  $p_i$  is a  $(end(e_i), start(e_{i+1}))$ -walk, and  $p_k$  is a  $(end(e_k), x)$ -walk. These are all walks using purely  $T$  edges, so by 5.37, these are all unique. This proves  $\varphi|_{\pi(x, G)}$  is a bijection, and therefore,  $\pi(G) \cong \mathbb{F}_{E+\backslash T}$ ,  $\pi(G)$  is a free group.  $\square$

With all these in hand, we are ready to prove 5.26.

*Proof of Nelsen-Schreier.* Let  $H \leq \mathbb{F}_X$ , then by 5.32,  $H \cong \pi(G)$  for some graph  $G$ , and by 5.38,  $\pi(G)$  is a free group, therefore,  $H$  is also a free group, as desired.  $\square$

### 5.3 Structure of finite groups

Groups, with a simple definition but complicated internal dynamics, so many people try to look at finite simple groups, and classify them based on certain criteria. In this section, we will try to do so.

**Theorem 5.39** (Cauchy). *If  $G$  is a finite group,  $p$  is a prime number such that  $p \mid |G|$ , then  $G$  has an element of order  $p$ .*

*Proof.* Consider the following set  $S := \{(a_1, a_2, \dots, a_p) \in G^p : a_1 a_2 \dots a_p = e\}$ . What is the cardinality of  $S$ ? The claim is  $|S| = |G|^{p-1}$ , the idea is we can freely pick  $p-1$  elements of the sequence, while the last element is fixed as  $(a_1 a_2 \dots a_{p-1})^{-1}$ . The sequence  $a_1 a_2 \dots a_p$  exhibits *rotational invariance*:  $a_1 a_2 \dots a_p = e \Rightarrow a_1^{-1} a_1 a_2 \dots a_p a_1 = a_1^{-1} a_1 = e \Rightarrow a_2 \dots a_p a_1 = e$ , so let's define an action  $\alpha : \mathbb{Z}_p \curvearrowright S$  by  $\alpha(1)(a_1, \dots, a_p) := (a_2, \dots, a_p, a_1)$ , and  $\alpha(m)(a_1, \dots, a_p) := (a_{m+1}, \dots, a_1, a_2, \dots, a_m)$ , i.e., shifts the sequence to the left by  $m$ . By orbit-stabilizer,  $\mathbb{Z}_p / \text{Stab}(s) \cong \mathbb{Z}_p \cdot s$ , since  $|\mathbb{Z}_p| = p$  and  $\text{Stab}(s) \leq \mathbb{Z}_p$ ,  $|\mathbb{Z}_p / \text{Stab}(s)|$  is either 1 or  $p$ , which also indicated every orbit of  $\alpha$  has size either 1 or  $p$ . Since orbits partition  $S$ , we can classify  $S$  into fixed points, i.e., elements with orbit size 1, let  $Z$  be the set of these points. Since  $(e, e, \dots, e) \in Z$ ,  $|Z| \geq 1$ . Moreover,  $|S| = |Z| + |S \setminus Z|$ , taking modulo  $p$ , we have  $|S| = |Z| \pmod{p}$ , since  $|S| = |G|^{p-1}$  and  $p \mid |G|$ ,  $|Z| = 0 \pmod{p}$ , so  $|Z| \geq p \geq 2$ . So let  $(a_1, \dots, a_p) \in Z \neq (e, e, \dots, e)$ , and by definition of fixed points,  $(a_1, a_2, \dots, a_p) = (a_2, a_3, \dots, a_p, a_1) \Rightarrow a_1 = a_2 = a_3 = \dots = a_p = a \neq e \Rightarrow a^p = e$ , as desired.  $\square$

**Exercise 5.40.** Let  $G$  be a finite group,  $p$  is a prime number such that  $p \mid |G|$ , then number of cyclic subgroups of  $G$ , of order  $p$ , equals  $1 \pmod{p}$ .

*Proof.* We make use of the fixed points set  $Z$  in 5.39. Since  $|Z| = 0 \pmod{p}$ , we can write  $|Z| = kp$  for some positive integer  $k$ , get rid of  $(e, e, \dots, e)$ , there are  $kp-1$  sequences remaining. For the same  $a$ , the sequence  $(a, a, \dots, a)$  is counted  $p-1$  times, so number of cyclic groups is essentially the number of unique sequence  $(a, a, \dots, a)$ , thus, the count is  $\frac{kp-1}{p-1} = 1 \pmod{p}$ .  $\square$

**Proposition 5.41.** *If  $G$  is a finite group,  $|G| = mp$  where  $p$  is a prime number and  $1 < m < p$ , then  $G$  is not simple.*

*Proof.* The claim is  $G$  has a normal subgroup of order  $p$ , suppose this is not the case, then  $G$  has  $\geq 2$  subgroups of order  $p$ , by 5.40, number of subgroups of order  $p$  is  $1 \pmod{p}$ , so the number must be  $\geq p+1$ . Note that if both  $H_1, H_2 \leq G$  with  $|H_1| = |H_2| = p$ ,  $H_1 \neq H_2 \Rightarrow H_1 \cap H_2 = \{e\}$ , so  $|G| \geq 1 + (p+1)(p-1) = p^2$ , contradicts  $|G| = mp < p^2$ .  $\square$

**Example 5.42.** Suppose we have a group  $G$  with  $|G| = 2019$ , notice  $2019 = 673 \times 3$ , and 673 is a prime, so there are no simple groups of order 2019.

**Theorem 5.43** (Sylow's First Theorem). *Let  $G$  be a finite group,  $p$  be a prime number, and  $k \in \mathbb{N}$ . If  $p^k \mid |G|$ , then  $G$  has a subgroup of order  $p^k$ .*

*Proof.* By induction on  $|G|$ . If  $k = 0$ , then it's trivial. Assume  $k \geq 1$ , in particular,  $p^k \mid |G|$ . If  $G$  has a subgroup  $H$  such that  $H \neq G$  and  $p^k \mid |H|$ , then by induction hypothesis, we are done.

Suppose  $G$  has no such subgroups, we claim that  $G$  has a normal subgroup of order  $p$ . We will make use of the *class formula* of  $G$ :

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

where  $Z(G)$  is the *center* of  $G$ , all elements in  $Z(G)$  can commute with any elements in  $G$ , and  $Z(a)$  is the *centralizer* of element  $a$ , which contains elements that can commute with  $a$ . Finally,  $A$  is a subset of  $G$  formed by picking an element from each non-trivial conjugacy class. To give a short proof of class formula, consider the conjugation action  $\alpha_{conj} : G \curvearrowright G$ , notice the stabilizer of  $a$  is exactly  $Z(a)$ , and by orbit-stabilizer, each orbit has size  $|G : Z(a)|$ . Since orbits partition  $G$ , we get the class formula.

Notice that each  $Z(a)$  is a subgroup of  $G$ , by our assumption,  $p^k \nmid |Z(a)|$ , which means  $p \mid |G|/|Z(a)| \Rightarrow p \mid |G : Z(a)|$ , so we can rewrite class formula as

$$mp^k = |Z(G)| + p \sum_{a \in A} C_a$$

where we write  $|G : Z(a)|$  as  $C_a p$ . Taking modulo  $p$  on both sides, we get  $0 = |Z(G)| + 0 \pmod{p}$ , so  $|Z(G)| = 0 \pmod{p}$ . Moreover,  $e \in Z(G)$ , so  $|Z(G)| \geq 1 \Rightarrow p \mid |Z(G)|$ . By 5.39, there exists a subgroup of  $Z(G)$  with order  $p$ , which is also normal: this comes from the fact that  $Z(G)$  is the center, so any subgroup of  $Z(G)$  is normal.

Let  $N \trianglelefteq G$  be the normal subgroup of  $G$  with order  $p$ , consider  $G/N$ . Notice that  $p^{k-1} \mid |G/N|$ , so there is a subgroup  $P \leq G/N$  of order  $p^{k-1}$ , by induction hypothesis. Let  $Q$  be the preimage of  $P$ , under the quotient map  $G \twoheadrightarrow G/N$ , one can verify that  $Q$  is a subgroup of  $G$  which contains  $N$ , so  $N \trianglelefteq Q$ , we can write  $P \cong Q/N \Rightarrow |Q| = |P||N| = p^{k-1}p = p^k$ , and we get our desired subgroup.  $\square$

**Definition 5.44.** A  $p$ -group is a group of size equal to a power of  $p$ . A *Sylow  $p$ -subgroup* of a finite group  $G$  is a subgroup  $P \leq G$  such that  $|P|$  = the largest power of  $p$  dividing  $|G|$ .

**Remark 5.45.** One can interpret 5.43 as saying that every finite group  $G$  has a Sylow  $p$ -subgroup, if  $p \mid |G|$ .

**Theorem 5.46** (Sylow's Second Theorem). *Let  $G$  be a finite group,  $p$  be a prime number,  $H \leq G$  be a  $p$ -group and  $P \leq G$  be a Sylow  $p$ -subgroup, then  $H$  is contained in a conjugate of  $P$ , i.e., there exists  $g \in G$  such that  $H \subseteq gPg^{-1}$ .*

Before proving the theorem, let's first prove a handy Lemma.

**Lemma 5.47.** *Let  $G$  be a  $p$ -group,  $S$  be a finite set, and  $Z$  denote the set of fixed points under any action  $G \curvearrowright S$ , then  $|Z| = |S| \pmod{p}$ .*

*Proof.* Given an element  $s \in S$ , let  $O_s$  denote the orbit contains  $s$ , by orbit-stabilizer,  $|O_s| = |G/\text{Stab}(s)| = |G|/|\text{Stab}(s)| \Rightarrow |O_s| \mid |G|$ , since  $G$  is a  $p$ -group, let  $p^k := |G|$ , so  $|O_s| \mid p^k$ . Since orbits partition  $S$ , we can write  $|S| = |Z| + \sum_{s \in A} |O_s|$ , where  $A$  is a subset of  $S$  formed by picking an element from each non-trivial orbit. For each non-trivial orbit,  $|O_s| \geq 2 \Rightarrow p \mid |O_s|$ , so if we take modulo  $p$  on both sides, we get  $|Z| = |S| \pmod{p}$ , as desired.  $\square$

*Proof of Sylow's Second Theorem.* Let  $H \curvearrowright G/P$  by left multiplication, by orbit-stabilizer, every orbit has size equal to  $|H/\text{Stab}(gP)|$ , so every orbit has size a divisor of  $|H|$ , hence a power of  $p$ . But  $|G/P| = |G|/|P| \not\equiv 0 \pmod{p}$ , since  $P$  is Sylow  $p$ -subgroup, so at least one orbit has size  $p^0 = 1$ , which means there is some  $g \in G$ , such that for any  $h \in H$ ,  $hgP = gP \Rightarrow g^{-1}hgP = P \Rightarrow g^{-1}hg \in P \Rightarrow H \subseteq gPg^{-1}$ .  $\square$

**Theorem 5.48** (Sylow's Third Theorem). *Let  $G$  be a finite group with  $|G| = mp^k$ ,  $m \not\equiv 0 \pmod{p}$ , where  $p$  is a prime number. Then number of Sylow  $p$ -subgroups of  $G$  divides  $m$ , and is  $1 \pmod{p}$ .*

**Definition 5.49.** Let  $H \leq G$ , the *normalizer* of  $H$  in  $G$  is  $N_G(H) := \{g \in G : gHg^{-1} = H\}$ , i.e., the stabilizer of  $H$  under conjugation action  $G \curvearrowright \text{Sub}(G)$ , several properties of  $N_G(H)$ :

- $N_G(H) \leq G$
- $H \trianglelefteq N_G(H)$
- Orbit-stabilizer: number of subgroups of  $G$  that are conjugate to  $H$ , i.e., size of orbit containing  $H$ , is equal to  $|G : N_G(H)|$

*Proof of Sylow's Third Theorem.* We first prove the number of Sylow  $p$ -subgroups of  $G$  divides  $m$ . Let  $P$  be any Sylow  $p$ -subgroup of  $G$ , we use  $n_P :=$  number of subgroups conjugate to  $P = |G : N_G(P)| = |G|/|N_G(P)|$ , notice  $|G| = mp^k$ , and  $|N_G(P)|$  is divisible by  $|P| = p^k$ , suppose  $|N_G(P)| = \ell p^k$ , then  $n_P = \frac{mp^k}{\ell p^k} = \frac{m}{\ell} \Rightarrow n_P \ell = m, n_P \mid m$ . Next, we prove  $n_P \equiv 1 \pmod{p}$ . Consider the following:

$$\begin{aligned} m &= |G : P| \\ &= |G : N_G(P)| |N_G(P) : P| \\ &= n_P |N_G(P) : P| \end{aligned}$$

**Lemma 5.50.** *Let  $G$  be a finite group,  $p$  be a prime number,  $H \leq G$  be a  $p$ -group, then  $|N_G(H) : H| \equiv |G : H| \pmod{p}$ .*

*Proof of Lemma.* Consider the action  $H \curvearrowright G/H$  by left multiplication. Orbits have sizes which are powers of  $p$ . By 5.47,  $|G : H| = |G/H| = (\text{number of fixed points of this action}) \pmod{p}$ , so it suffices to show  $|N_G(H) : H|$  equals to the number of fixed points, modulo  $p$ . Consider the following chain of logical equivalence:

$$\begin{aligned} gH \text{ is a fixed point} &\Leftrightarrow \forall h \in H, hgH = gH \\ &\Leftrightarrow g^{-1}hgH = H \\ &\Leftrightarrow ghg^{-1} \in H \\ &\Leftrightarrow H = gHg^{-1} \\ &\Leftrightarrow g \in N_G(H) \end{aligned}$$

So  $gH$  is a fixed point if and only if  $g \in N_G(H)$ , i.e., it corresponds to a coset of  $N_G(H)/H$ . Thus, we have the identity.  $\square$

By Lemma, our original equation becomes  $m = |G : P| = |N_G(P) : P| \pmod{p}$ , i.e.,  $n_P |N_G(P) : P| \equiv |N_G(P) : P| \pmod{p}$ , since  $P$  is Sylow  $p$ -subgroup,  $|N_G(P) : P|$  is not divisible by  $p$ , so we must have  $n_P \equiv 1 \pmod{p}$ , as desired.  $\square$

**Proposition 5.51.** *There are no simple groups of order 12.*

*Proof.*  $12 = 2^2 \times 3$ . Number of Sylow 2-subgroups: 1 or 3, number of Sylow 3-subgroups: 1 or 4. Assume for a contradiction that there is a simple group of order 12, then there must be 3 Sylow 2-subgroups and 4 Sylow 3-subgroups, so there are 3 subgroups of order 4, 4 subgroups of order 3. How many elements are there of order 3? At most  $2 \times 4 = 8$  elements, so it remains  $12 - 8 = 4$  elements, and we cannot fit 3 subgroups of order 4 into 4 elements.  $\square$

**Proposition 5.52.** *There are no simple groups of order 24.*

*Proof.*  $24 = 2^3 \times 3$ . Number of Sylow 3-subgroups: 1 or 4, number of Sylow 2-subgroups: 1 or 3, again assume for a contradiction that there is a simple group of order 24, so number of Sylow 3-subgroups is 4, and number of Sylow 2-subgroups is 3. Let  $G \curvearrowright \{\text{Sylow 2-subgroups}\}$  by conjugation, we can view it as  $\alpha : G \rightarrow \text{Sym}(\{1, 2, 3\})$ . Now let's examine  $\ker(\alpha)$ , since  $|G| = 24, |\text{Sym}(\{1, 2, 3\})| = 6$ ,  $\alpha$  is not injective, so  $\ker(\alpha) \neq \{e\}$ , on the other hand, since  $\alpha$  is conjugation, clearly  $\ker(\alpha) \neq G$ , since we have assumed  $G$  is simple, so all Sylow 2-subgroups conjugate with each other. Thus, we have found a non-trivial normal subgroup of  $G$ , which is  $\ker(\alpha)$ .  $\square$

## 6 Rings and Modules

### 6.1 Basic definitions

Rings and modules are built upon groups, they are less “abstract”, in the sense that they allow more operations, so there are real life examples and applications of this concept.

**Definition 6.1.** Let  $A$  be an abelian group. An *endomorphism* of  $A$  is a homomorphism  $f : A \rightarrow A$ .

**Example 6.2.** Some examples of endomorphisms:

- identity map,  $\mathbf{1}$
- zero map, i.e., map all elements to 0,  $\mathbf{0}$
- inverse map:  $a \mapsto -a$ , denoted by  $-\mathbf{1}$ , this uses abelian:  $-\mathbf{1}(a+b) = -b-a = -a-b = -\mathbf{1}(a) + -\mathbf{1}(b)$

**Definition 6.3.** Let  $\text{End}(A) := \{\text{all endomorphisms of } A\}$ , except for standard function composition, we also equip  $\text{End}(A)$  with pointwise addition: for  $f, g \in \text{End}(A)$ , define  $f+g : A \rightarrow A$  by  $(f+g)(a) = f(a) + g(a)$ .

**Proposition 6.4.**  $f+g$  is an endomorphism.

*Proof.*

$$\begin{aligned}
 (f+g)(a+b) &= f(a+b) + g(a+b) \\
 &= f(a) + f(b) + g(a) + g(b) \\
 &= f(a) + g(a) + f(b) + g(b) \\
 &= (f+g)(a) + (f+g)(b)
 \end{aligned}
 \quad \square$$

**Exercise 6.5.** Check that  $(\text{End}(A), +)$  is abelian.

**Definition 6.6.** A *concrete ring* is a subgroup  $R \leq (\text{End}(A), +)$ , such that for all  $f, g \in R$ ,  $f \circ g \in R$ . If  $\text{id}_A = \mathbf{1} \in R$ , then  $R$  is called a *unital* ring.

**Example 6.7.** 1.  $\text{End}(A)$ , analogous to  $\text{Sym}(A)$ , called the *endomorphism ring* of  $A$ .

2.  $\{\mathbf{0}\} \leq \text{End}(A)$  is a ring.
3. What is  $\text{End}(\mathbb{Z})$ ? For  $f \in \text{End}(\mathbb{Z})$ , all its values are determined by  $f(1)$ , for each  $n \in \mathbb{Z}$ ,  $\exists! f \in \text{End}(\mathbb{Z})$  with  $f(1) = n, f(m) = nm$ . Let  $f_n$  denote the function that  $f(1) = n$ , so  $\text{End}(\mathbb{Z}) = \{f_n : n \in \mathbb{Z}\}$ , and  $f_n + f_k = f_{n+k}, f_n \circ f_k = f_{nk}$ , so  $(\text{End}(\mathbb{Z}), +, \circ) \cong (\mathbb{Z}, +, \cdot)$ .
4.  $\{f_r : r \in \mathbb{R}\} \subseteq \text{End}(\mathbb{R})$ , for each  $r \in \mathbb{R}$ ,  $f_r : \mathbb{R} \rightarrow \mathbb{R}$  is given by  $f_r(s) = rs$ , then  $f_r \in \text{End}(\mathbb{R})$ ,  $f_r + f_s = f_{r+s}, f_r \circ f_s = f_{rs}$ , so  $\{f_r : r \in \mathbb{R}\}$  is a concrete ring on  $\mathbb{R}$ , and it is isomorphic to  $(\mathbb{R}, +, \cdot)$ . However, it is not the entire  $\text{End}(\mathbb{R})$ : there exists  $f \in \text{End}(\mathbb{R})$  such that  $f(1) = \pi, f(\sqrt{2}) = e$ .

**Definition 6.8.** An (*abstract*) *ring* is a set  $R$  with two binary operations  $+, \cdot$ , such that  $(R, +)$  is an abelian group with identity  $0 \in R$ .  $\cdot$  is associative and for all  $a, b, c \in R$ ,  $a \cdot (b+c) = a \cdot b + a \cdot c$ . If  $\cdot$  has an identity element  $1$ , then  $R$  is called *unital*. If  $\cdot$  is commutative, then  $R$  is called a *commutative ring*.

Analogous to concrete group and group, if  $R \subseteq \text{End}(A)$  is a concrete ring,  $f, g, h \in R$ , then

$$\begin{aligned}(f \circ (g + h))(a) &= f \circ (g + h)(a) \\ &= f(g(a) + h(a)) \\ &= f(g(a)) + f(h(a)) \\ &= f \circ g(a) + f \circ h(a)\end{aligned}$$

**Theorem 6.9.** Let  $(R, +, \cdot)$  be a ring, for each  $r \in R$ , let  $f_r : R \rightarrow R : a \mapsto ra$ , then  $f_r \in \text{End}(R, +)$ ,  $\tilde{R} := \{f_r : r \in R\}$  is a concrete ring on  $(R, +)$  and the map  $R \rightarrow \tilde{R} : r \mapsto f_r$  is an isomorphism from  $(R, +, \cdot)$  to  $(\tilde{R}, +, \circ)$ .

*Proof.* One can easily duplicate the argument from 3.22. We won't repeat it here.  $\square$

**Example 6.10.**  $\text{End}(\mathbb{Z}^2)$ . Let  $f : \mathbb{Z}^2 \rightarrow \mathbb{Z}^2$  be an endomorphism, suppose  $f(1, 0) = (a, b)$ ,  $f(0, 1) = (c, d)$ , then  $f(x, y) = xf(1, 0) + yf(0, 1) = (xa, xb) + (yc, yd) = (xa + yc, xb + yd)$ . It is best to write it in matrix notation:

$$f(x, y) = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

So  $\text{End}(\mathbb{Z}^2)$  is all  $2 \times 2$  integer matrices.

**Exercise 6.11.** Verify that in  $\text{End}(\mathbb{Z}^2)$ , ring addition is matrix addition, and function composition is matrix multiplication. It's worth noticing that this ring is not commutative.

**Definition 6.12.** Let  $R, S$  be rings, a *homomorphism* from  $R$  to  $S$  is a function  $f : R \rightarrow S$  such that

- $f$  is a homomorphism of abelian groups  $(R, +_R), (S, +_S)$
- $\forall a, b \in R, f(ab) = f(a)f(b)$

If  $R, S$  are unital, then a homomorphism  $f : R \rightarrow S$  is called *unital* if  $f(1_R) = 1_S$ .

**Definition 6.13.** An *R-module* or a *module over R* is an abelian group  $M$ , with a homomorphism  $\alpha : R \rightarrow \text{End}(M)$ . If  $R$  is unital, then  $R$ -module  $\alpha : R \rightarrow \text{End}(M)$  is unital, if  $\alpha(1_R) = \text{id}_M$ . Often, we say “ $M$  is an  $R$ -module” and write  $ra$  for  $\alpha(r)(a)$ .

**Example 6.14.** 1. Let  $R$  be a ring, then  $R \rightarrow \text{End}(R) : r \mapsto (a \mapsto ra)$  is a homomorphism, so  $R$  is a module of itself.

2. Let  $R$  be a ring,  $M$  be any abelian group, the trivial homomorphism  $R \rightarrow \text{End}(M) : r \mapsto \mathbf{0}$ .

3.  $\mathbb{Z}$ -module: Let  $M$  be an abelian group, consider the following homomorphism:  $\mathbb{Z} \rightarrow \text{End}(M) : 0 \mapsto \mathbf{0}, 1 \mapsto \text{id}_M, n \mapsto n \cdot \text{id}_M = \underbrace{\text{id}_M + \text{id}_M + \dots + \text{id}_M}_n$ , i.e.,  $(n\text{id}_M)(a) = \underbrace{a + a + \dots + a}_n = na, \forall n \in \mathbb{Z}, a \in M$ .

**Exercise 6.15.** Show that this is a ring homomorphism, i.e., it preserves multiplication.

**Remark 6.16.** This establishes a relation: unital  $\mathbb{Z}$ -modules correspond to abelian groups.

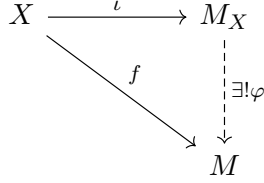
4. Let  $R$  be a ring,  $R^n$  (as abelian group) can be equipped with an  $R$ -module structure as follows:  $r(a_1, a_2, \dots, a_n) = (ra_1, \dots, ra_n)$ .



## 6.2 Free modules, independent, spanning, and basis

**Definition 6.17.** Let  $R$  be a unital ring and  $X$  be a set, a *free  $R$ -module over  $X$*  is a (unital)  $R$ -module  $M_X$ , together with the function  $\iota : X \rightarrow M_X$ , such that for all (unital)  $R$ -modules  $M$  and functions  $f : X \rightarrow M$ , there exists a unique  $R$ -module homomorphism  $\varphi : M_X \rightarrow M$ , such that  $\varphi \circ \iota = f$ .

**Remark 6.18.** This is almost the same diagram as free group:



**Definition 6.19.** Let  $M, M'$  be  $R$ -modules, a function  $\varphi : M \rightarrow M'$  is an  *$R$ -module homomorphism* if it is a group homomorphism and for all  $r \in R$ ,  $a \in M$ ,  $\varphi(ra) = r\varphi(a)$ .

Let's now discover the structure of  $M_X$ . If  $X$  is finite, then  $M_X \cong R^n$ , where  $n = |X|$ . The idea is to think of the embedding function  $\iota$  as map each element of  $X$  to an indicator vector, or more formally, define  $M_X = \{\omega : X \rightarrow R\}$  and  $\iota : X \rightarrow M_X : x \mapsto \omega_x$ , where  $\omega_x(y) = \begin{cases} 1_R, & \text{if } y = x \\ 0_R, & \text{otherwise} \end{cases}$ .

On the other hand, if  $X$  is infinite, we just change the definition of  $M_X$  a little bit:  $M_X = \{\omega : X \rightarrow R : \text{there are finitely many } x \in X \text{ such that } \omega(x) \neq 0_R\}$ . For each  $r \in R, \omega \in M_X$ , define  $r \cdot \omega \in M_X$  by  $(r \cdot \omega)(y) = r(\omega(y))$ . Then the definition of  $\varphi$  becomes obvious, let's first write elements of  $M_X$  as  $\sum_{x \in X} a_x \omega(x)$ , where  $a_x \in R$ , so  $\varphi(\omega) := \varphi(\sum_{x \in X} a_x \omega(x)) = \sum_{x \in X} a_x f(x)$ .

**Exercise 6.20.** Check this is a homomorphism, and it is unique.

We will extend on  $\varphi$  in free modules, to introduce some concepts the reader might recall from linear algebra.

**Definition 6.21.** Let  $X \subseteq M$ .

- $X$  is *independent* if  $\varphi$  is injective:  $\varphi$  is injective  $\rightarrow \ker(\varphi) = \{0\} \rightarrow$  for any coefficients  $a_x$ ,  $\sum_{x \in X} a_x \cdot x = 0$  implies  $a_x = 0, \forall x \in X$ .
- $X$  is *spanning* if  $\varphi$  is surjective:  $\varphi$  is surjective  $\rightarrow \forall m \in M, \exists$  coefficients  $a_x, x \in X$ , only finitely many of which are non-zero, such that  $\sum_{x \in X} a_x \cdot x = m$ . We write  $\text{span}(X)$  as the span of  $X$ .
- $X$  is a *basis*, if  $\varphi$  is bijective. In this case,  $M$  is a *free  $R$ -module*.

Before looking at free modules, let's first check out some examples on non-free modules.

**Definition 6.22.** Let  $G$  be a group,  $G$  is *torsion-free*, if for any  $g \in G$ ,  $g$  has infinite order, i.e., for  $k \in \mathbb{Z} \setminus \{0\}$ ,  $g^k \neq 0$ .

**Example 6.23.** 1.  $\mathbb{Z}_n$  is a  $\mathbb{Z}$ -module that has no basis, there are no non-empty independent sets.  $\forall x \in \mathbb{Z}_n, n \cdot x = 0 \Rightarrow \{x\}$  is not independent. Note that  $(\mathbb{Z}_n, +, \cdot)$  is a ring, and as a  $\mathbb{Z}_n$ -module,  $\mathbb{Z}_n$  is free, since  $\{1\}$  is a basis. Observe that any free  $\mathbb{Z}$ -module is *torsion-free*, i.e., any element in module  $M$  has infinite order:  $\forall r \in \mathbb{Z} \setminus \{0\}$  and  $x \in M \setminus \{0\}, r \cdot x \neq 0$ . For basis, this is trivially true, so suppose  $x$  is not a basis, we can write it as  $\sum_{b \in B} a_b \cdot b$ , so  $r \cdot x = \sum_{b \in B} r a_b \cdot b$ , since  $r$  is non-zero, there is at least one coefficient is non-zero, so  $r \cdot x \neq 0$ .

2.  $(\mathbb{Q}, +)$  is a torsion-free abelian group. As a  $\mathbb{Z}$ -module, it has no basis: suppose  $X \subseteq \mathbb{Q}$  is a basis for  $\mathbb{Q}$  as a  $\mathbb{Z}$ -module, pick  $x \in X, x \neq 0$ , then  $\frac{1}{2}x = \sum_{y \in X} c_y \cdot y$ , with only finitely many non-zero  $\Rightarrow 1 \cdot x = \sum_{y \in X} (2c_y) \cdot y$ , the coefficient of  $x$  is odd, but coefficients on RHS are even, so  $X$  cannot be a basis.

**Fact:** If  $X$  is a basis, then  $\sum_{x \in X} a_x \cdot x = \sum_{x \in X} b_x \cdot x$ , then  $a_x = b_x, \forall x \in X$ .

3. If  $X$  is infinite, then  $\mathbb{Z}^X$  is not a free  $\mathbb{Z}$ -module.

**Definition 6.24.** A *division ring* is a unital ring  $R$  in which every non-zero element has multiplicative inverse. A non-zero commutative division ring is called a *field*.

**Example 6.25.**  $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_p$  where  $p$  is a prime number,  $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \subset \mathbb{R}$ . Let's verify the last one for the multiplicative inverse part:  $\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$ .

In the next part, we will try to prove that every module over division ring is free.

**Exercise 6.26.** If every  $R$ -module is free, then  $R$  is a division ring.

**Lemma 6.27.** Let  $R$  be a division ring,  $M$  be an  $R$ -module, if  $I \subseteq M$  is an inclusion maximal independent set, i.e., if  $I \subseteq J$  and  $J$  is independent, then  $I = J$ . Then  $I$  is a basis.

*Proof.* We need to show  $\text{span}(I) = M$ . Take  $x \in M \setminus I$ , we want  $x \in \text{span}(I)$ . Notice by definition of  $I$ ,  $I \cup \{x\}$  is not independent, so for some  $(c_y : y \in I \cup \{x\}) \in R^{I \cup \{x\}}$ , only finitely many are non-zero, we have  $\sum_{y \in I \cup \{x\}} c_y \cdot y = 0 \Rightarrow c_x \cdot x + \sum_{y \in I} c_y \cdot y = 0$ , since  $I$  is independent,  $c_x \neq 0$ , so  $c_x \cdot x = \sum_{y \in I} -c_y \cdot y \Rightarrow x = \sum_{y \in I} (-c_x^{-1}c_y) \cdot y$ .  $\square$

**Definition 6.28.** Let  $P$  be a set,  $\preceq$  be a binary relation on  $P$ , we say that  $\preceq$  is a *partially-ordered relation* if

- $\preceq$  is reflexive
- $\preceq$  is antisymmetric, i.e., for  $x, y \in P$ , if  $x \preceq y$  and  $y \preceq x \Rightarrow x = y$
- $\preceq$  is transitive

We say  $(P, \preceq)$  is a *partially-ordered set*, or *poset* for short.

**Definition 6.29.** Let  $(P, \preceq)$  be a poset, a subset  $C \subseteq P$  is a *chain* if for every  $x, y \in C$ ,  $x \preceq y$  or  $y \preceq x$ . An *upper bound* for  $C$  is an element  $x \in P$  such that  $\forall y \in C, y \preceq x$ .

**Lemma 6.30 (Zorn).** If  $(P, \preceq)$  is a poset such that every chain has an upper bound, then  $P$  has a maximal element.

*Proof.* We refer readers any online resources for the proof, since it is out of the scope of this course.  $\square$

**Proposition 6.31.** *Let  $R$  be a ring, and  $R$  be a module of itself by left multiplication. If  $R$  is unital, then  $\alpha : R \rightarrow \text{End}(R)$  is injective.*

*Proof.* Let  $r, s \in R$  with  $r \neq s$ , then  $\alpha(r)(1) = r \cdot 1 = r$ ,  $\alpha(s)(1) = s \cdot 1 = s$ , so  $\alpha(r) \neq \alpha(s)$ .  $\square$

**Theorem 6.32.** *All modules over a division ring are free.*

*Proof.* Let  $R$  be a division ring,  $M$  be an  $R$ -module, let  $P = \{I \subseteq M : I \text{ is independent}\}$ , consider the poset  $(P, \subseteq)$ , if  $(P, \subseteq)$  has a maximal element, then by 6.27,  $M$  has a basis. Let  $C \subseteq P$  be a chain, we want to show that  $C$  has an upper bound, the claim is  $\bigcup C = \bigcup_{I \in C} I$  is the upper bound we want, we need to show that  $\bigcup C$  is independent. Suppose not, then  $\sum_{x \in \bigcup C} c_x \cdot x = 0$  is a nontrivial linear combination, we write it as  $c_1 \cdot x_1 + c_2 \cdot x_2 + \dots + c_k \cdot x_k = 0$ , let  $x_i \in I_i \subseteq C$ , reorder them as  $I_1 \subseteq I_2 \subseteq \dots \subseteq I_k$ , then  $x_1, \dots, x_k \in I_k$ , but  $I_k$  is independent, a contradiction. By 6.30,  $(P, \subseteq)$  has a maximal element.  $\square$

Next, we want to define  $\text{rank}(R^n)$  to be  $n$ , but what if  $R^n \cong R^m$  for  $n \neq m$ ?

**Definition 6.33.** A unital ring  $R$  has the *Invariant Basis Number*, or *IBN* for short, if for all  $n, m \in \mathbb{N}^+$ ,  $R^n \cong R^m \Rightarrow n = m$ .

**Theorem 6.34.** *Every division ring has IBN.*

**Lemma 6.35** (Exchange property). *Let  $R$  be a division ring, let  $M$  be an  $R$ -module, let  $I \subseteq M$  be independent,  $B \subseteq M$  a basis. Then for all  $x \in I \setminus B$ , there exists  $y \in B \setminus I$  such that  $(I \setminus \{x\}) \cup \{y\}$  is independent.*

*Proof of Exchange property.* Suppose no such  $y$ , this means for any  $y \in B \setminus I$ ,  $(I \setminus \{x\}) \cup \{y\}$  is not independent, i.e.,  $\sum_{a \in (I \setminus \{x\}) \cup \{y\}} c_a \cdot a = 0$ , for coefficients  $c_a$  non-zero. By an argument analogous to 6.27, we have  $y \in \text{span}(I \setminus \{x\})$ , so  $B \setminus I \subseteq \text{span}(I \setminus \{x\})$ , also  $B \cap I \subseteq I \setminus \{x\} \subseteq \text{span}(I \setminus \{x\})$ , so  $B \subseteq \text{span}(I \setminus \{x\})$ , since  $\text{span}(B) = M$ , so  $I \setminus \{x\}$  spans  $M$ . However,  $x \in \text{span}(I \setminus \{x\})$ , contradicts  $I$  is independent.  $\square$

*Proof of Theorem.* Suppose for a contradiction that  $R^n \cong R^m$  but  $n \neq m$ , without loss of generality, assume  $n < m$ . Let  $B_n$  be a basis for  $R^n$ , and  $B_m$  be a basis for  $R^m$ , so  $|B_n| = n, |B_m| = m$ . We can then apply exchange property, to “swap” elements of  $B_n$  out, replace with elements in  $B_m$ . This results in  $B'_n \subset B_m$ , and  $B'_n$  is a basis, however,  $|B_m| > |B'_n|$ , this means  $B_m$  is not independent, contradicts  $B_m$  is a basis.  $\square$

### 6.3 Commutative rings and IBN

In this section, we will prove an important theorem

**Theorem 6.36.** *Every commutative unital ring  $R$  has IBN.*

**Example 6.37.**  $\mathbb{Z}$  has the IBN. However, as a  $\mathbb{Z}$ -module, it has maximal independent set, say  $\{2\}$ , but it is not a basis. So the idea is to choose a correct module. We provide two proofs.

*Proof #1.* Notice  $\mathbb{Z} \subseteq \mathbb{Q}$ , and  $\mathbb{Q}$  is a field. Let  $B_n := \{x_1, \dots, x_n\}$  be a basis of  $\mathbb{Z}^m$  of size  $n$ , so  $\text{span}_{\mathbb{Z}}(B_n) = \mathbb{Z}^m$ , and  $\text{span}_{\mathbb{Q}}(B_n) = \mathbb{Q}^m$ . Let's show this. Let  $y = \left(\frac{p_1}{q_1}, \dots, \frac{p_m}{q_m}\right) \in \mathbb{Q}^m$ , let  $\tilde{y} = (q_1 \dots q_m) y \in \mathbb{Z}^m$ , so  $\tilde{y} = c_1 x_1 + \dots + c_n x_n \Rightarrow y = \frac{c_1}{q_1 \dots q_m} x_1 + \dots + \frac{c_n}{q_1 \dots q_m} x_n$ . However, since  $\mathbb{Q}$  is a division ring, by 6.34,  $\text{rank}(\mathbb{Q}^m) = m$ , contradicts  $\mathbb{Q}^m$  can be spanned by  $B_n$ .  $\square$

*Proof #2.* Let  $p$  be a prime number,  $\pi_p : \mathbb{Z} \rightarrow \mathbb{Z}_p : k \mapsto k \bmod p$ , again let  $B_n = \{x_1, \dots, x_n\}$  be a basis of  $\mathbb{Z}^m$  with  $n$  elements, define  $\pi_p^m : \mathbb{Z}^m \rightarrow \mathbb{Z}_p^m : (a_1, a_2, \dots, a_m) \mapsto (\pi_p(a_1), \pi_p(a_2), \dots, \pi_p(a_m))$ , so  $\text{span}(\pi_p^m(B_n)) = \mathbb{Z}_p^m$  (here we overload  $\pi_p^m$  to apply on each element of  $B_n$ ): take  $y \in \mathbb{Z}_p^m$ , let  $\tilde{y} \in \mathbb{Z}^m$  be the element such that  $\pi_p^m(\tilde{y}) = y$ , write  $\tilde{y} = c_1 x_1 + \dots + c_n x_n$ , so  $y = \pi_p(c_1) \pi_p^m(x_1) + \dots + \pi_p(c_n) \pi_p^m(x_n)$ , however,  $\mathbb{Z}_p$  is a field, so this contradicts  $\mathbb{Z}_p$  has IBN.  $\square$

We can extend from  $\mathbb{Z}^n$ , to show something about  $\mathbb{F}_n$ , the free group.

**Corollary 6.38.** *Let  $n, m \in \mathbb{N}$ , then  $\mathbb{F}_n \cong \mathbb{F}_m \Rightarrow n = m$ .*

*Proof.* The abelianization of  $\mathbb{F}_n$  is  $\mathbb{Z}^n$ , then  $\mathbb{F}_n \cong \mathbb{F}_m \Rightarrow \mathbb{Z}^n \cong \mathbb{Z}^m \Rightarrow n = m$ .  $\square$

For the definition and property of abelianization, we refer reader to any online resources.

Let  $R$  be a non-zero, commutative, unital ring. For 6.37 to work, we need to embed  $R$  into a field, but this might not work: for example,  $\mathbb{Z}_6$  cannot be embedded into a field, since  $2 \times 3 = 0 \bmod 6$ , suppose we can embed  $\mathbb{Z}_6$  into some field  $K$ , then in  $K$ , 3 has inverse  $3^{-1}$ , so  $2 \times 3 \times 3^{-1} = 2 \times (3 \times 3^{-1}) = 2 = (2 \times) \times 3^{-1} = 0$ , which is not possible. For this to work, one requires additional structure on  $R$ .

**Definition 6.39.** A commutative, non-zero, unital ring  $R$  is called *integral domain* if  $\forall a, b \in R, a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$ .

**Theorem 6.40.** *A commutative, non-zero, unital ring  $R$  can be embedded into a field if and only if  $R$  is integral domain.*

*Proof.* ( $\Rightarrow$ ): We have already shown the contrapositive.

( $\Leftarrow$ ): Given an integral domain  $R$ , we shall construct a field  $\text{Frac}(R)$ , called *field of fractions* of  $R$ . Every element of  $\text{Frac}(R)$  is a fraction of the form  $\frac{a}{b}, a, b \in R, b \neq 0$ .

Idea: we want  $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \frac{a}{c} \cdot \frac{b}{d} = \frac{ab}{cd}$ . Let's try to do so. Define  $\tilde{+}, \tilde{\cdot}$  be binary operations on  $R \times (R \setminus \{0\})$  via  $(a, b) \tilde{+} (c, d) = (ad + bc, bd), (a, b) \tilde{\cdot} (c, d) = (ac, bd)$ .

- $\tilde{+}, \tilde{\cdot}$  are commutative, by definition of  $R$

- $\tilde{+}, \tilde{\cdot}$  are associative:

$$\begin{aligned} [(a, b) \tilde{+} (c, d)] \tilde{+} (e, f) &= (ad + bc, bd) \tilde{+} (e, f) \\ &= (adf + bcf + bde, bdf) \\ (a, b) \tilde{+} [(c, d) \tilde{+} (e, f)] &= (a, b) \tilde{+} (cf + de, df) \\ &= (adf + bcf + bde, bdf) \end{aligned}$$

One can follow the same strategy to show  $\tilde{\cdot}$  is associative.

- identity for  $\tilde{+} : (0, 1)$ , for  $\tilde{\cdot} : (1, 1)$
- distributivity, however, does not hold:

$$\begin{aligned} (a, b) \tilde{\cdot} [(c, d) \tilde{+} (e, f)] &= (a, b) \tilde{\cdot} (cf + de, df) \\ &= (acf + ade, bdf) \\ [(a, b) \tilde{\cdot} (c, d)] \tilde{+} [(a, b) \tilde{\cdot} (e, f)] &= (ac, bd) \tilde{+} (ae, bf) \\ &= (acb + aebd, b^2df) \end{aligned}$$

The problem is different pairs may represent the same fraction, i.e.,  $\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$ . Define a binary relation  $\sim$  on  $R \times (R \setminus \{0\})$  via  $(a, b) \sim (c, d) \Leftrightarrow ad = bc$ .

**Proposition 6.41.**  $\sim$  is an equivalence relation.

*Proof.* Reflexive and symmetric is obvious, let's focus on transitivity. Suppose  $(a, b) \sim (c, d)$ ,  $(c, d) \sim (e, f)$ , then  $ad = bc$ ,  $cf = de$ , we want to show:  $af = be$ .

$$\begin{aligned} ad &= bc \\ adef &= bcef \\ afde &= bec f \\ afde &= bede \\ afde - bede &= 0 \\ (af - be)de &= 0 \end{aligned}$$

Since  $R$  is an integral domain, either  $af - be$  is 0 or  $de$  is 0. In the former case, we are done, so let's check for the latter case. If  $de$  is 0, then  $e$  must be 0, since  $cf = de$ ,  $c$  must also be 0, and again, since  $ad = bc$ ,  $a$  must be 0, so  $af = 0 = be$ , as desired.  $\square$

Let's now formally define  $\text{Frac}(R) := R \times (R \setminus \{0\}) / \sim$ , notation: we write  $\frac{a}{b}$  for the  $\sim$  class of the pair  $(a, b)$ .

Define  $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ ,  $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ , one can verify this is well-defined. Now  $+, \cdot$  on  $\text{Frac}(R)$  are associative, commutative, distributive, and have identities:

- Additive inverse:  $-\frac{a}{b} = \frac{-a}{b} : \frac{a}{b} + \frac{-a}{b} = \frac{0}{1}$ ,  $\frac{ab+b(-a)}{b^2} = \frac{0}{b^2}$ , but  $0 \cdot 1 = 0 \cdot b^2$ , so  $\frac{0}{b^2} = \frac{0}{1}$ .
- Multiplicative inverse:  $(\frac{a}{b})^{-1} = \frac{b}{a}$ , the multiplicative identity is  $\frac{1}{1}$ ,  $\frac{1}{1} \neq \frac{0}{1}$  since  $0 \neq 1$  in  $R$ .

So  $\text{Frac}(R)$  is a field. Define  $\iota : R \rightarrow \text{Frac}(R) : a \mapsto \frac{a}{1}$ , this is an injective unital ring homomorphism.  $\square$

**Remark 6.42.**  $\text{Frac}(R)$  is the smallest field containing  $R$ , we always have the following diagram:

$$\begin{array}{ccc} R & \xrightarrow{\iota} & \text{Frac}(R) \\ & \searrow f & \downarrow \exists! \text{embedding} \\ & & K \end{array}$$

where  $f$  is an unital embedding,  $K$  is a field. The embedding from  $\text{Frac}(R)$  to  $K$  is given by  $\frac{a}{b} \mapsto f(a) f(b)^{-1}$ .

**Corollary 6.43.** *Integral domains have IBN.*

*Proof.* Repeat the proof for  $\mathbb{Z}$  using embedding  $\mathbb{Z} \hookrightarrow \mathbb{Q}$  for arbitrary integral domain to its fractional field.  $\square$

To achieve our goal, i.e., prove commutative ring has IBN, we need to adapt the idea in  $\mathbb{Z} \twoheadrightarrow \mathbb{Z}_p$ , i.e., find a surjective homomorphism  $R \twoheadrightarrow F$ , where  $F$  is a field.

Let  $R$  be a ring,  $M, N$  be  $R$ -modules,  $\varphi : M \rightarrow N$  be an  $R$ -module homomorphism, we have the following diagram:

$$M \twoheadrightarrow N/\ker(\varphi) \xrightarrow{\cong} \text{im}(\varphi) \hookrightarrow N$$

This is called the *isomorphism theorem for  $R$ -module*. In fact,  $\text{im}(\varphi)$ ,  $\ker(\varphi)$  and  $N/\ker(\varphi)$  are all  $R$ -modules.

- $\text{im}(\varphi)$  is a submodule of  $N$ : if  $x \in \text{im}(\varphi)$ ,  $r \in R$ , then there exists some  $y \in M$  with  $x = \varphi(y)$ , so  $r \cdot x = \varphi(r \cdot y) \in \text{im}(\varphi)$ .
- $\ker(\varphi)$  is a submodule of  $M$ : if  $x \in \ker(\varphi)$ ,  $r \in R$ , then  $\varphi(x) = 0$ ,  $\varphi(r \cdot x) = r \cdot \varphi(x) = r \cdot 0 = 0$ , so  $r \cdot x \in \ker(\varphi)$ .

Generally speaking, if  $M' \subseteq M$  is a submodule, then  $M/M'$  becomes an  $R$ -module under  $r \cdot (x + M') := (r \cdot x) + M'$ . This is well-defined: if  $x + M' = y + M' \Rightarrow x - y \in M' \Rightarrow r \cdot (x - y) \in M' \Rightarrow r \cdot (x - y) + M' = M' \Rightarrow (r \cdot x) + M' = (r \cdot y) + M'$ .

**Exercise 6.44.** Check this makes  $M/M'$  an  $R$ -module.

**Remark 6.45.** If  $R$  is a unital ring,  $M, N$  be *unital*  $R$ -modules, i.e.,  $1 \cdot x = x$ ,  $\varphi : M \rightarrow N$  be a module homomorphism, then  $M \twoheadrightarrow N/\ker(\varphi) \cong \text{im}(\varphi) \hookrightarrow N$ , all intermediate modules are also unital.

**Definition 6.46.** Let  $R$  be a ring,  $R$  is an  $R$ -module under left multiplication, submodules of  $R$ , viewed as an  $R$ -module, are called (*left*) *ideals*. In other words,  $I \subseteq R$  is a (left) ideal if

1.  $I$  is a subgroup of  $(R, +)$
2. for all  $x \in I, r \in R$ , we have  $r \cdot x \in I$

Note that an ideal is a subring.

**Example 6.47.** • For every ring  $R$ :  $R, \{0\}$ .

- $\mathbb{Z}$ :  $\{0\}, \mathbb{Z}, n\mathbb{Z}$ , i.e., every subgroup of  $\mathbb{Z}$  is an ideal, but not necessarily unital, for example,  $2\mathbb{Z}$  is not unital.

**Proposition 6.48.** *Let  $K$  be a field, the only ideals in  $K$  are  $\{0\}, K$ .*

*Proof.* Suppose  $I \subseteq K$  is an ideal,  $\{0\} \subset I \subset K$ , take any  $x \in I \setminus \{0\}$ , then for all  $y \in K$ ,  $y = (yx^{-1})x \in I$ , so  $I = K$ .  $\square$

**Proposition 6.49.** *Let  $R$  be a non-zero commutative, unital ring.  $R$  is a field if and only if the only ideals are  $R$  and  $\{0\}$ .*

*Proof.*  $(\Rightarrow)$ : 6.48.

$(\Leftarrow)$ : Suppose  $R$  is not a field, take  $x \neq 0$  with no multiplicative inverse, consider  $I := \{rx : r \in R\}$ ,  $I \neq R$ , since  $1 \notin I$ , and it is also non-zero, since  $x \in I$ . Let's check  $I$  is an ideal:

$$1. \ 0 \in I, rx + sx = (r + s)x \in I, -(rx) = (-r)x \in I.$$

$$2. \ s \cdot rx = (sr)x \in I.$$

$\square$

**Proposition 6.50.** *Let  $I$  be an ideal in a unital ring  $R$ , then  $I \neq R$  if and only if  $1 \notin I$ , i.e.,  $I$  is a proper ideal.*

*Proof.*  $(\Rightarrow)$ : Clear.

$(\Leftarrow)$ : If  $1 \in I$ , then for any  $r \in R$ ,  $r \cdot 1 = r \in I$ .  $\square$

Let  $R, Q$  be rings,  $\varphi : R \rightarrow Q$  be a ring homomorphism, consider the diagram:

$$R \twoheadrightarrow R/\ker(\varphi) \xrightarrow{\cong} \text{im}(\varphi) \hookrightarrow Q$$

where  $\ker(\varphi)$  is an ideal of  $R$ : it's a subgroup, and for  $x \in \ker(\varphi)$ ,  $\varphi(x) = 0 \Rightarrow \varphi(rx) = r\varphi(x) = r \cdot 0 = 0$ , so  $rx \in \ker(\varphi)$ .  $\text{im}(\varphi)$  is a subring of  $Q$ : for  $x, y \in \text{im}(\varphi)$ ,  $\varphi(a) = x, \varphi(b) = y \Rightarrow \varphi(ab) = xy$ , so  $xy \in \text{im}(\varphi)$ .

Remember the group situation:  $\varphi : G \rightarrow H$ , then

$G \twoheadrightarrow G/\ker(\varphi) \xrightarrow{\cong} \text{im}(\varphi) \hookrightarrow H$  where  $\ker(\varphi)$  is normal, so  $G/\ker(\varphi)$  is a group, and  $\text{im}(\varphi)$  is a subgroup of  $H$ . In our ring analogy,  $\ker(\varphi)$  is not only a left ideal, but also a right ideal: for  $x \in I, r \in R, xr \in I$ . In fact,  $\ker(\varphi)$  is a *two-sided* ideal, both left and right ideal.

Let  $R$  be a ring,  $I \subseteq R$  be a two-sided ideal, then  $R/I$  becomes a ring under multiplication:  $(x + I)(y + I) := (xy) + I$ , let's check it's well-defined: suppose  $x + I = x' + I, y + I = y' + I$ , want to show that  $(xy) + I = (x'y') + I$ . Notice  $x - x', y - y' \in I$ , so  $(x - x')y = xy - x'y \in I$ ,  $x'(y - y') = x'y - x'y' \in I \Rightarrow xy - x'y + x'y - x'y' = xy - x'y' \in I \Rightarrow (xy) + I = (x'y') + I$ .

**Exercise 6.51.** Check  $R/I$  is a ring.

**Theorem 6.52.** *Let  $R$  be a non-zero, commutative, unital ring, then there exists a surjective homomorphism  $R \twoheadrightarrow K$ , where  $K$  is a field.*

For what ideals  $I \subseteq R$  is  $R/I$  a field?

**Example 6.53.**  $R = \mathbb{Z}$ , then  $\mathbb{Z}/I$  is a field for  $I = p\mathbb{Z}$ , where  $p$  is a prime number.  $R/I \neq \{0\} \Leftrightarrow I \neq R$ , so  $I$  is a proper ideal.

**Lemma 6.54.** *Let  $R$  be a commutative, unital ring,  $I \subseteq R$  be an ideal, then there is a one-to-one correspondence between  $\{J \subseteq R/I, \text{an ideal}\}$  and  $\{I' \subseteq R, \text{an ideal}, I \subseteq I'\}$ , the bijective mapping is given by  $J \mapsto \{x \in R : x + I \in J\} = \bigcup J$ , and the inverse is  $I' \mapsto \{x + I : x \in I'\}$ .*

*Proof.* We'll verify the direction  $I' \mapsto \{x + I : x \in I'\}$ , let  $I \subseteq I' \subseteq R$ , and  $J := \{x + I : x \in I'\}$ , we need to check that  $J$  is an ideal of  $R/I$ . This is the case, since  $J$  is the image of  $I'$  under quotient map  $R \Rightarrow R/I$ , so  $J$  is a subgroup of  $R/I$ . To see it's an ideal, take  $x + I \in J, x \in I'$ , and  $y + I \in R/I$ , then  $(y + I)(x + I) = (yx) + I \in J$ , since  $yx \in I'$ .

Now let's consider the inverse, let  $I'' = \{y \in R : y + I \in J\}$ , the goal is to show  $I' = I''$ . Since  $x \in I' \Rightarrow x + I \in J$ , so  $x \in I'' \Rightarrow I' \subseteq I''$ .

For the other inclusion, suppose  $y + I \in J$ , then there exists  $x \in I'$  such that  $x + I = y + I \Rightarrow x - y \in I \subseteq I'$ , so  $y \in I' \Rightarrow I'' \subseteq I'$ . Thus, this is a valid bijection.

The other direction is left as an exercise to the reader.  $\square$

Let  $I \subseteq R$  be a proper ideal, consider the following chain of logical equivalence:

$$\begin{aligned} R/I \text{ is a field} &\Leftrightarrow \text{the only ideals in } R/I \text{ are } \{0\}, R/I \\ &\Leftrightarrow \text{the only ideals in } R \text{ containing } I \text{ are } I \text{ and } R \\ &\Leftrightarrow \text{the only proper ideal containing } I \text{ is } I \\ &\Leftrightarrow I \text{ is inclusion maximal among all proper ideals} \end{aligned}$$

**Theorem 6.55** (Krull). *Let  $R$  be a commutative, unital, non-zero ring, then  $R$  has a maximal proper ideal.*

*Proof.* We will use 6.30. Let  $P := \{I \subset R : I \text{ is a proper ideal}\}$ , consider the poset  $(P, \subseteq)$ , we want to show every chain has an upper bound in this poset. Take  $C \subseteq P$  be a chain, if  $C = \emptyset$ , then  $\{0\}$  is an upper bound, otherwise,  $C \neq \emptyset$ , then  $\bigcup C$  is an upper bound for  $C$ . Let's check  $\bigcup C$  is an ideal, take  $x \in \bigcup C, r \in R$ , suppose  $x \in I_i$ , then  $r \cdot x \in I_i \subseteq \bigcup C$ . Take  $x, y \in \bigcup C, x \in I_1 \subseteq \bigcup C, y \in I_2$ , so  $I_2 \subseteq I_1$  or  $I_1 \subseteq I_2$ , this means  $x + y$  belongs to the larger ideal, which is a subset of  $\bigcup C$ . So  $\bigcup C$  is an ideal.

Is  $\bigcup C$  proper? Notice  $1 \notin \bigcup C$ , this is true because for any  $I \in C, 1 \notin I$ .

So every chain in  $(P, \subseteq)$  has an upper bound, by Zorn, it has a maximal element.  $\square$

**Corollary 6.56.** *If  $I$  is a proper ideal, then there is a maximal ideal containing  $I$ , i.e.,  $I \subseteq I'$ .*

*Proof.* Apply 6.55 to  $R/I$ , obtaining a maximal proper ideal in  $R/I$ , call it  $J$ , using the bijective mapping from  $R/I$  to  $I$  in 6.54, map  $J$  to  $\bigcup J$ , clearly,  $I \subseteq \bigcup J$ , so it suffices to show  $\bigcup J$  is a maximal proper ideal in  $R$ . Suppose it is not maximal, and adding  $y$  to  $\bigcup J$  still keeps it an ideal, then  $y + I$  is not in  $J$ , again using the mapping in 6.54, we can map  $\bigcup J \cup \{y\}$  to  $J \cup \{y + I\}$ , but the latter is a larger ideal, contradicts  $J$  is maximal.  $\bigcup J$  is proper comes from  $J$  is proper.  $\square$

Let's now prove 6.52.

*Proof.* Use 6.55 to get a maximal proper ideal  $I \subset R$ , consider  $R/I$ , it is a field by our above reasoning. The surjective embedding:  $R \twoheadrightarrow R/I$  is then given by the quotient map.  $\square$

Now we have enough tools to prove 6.36.

*Proof.* Suppose for a contradiction that  $R^m \cong R^n$  but  $n < m$ , take a basis  $x_1, \dots, x_n \in R^m$ , fix a surjective homomorphism  $\pi : R \twoheadrightarrow K$  with  $K$  a field, set  $\pi^m : R^m \rightarrow K^m : (a_1, a_2, \dots, a_m) \mapsto (\pi(a_1), \pi(a_2), \dots, \pi(a_m))$ , then the set  $\{\pi^m(x_1), \dots, \pi^m(x_n)\}$  spans  $K^m$ , but  $n < m, K$  is a field, so it's impossible.



For the spanning part, take any  $y \in K^m$ ,  $\pi$  is surjective, so  $y = \pi^m(z)$  for some  $z \in R^m$ , where  $z = a_1x_1 + \dots + a_nx_n$ , for some  $a_1, \dots, a_n \in R$ , therefore  $y = \pi(a_1)\pi^m(x_1) + \dots + \pi(a_n)\pi^m(x_n)$ , so the set is spanning.  $\square$

## 6.4 Polynomials

We have studied free groups and free modules, so it's time to consider what is free (unital, commutative) rings? The diagram always looks similar:

$$\begin{array}{ccc} X & \xrightarrow{\iota} & R(X) \\ & \searrow f & \downarrow \exists! \varphi \\ & & Q \end{array}$$

where  $R(X)$  is a commutative unital ring,  $\varphi$  is a unital ring homomorphism, and so is  $Q$ .

Let's first consider  $X = \emptyset$ , then  $R(\emptyset) \cong \mathbb{Z}$ , since the only restriction has become  $\varphi$  to be a unique unital ring homomorphism, and we achieve so by  $0 \mapsto 0_Q, 1 \mapsto 1_Q$ . What if  $X = \{x\}$ ? We will show  $R(\{x\}) \cong \mathbb{Z}[x]$ , the *polynomial ring in one variable over  $\mathbb{Z}$* .

**Definition 6.57.** A *polynomial* over  $\mathbb{Z}$  in one variable  $x$  is a sequence  $p = (a_0, a_1, \dots) \in \mathbb{Z}^{\mathbb{N}}$ , such that only finitely many  $a_i$ 's are nonzero, usually, we write  $a_0 + a_1x + a_2x^2 + \dots = \sum_{i=0}^{\infty} a_i x^i = (a_0, a_1, \dots)$ .

The set of all such polynomials is denoted by  $\mathbb{Z}[x]$ .  $\mathbb{Z}[x]$  is an abelian group under  $+$ , defined by  $(a_0, a_1, \dots) + (b_0, b_1, \dots) = (a_0 + b_0, a_1 + b_1, \dots)$ . As an abelian group,  $\mathbb{Z}[x] \cong \bigoplus_{\mathbb{N}} \mathbb{Z}$ , we turn  $\mathbb{Z}[x]$  into a commutative, unital ring by defining a product. For notation, let  $[x^n](a_0, a_1, \dots) := a_n$ , for example,  $[x^2](1 + 3x - x^2 + 7x^8) = -1$ . The product is defined as follows: for  $p, q \in \mathbb{Z}[x]$ ,  $[x^n](pq) := \sum_{i+j=n, i, j \in \mathbb{N}} \{[x^i](p)\} \{[x^j](q)\}$ , or we can write it as  $(\sum_i a_i x^i) (\sum_j b_j x^j) = \sum_n c_n x^n$ , where  $c_n = \sum_{i+j=n} a_i b_j$ .  
Multiplicative identity:  $(1, 0, 0, 0, \dots)$ , and  $x \mapsto (0, 1, 0, 0, \dots)$ . Observe that  $(0, 1, 0, 0, \dots)^n = \left(0, 0, 0, \dots, 0, \underbrace{1}_n, 0, \dots\right)$ .

**Exercise 6.58.** Check  $\mathbb{Z}[x]$  is indeed a commutative ring.

We can now complete the diagram:

$$\begin{array}{ccc} \{x\} & \xrightarrow{x \mapsto x} & \mathbb{Z}[x] \\ & \searrow f \mapsto a & \downarrow \exists! \varphi \\ & & Q \end{array}$$

For  $p \in (c_0, c_1, c_2, \dots) \in \mathbb{Z}[x]$ , define  $\varphi(p) = c_0 + c_1a + c_2a^2 + \dots$ , with only finitely many  $c_i$ 's are nonzero. By our definition,  $\varphi(p)$  is essentially  $p(a)$ , polynomial  $p$  evaluates at point  $a$ .

$\mathbb{Z}[x]$  is free abelian group, generated by  $(1, 0, 0, \dots), (0, 1, 0, \dots), (0, 0, 1, 0, \dots), \dots$

What if  $X = \{x, y\}$ ? We can extend to  $\mathbb{Z}[x, y]$ , *integer polynomials over 2 variables*.

**Definition 6.59.** A *polynomial over  $\mathbb{Z}$  in two variables  $x, y$*  is denoted by  $\mathbb{Z}[x, y]$ , defined as the set  $\{\text{functions } c : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{Z}, \text{ such that } \{(i, j) \in \mathbb{N}^2 : c(i, j) \neq 0\} \text{ is finite}\}$ .

Addition is defined pointwise, so  $\mathbb{Z}[x, y] \cong \bigoplus_{\mathbb{N} \times \mathbb{N}} \mathbb{Z}$ , and multiplication is defined as follows: for  $p, q \in \mathbb{Z}[x, y]$ ,  $[x^n y^m](pq) := \sum_{a, b, c, d \in \mathbb{N}, (a, b) + (c, d) = (n, m)} \{[x^a y^b](p)\} \{[x^c y^d](q)\}$ .  
Define the *evaluation of  $p$  on point  $(a, b)$*  by, for  $p \in \mathbb{Z}[x, y]$ ,  $a, b \in Q$ ,  $p(a, b) := \sum_{(n, m) \in \mathbb{N}^2} ([x^n y^m]) a^n b^m$ .

**Exercise 6.60.** Check the map  $\mathbb{Z}[x, y] \rightarrow Q : p \mapsto p(a, b)$  is a unital ring homomorphism.

If  $X$  is infinite, say  $X = \{x_0, x_1, x_2, \dots\}$ , then we can characterize them as  $x_0^{t_0} x_1^{t_1} x_2^{t_2} \dots$ , where  $t_0, t_1, t_2 \in \mathbb{N}$ , finitely many of them are nonzero.

**Definition 6.61.** Let  $R$  be a commutative, unital ring, and  $X$  be a set, a *polynomial over  $R$  in variable  $X$* , denoted by  $R[X]$ , is a polynomial with coefficients in  $R$ , with variable set  $X$ , and finitely many coefficients are nonzero.

**Definition 6.62.** Let  $M$  be an  $R$ -module, where  $R$  is a commutative, unital ring. An  *$R$ -Endomorphism* of  $M$  is a homomorphism  $f : M \rightarrow M$  of  $R$ -modules, i.e.

- $f$  is a homomorphism of groups  $(M, +) \rightarrow (M, +)$ .
- for all  $r \in R, x \in M$ ,  $f(r \cdot x) = r \cdot f(x)$ .

One can interpret  $R$ -Endomorphism as a standard endomorphism, with additional constraint that  $f$  is linear in  $r \cdot x$ .

Let  $\text{End}_R(M) := \{\text{all } R\text{-endomorphisms of } M\} \subseteq \text{End}(M, +)$ .

- It is a ring: closed under addition, additive inverses, contains 0, and closed under composition.
- It is an  $R$ -module: define for  $r \in R$  and  $f \in \text{End}_R(M)$ ,  $r \cdot f : M \rightarrow M$  via  $(r \cdot f)(x) = r \cdot (f(x))$ .

—

$$\begin{aligned} (r \cdot f)(x + y) &= r \cdot (f(x + y)) \\ &= r \cdot (f(x) + f(y)) \\ &= r \cdot f(x) + r \cdot f(y) \\ &= (r \cdot f)(x) + (r \cdot f)(y) \end{aligned}$$

—

$$\begin{aligned} (r \cdot f)(s \cdot x) &= r \cdot (f(s \cdot x)) \\ &= r \cdot (s \cdot f(x)) \\ &= r \cdot s \cdot f(x) \\ &= s \cdot r \cdot f(x) \\ &= s \cdot (r \cdot f)(x) \end{aligned}$$

**Exercise 6.63.** Finish the check that  $\text{End}_R(M)$  is an  $R$ -module.

**Definition 6.64.** A *concrete  $R$ -algebra* is a subset  $A \subseteq \text{End}_R(M)$  that is both a subring and submodule of  $\text{End}_R(M)$ .

An (*abstract*)  *$R$ -algebra* is a set  $A$  together with a ring structure  $(A, +, \cdot)$  and a (unital)  $R$ -module structure such that for all  $r, s \in R, x, y \in A$ ,  $(r \cdot x) \cdot (s \cdot y) = (rs) \cdot (xy)$ .

So  $\text{End}_{\mathbb{R}}(\mathbb{R}^2) \cong 2 \times 2$  real matrices, since any  $f \in \text{End}_{\mathbb{R}}(\mathbb{R}^2)$  must preserve linear scaling, we won't have something like  $f(1) = \pi, f(\sqrt{2}) = e$ .

**Proposition 6.65.**  $\text{End}_{\mathbb{Z}}(\mathbb{R}^2) = \text{End}_{\mathbb{Q}}(\mathbb{R}^2)$ .

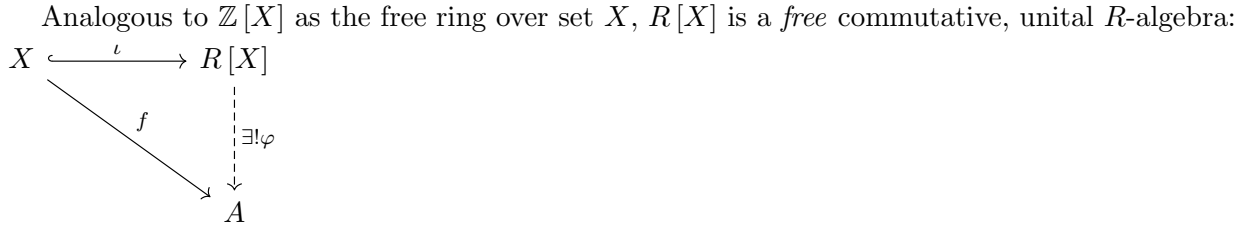
*Proof.* ( $\supseteq$ ): Clear, if  $f$  is linear on all rationals, then it must be linear on all integers.

( $\subseteq$ ): Take  $f \in \text{End}_{\mathbb{Z}}(R)$ , we want to show:  $f \in \text{End}_{\mathbb{Q}}(\mathbb{R}^2)$ , i.e., for all  $q \in \mathbb{Q}, x \in \mathbb{R}^2, f(qx) = qf(x)$ . Write  $q = \frac{s}{t}$  for  $s, t \in \mathbb{Z}, t \neq 0$ , so the question is whether  $\frac{s}{t}f(x) = f(\frac{s}{t}x)$ . Notice that  $f(sx) = f(\frac{s}{t}tx) = sf(\frac{t}{t}x) = sf(x)$ , and  $f(\frac{s}{t}tx) = tf(\frac{s}{t}x)$ , so  $sf(x) = tf(\frac{s}{t}x) \Rightarrow \frac{s}{t}f(x) = f(\frac{s}{t}x)$ .  $\square$

**Exercise 6.66.** Show that  $\mathbb{R}$  as a  $\mathbb{Q}$ -vector space is infinitely dimensional, in fact, the following infinite subset of  $\mathbb{R}$  is  $\mathbb{Q}$ -linearly independent:

- (Tricky):  $1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \dots$
- (Easy):  $\ln 2, \ln 3, \ln 5, \ln 7, \dots$
- (Median): Give an example of an uncountable such set.

Notice that  $\text{End}_{\mathbb{R}}(\mathbb{R}) \cong \mathbb{R}$ , but  $\text{End}_{\mathbb{Q}}(\mathbb{R})$  is much bigger.



Here  $A$  is an  $R$ -algebra, and  $\varphi$  is a unital  $R$ -algebra homomorphism.

From now on, we focus on the ring  $R[x]$ .

**Definition 6.67.** Let  $R$  be a ring,  $r \in R$  is called *unit* if it has multiplicative inverse.

In  $R[x]$ , units are all nonzero constants, whose coefficients are units.

Recall the fundamental theorem of arithmetic: every natural number admits a unique prime factorization. In the proof, we first use a strong induction to show every natural number *has* a prime factorization, then we use a contradicting argument to show it's unique. We remind reader the proof:

**Theorem 6.68** (Fundamental Theorem of Arithmetic). *Every natural number has a unique prime factorization.*

*Proof.* **Existence:** Induction on  $n$ . For  $n = 0, 1$ , it's clear. Otherwise, either  $n$  is a prime number, then we are done, or  $n$  is a composite, let  $p$  be one of its prime divisor, then by induction hypothesis,  $n/p$  has a prime factorization, plus  $p$ , we get a prime factorization for  $n$ .

**Uniqueness:** Suppose otherwise,  $n$  has two prime factorizations:  $n = p_1 \dots p_s = q_1 \dots q_t$ , let  $p_i$  be the first uncommon prime divisor, then  $p_i \mid n \Rightarrow p_i \mid q_1 \dots q_t$ . Recall *Euclid Lemma*: if  $p$  is a prime,  $p \mid ab \Rightarrow p \mid a$  or  $p \mid b$ , so  $p_i \mid q_1$  or  $p_i \mid q_2 \dots q_t$ , since  $p_i \neq q_1$ , it must be the latter case, we iteratively apply this argument to the product part, finally we will have  $p_i \mid q_j$ , for any  $1 \leq j \leq t$ , but  $p_i$  does not exist in  $q_1 \dots q_t$ , a contradiction.  $\square$

To this end, we will adapt the same argument to show that any polynomial in  $R[x]$  admits a unique “prime” factorization.

**Definition 6.69.** Let  $R$  be a ring, a nonunit  $a \in R$  is *irreducible* if it cannot be written as  $a = bc$ , for nonunits  $b, c$ .

**Definition 6.70.** A nonunit  $a \in R$  is *prime* if  $\forall b, c \in R, a \mid bc \Rightarrow a \mid b$  or  $a \mid c$ .

**Definition 6.71.** Let  $a, b \in R$ , the *greatest common divisors* of  $a, b$ , denoted by  $\gcd(a, b)$ , is the set  $\{g : g \mid a \wedge g \mid b, \forall h, h \mid a \wedge h \mid b \Rightarrow h \mid g\}$ .

**Proposition 6.72.** Any two  $\gcd$ 's are related by units.

*Proof.* Suppose  $g_1, g_2 \in \gcd(a, b)$ , then  $g_1 \mid g_2, g_2 \mid g_1$ , so there exists  $k, \ell, g_1 = kg_2, g_2 = \ell g_1 \Rightarrow g_2 = k\ell g_2$ , which means  $k\ell = 1 \Rightarrow k, \ell$  are units.  $\square$

In our familiar  $\mathbb{Z}$ , we have  $\gcd(a, b) \neq \emptyset, \gcd(a, b) = \gcd(a - kb, b), \gcd(a, 0) = \{\pm a\}$ . Moreover, for any  $n \in \mathbb{Z}$ ,  $n$  is prime  $\Leftrightarrow n$  is irreducible. We prove so by using *Bezout identity*.

**Lemma 6.73** (Bezout identity). For any  $a, b \in \mathbb{Z}$ , there exists  $x, y \in \mathbb{Z}$ , such that  $ax + by = g, \forall g \in \gcd(a, b)$ .

**Lemma 6.74** (Euclid Lemma). In  $\mathbb{Z}$ , prime and irreducible are equivalent.

*Proof.* Suppose  $p$  is irreducible in  $\mathbb{Z}$  and  $p \mid ab$ , without loss of generality, assume  $p \nmid a$ , then by 6.73,  $\gcd(a, p) = 1$ , so there exists  $x, y$  such that  $px + ay = 1 \Rightarrow pbx + aby = b$ , since  $p \mid ab, ab = kp$  for some  $k$ , so  $bxp + kyp = b \Rightarrow p \mid b$ .  $\square$

How to prove Bezout identity? We will make use of *Euclidean algorithm*, which relies on *division algorithm*, or more concretely, *division with remainders*.

Consider  $R = \mathbb{F}[x]$ , where  $\mathbb{F}$  is some field, we need to define division with remainders for polynomials.

**Lemma 6.75** (Division algorithm). For any  $a(x), b(x) \in \mathbb{F}[x], b(x) \neq 0$ , there exists  $q(x), r(x)$  such that  $a(x) = q(x)b(x) + r(x)$ , such that  $\deg(r) < \deg(b)$  or  $r = 0$ .

*Proof.* Let  $n := \deg(a), m := \deg(b)$ , we prove by induction on  $n$ . Consider two cases.

Case 1  $m > n$ , then  $q(x) = 0, r(x) = a(x)$ .

Case 2  $m \leq n$ , write  $a(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ , with  $a_n \neq 0$ , and  $b(x) = b_0 + b_1x + b_2x^2 + \dots + b_mx^m$ , consider  $a'(x) := a(x) - \frac{a_n}{b_m}x^{n-m}b(x)$ , so  $\deg(a') < n$ , by induction hypothesis,  $a'(x) = q'(x)b(x) + r(x)$ , take  $q(x) = q'(x) + \frac{a_n}{b_m}x^{n-m}$ , then  $a(x) = q(x)b(x) + r(x)$ .  $\square$

The proof also gives an algorithm, which is referred as the *division algorithm*.

Algorithm Division:

```

input: a(x), b(x) != 0;
output: q(x), r(x);
n = deg(a);
m = deg(b);
// Base case
if n < m:
    q(x) = 0;
    r(x) = a(x);
else:
    a'(x) = a(x) - (a_n / b_m)x^(n-m) b(x);
    // Degree of a' < a
    (q'(x), r(x)) = Division(a'(x), b(x));
    q(x) = q'(x) + (a_n / b_m)x^(n-m);
return (q(x), r(x));

```

Let's now prove Euclidean algorithm works in  $\mathbb{F}[x]$ .

**Lemma 6.76** (Euclidean algorithm). *For any  $a(x), b(x), q(x)$ ,  $\gcd(a(x), b(x)) = \gcd(a(x) - q(x)b(x), b(x))$ .*

*Proof.*  $(\subseteq)$  : Given  $g \in \gcd(a, b)$ ,  $g \mid a, b \Rightarrow g \mid qb, \forall q$ , so  $g \mid a - qb$ .

$(\supseteq)$  :  $g \mid a - qb, g \mid b \Rightarrow g \mid a$ . □

Now we are ready to prove Bezout identity for polynomials.

**Lemma 6.77** (General Bezout identity). *For any  $a(x), b(x) \in \mathbb{F}[x]$ , there exists  $w(x), z(x)$ , such that  $a(x)w(x) + b(x)z(x) = g(x)$ , where  $g(x) \in \gcd(a(x), b(x))$ .*

*Proof.* We will perform induction on degree. Using 6.75, we write  $a(x) = q(x)b(x) + r(x)$ , by 6.76,  $\gcd(a(x), b(x)) = \gcd(r(x), b(x))$ , so by induction hypothesis,

$$\begin{aligned}
 g(x) &= w(x)r(x) + z(x)b(x) \\
 &= w(x)(a(x) - q(x)b(x)) + z(x)b(x) \\
 &= w(x)a(x) - w(x)q(x)b(x) + z(x)b(x) \\
 &= w(x)a(x) + (z(x) - w(x)q(x))b(x)
 \end{aligned}$$

□

With Bezout in hand, we get similar result for integers: irreducible polynomials are primes, i.e.,  $p(x) \mid a(x)b(x) \Rightarrow p(x) \mid a(x)$  or  $p(x) \mid b(x)$ .

**Theorem 6.78.** *Let  $\mathbb{F}$  be a field, then for any  $f(x) \in \mathbb{F}[x]$ ,  $f(x)$  admits a unique prime factorization.*

In the last part of this notes, we will take a look at *roots* or *zeros* of polynomials.

**Theorem 6.79.** *Let  $K$  be a field,  $p \in K[x]$  be a monic polynomial of degree  $\geq 1$ , where monic means the coefficient of highest degree is 1. Then there is a field  $L$  such that  $K \subseteq L$ ,  $p$  has a root in  $L$ .*

*Proof.* Let's introduce a new variable  $t$ , and consider  $K[t]$ . Let  $I$  be the ideal in  $K[t]$ , generated by  $p(t)$ , i.e.,  $I := \{q(t)p(t) : q(t) \in K[t]\}$ . Look at  $K[t]/I$ , define  $\varphi(t) = t + I \in K[t]/I$ , so

$$\begin{aligned}
p(t + I) &= a_0 + a_1\varphi(t) + a_2\varphi(t)^2 + \dots + \varphi(t)^d \\
&= a_0 + a_1\varphi(t) + a_2\varphi(t^2) + \dots + \varphi(t^d) \quad \text{since the quotient map is a homomorphism} \\
&= a_0 + \varphi(a_1t) + \varphi(a_2t^2) + \dots + \varphi(t^d) \\
&= \varphi(a_0 + a_1t + a_2t^2 + \dots + t^d) \\
&= \varphi(p(t)) \\
&= p(t) + I \\
&= I \quad \text{since } p(t) \in I \\
&= 0_{K[t]/I}
\end{aligned}$$

**Example 6.80.** Consider  $p(x) = x^2 + 1 \in \mathbb{R}[x]$ , then the field we consider is  $\mathbb{R}[t]/\langle t^2 + 1 \rangle$ , elements are of the form  $q(t) + I$ , and  $p(t + I) = (t + I)^2 + (1 + I) = t^2 + I + 1 + I = (t^2 + 1) + I = I$ .

It remains to show  $K[t]/I$  is a field.

- $K[t]/I$  is nonzero, especially,  $1 \notin I$ . Notice  $\deg(p(t)) \geq 1$ , so for any  $q(t) \in K[t]$ ,  $\deg(q(t)p(t)) \geq 1$ , but 1 has degree 0, so  $1 \neq q(t)p(t)$ . Thus,  $1 \notin I$ , and  $1 + I \in K[t]/I$ .
- $K[t]/I$ , in fact, might fail to be a field, unless  $p(x)$  is irreducible. More formally, if  $p(x)$  is a irreducible polynomial with degree  $\geq 1$ , then the ideal in  $K[t]$  generated by  $p(t)$  is maximal. Suppose not, let  $J$  be a proper ideal of  $K[t]$  such that  $\langle p(t) \rangle \subset J$ , take any  $q(t) \in J \setminus \langle p(t) \rangle$ , let  $g(t)$  be a gcd of  $p(t), q(t)$ , then  $g(t) \neq p(t)$ , since  $q(t) \notin \langle p(t) \rangle$ , so  $g(t) = 1$ , but by 6.77,  $g(t) = s(t)p(t) + f(t)q(t) \in \langle p(t), q(t) \rangle \subseteq J$ , which means  $1 \in J$ ,  $J$  is no longer proper, a contradiction.

By 6.78, we factor  $p(x) = p_1(x)p_2(x)\dots p_k(x)$ , where all of them are irreducible, then pick one of  $p_i(x)$  to generate  $\langle p_i(t) \rangle$ , and take a quotient, we get our desired result.  $\square$

**Exercise 6.81.** Every ideal in  $K[t]$  is generated by one element.

We can even embed  $K$  into  $K[t]/I$ . Let  $p$  be a irreducible polynomial, then  $K[t]/\langle p(t) \rangle$  is a field, moreover, the embedding  $K \hookrightarrow K[t]/\langle p(t) \rangle : a \mapsto (a, 0, 0, \dots) + I$ , is injective. The injectivity comes from the fact that, except for 0, all other polynomials of degree 0 are not in  $\langle p(t) \rangle$ .

**Theorem 6.82.** Let  $K$  be a field, there is a field  $L$  with  $K \subseteq L$ , such that  $L$  is algebraically closed, i.e., every polynomial  $p \in L[x]$  of degree  $\geq 1$  has a root in  $L$ .

*Proof.* Iteratively apply 6.79, until every polynomial has a root.  $\square$

Finally, we are ready to state the *Fundamental Theorem of Algebra*, though it is not fundamental, and even not formally a theorem, nor does it closely connect to algebra.

**Theorem 6.83** (Fundamental Theorem of Algebra).  $\mathbb{C}$  is algebraically closed.