

# Introduction to Algebra I

Kon Yi

October 1, 2025

### **Abstract**

The Introduction to Algebra course by professor 佐藤信夫.

# Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
1.1	Why study groups? . . . . .	2
1.2	Basis Properties of Groups . . . . .	6
1.3	Group homomorphisms/isomorphisms . . . . .	9
1.4	Properties of homomorphism . . . . .	10
1.5	Equivalenec relation . . . . .	11
1.6	Normal subgroups . . . . .	15

# Chapter 1

## Introduction

### Lecture 1

#### 1.1 Why study groups?

10 Sep. 13:20

Since groups appear everywhere, so we have to study them.

- Galois Theory: permutations of roots of polynomials.
- Number Theory: Ideal Class Group, Unit Group (unique factorization).
- Topology:

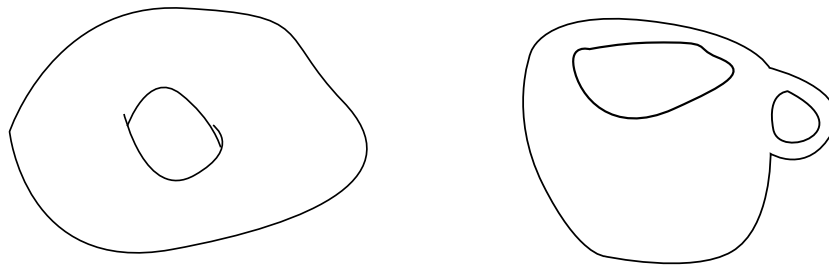


Figure 1.1: Fundamental Groups

- Physics/Chemistry: crystal symmetries and Gauge theory.

**Definition 1.1.1 (mod).** For two integers  $a, b$  we define  $a \equiv b \pmod{N}$  if and only if  $a - b \mid n$ .

Consider the sequence  $1, 2, 4, 8, 16, 32, \dots$ , and observe the remainders after mod  $p$  for different prime  $p$ , then

- $p = 5$ :  $\overbrace{1, 2, 4, 3}, \overbrace{1, 2, 4, 3}, \dots$
- $p = 7$ :  $\overbrace{1, 2, 4}, \overbrace{1, 2, 4}, \dots$

**Theorem 1.1.1 (Fermat's little theorem).** The period divides  $p - 1$ .

**Note 1.1.1.** This is the special case of Lagrange's theorem.

Consider the symmetry of a triangle.

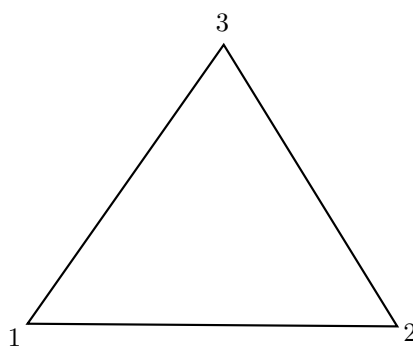


Figure 1.2: Triangle

Consider the rotation:

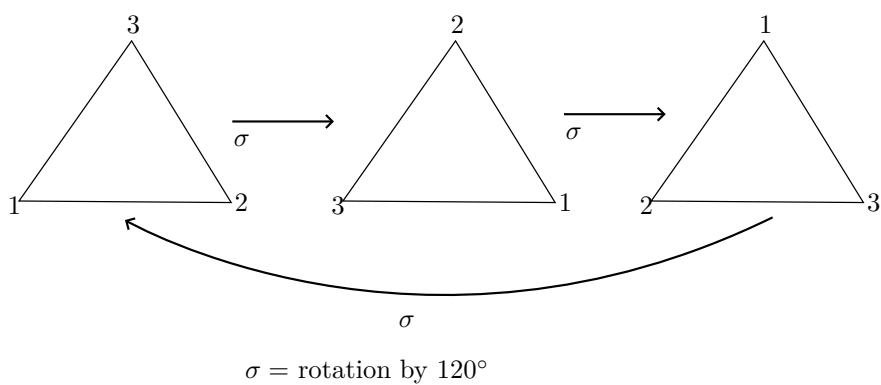


Figure 1.3: title

and reflection

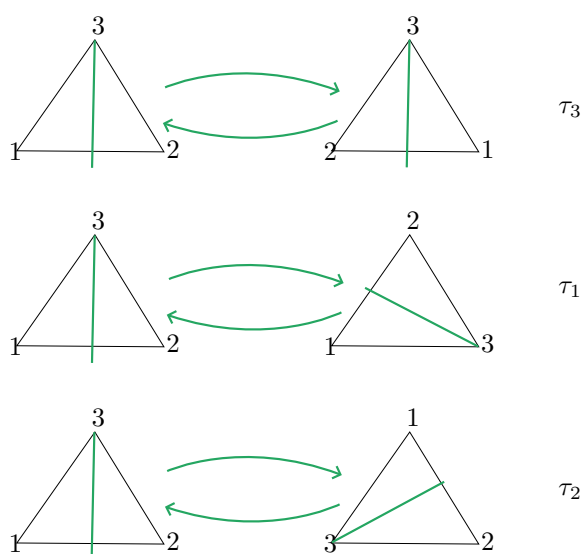


Figure 1.4: title

Hence, symmetries are defined by permutations of the vertices  $\{1, 2, 3\}$ , and thus there are 6 operations  $id, \sigma, \sigma^2, \tau_1, \tau_2, \tau_3$ . It is trivial that there are  $3 \times 2 \times 1$  permutations of  $\{1, 2, 3\}$ . Next, consider the six functions

$$\begin{aligned}\varphi_1(x) &= x \\ \varphi_2(x) &= 1 - x \\ \varphi_3(x) &= \frac{1}{x} \\ \varphi_4(x) &= \frac{x-1}{x} \\ \varphi_5(x) &= \frac{1}{1-x} \\ \varphi_6(x) &= \frac{x}{x-1}\end{aligned}$$

Observe that

$$\begin{aligned}\varphi_2(\varphi_3(x)) &= 1 - \frac{1}{x} = \frac{x-1}{x} \\ \varphi_4(\varphi_4(x)) &= \frac{1}{1-x} = \varphi_5(x) \\ \varphi_4(\varphi_4(\varphi_4(x))) &= x = \varphi_1(x)\end{aligned}$$

**Theorem 1.1.2.**  $\varphi_1, \varphi_2, \dots, \varphi_6$  are closed under composition.

**Note 1.1.2.** There's a fact that:

$$\begin{aligned}&\text{operations preserving symmetry of triangle} \\ &\Leftrightarrow \text{permutations on } \{1, 2, 3\} \\ &\Leftrightarrow \text{compositions of } \varphi_1, \dots, \varphi_6\end{aligned}$$

Actually, below things are somewhere similar,

- Addition of integers,
- Addition of classes of integers  $\pmod{p}$ ,
- Operations on geometric shape,
- Permutation on letters,
- Composition of functions.

Since they are all binary operations.

**Definition 1.1.2 (Binary operations).** Suppose  $X$  is a set. Binary operation  $\star$  is a rule that allocates an element of  $X$  to a pair of elements of  $X$ .

**Example 1.1.1.**

- Addition on  $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  or vector spaces.
- Subtractions on  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  or vector spaces.
- A map  $X \rightarrow X$  (self map) with composition  $(\varphi_1 \star \varphi_2)(x) = \varphi_1(\varphi_2(x))$ .
- Set of subsets of  $\mathbb{R}$ . We can define
  - $(A, B) \mapsto A \cup B$
  - $(A, B) \mapsto A \cap B$

–  $(A, B) \mapsto A \setminus B$ .

- $n \times n$  real square matrices

$$(A, B) \mapsto A \cdot B.$$

**Definition (Special relations).** Suppose  $X$  is a set and  $*$  is a binary operation on  $X$ .

**Definition 1.1.3 (Associativity).**  $(a * b) * c = a * (b * c)$ .

**Definition 1.1.4 (Identity).**  $\exists e \in X$  s.t.  $a * e = e * a = a$  for all  $a \in X$ .

**Definition 1.1.5 (Inverse).**  $\forall a \in X, \exists a^{-1} \in X$  s.t.  $a * a^{-1} = a^{-1} * a = e$ .

**Definition 1.1.6 (Commutativity).**  $a * b = b * a$ .

**Definition 1.1.7.** Some names:

**Definition 1.1.8 (Semigroup).** Only has Associativity.

**Definition 1.1.9 (Monoid).** Only has Associativity and Identity.

**Definition 1.1.10 (Group).** Only has Associativity and Identity and Inverse.

**Definition 1.1.11 (Abelian Group).** Has all the 4 properties.

**Note 1.1.3.** Actually, in these algebra structure, we also need closure under operations.

## Lecture 2

Set is a collection of elements.

12 Sep. 13:20

**Example 1.1.2.** The set of natural numbers

$$\mathbb{N} = \{1, 2, 3, \dots\}$$

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$$

$$\mathbb{R} = \{\text{real numbers}\}$$

$$M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$$

$$GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}$$

The set of integers modulo 5 =  $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ , where  $\bar{i} = \{5k + i \mid k \in \mathbb{N} \cup \{0\}\}$ .

**Notation.** For a set  $X$ ,  $x \in X$  means that  $x$  is a member of  $X$ . For sets  $X, Y$ , a map  $f$  from  $X$  to  $Y$  means that  $f$  is a rule that assigns a member of  $Y$  to every member of  $X$ . It is commonly denoted as  $f : X \rightarrow Y$ . The assigned element of  $Y$  to  $x \in X$  is denoted as  $f(x)$ .  $X$  is said to be a subset of

$Y$  if all numbers of  $X$  are members of  $Y$ . It is denoted by  $X \subseteq Y$ . Sets are often denoted as

$$\{x \mid \text{conditions on } x\} \text{ or } \{x \in X \mid \text{extra conditions on } x\}$$

**Example 1.1.3.**  $(\mathbb{N}, +)$  is a semigroup, and  $(\mathbb{N} \cup \{0\}, +)$  is a monoid with identity 0, and  $(\mathbb{N}, \times)$  is a monoid with identity 1.

**Example 1.1.4.**  $(X, +)$  with  $X = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$  are abelian groups.  $(X, \cdot)$  with  $X = \mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}$  are abelian groups. Also,  $(\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, +)$  is an abelian group.

**Example 1.1.5.**  $S_n = \{\text{Permutations on } n \text{ letters}\}$  is a group, and non-abelian if  $n \geq 3$  and abelian if  $n = 1, 2$ .

**Example 1.1.6.** Suppose  $\text{GL}_n(\mathbb{R}) = \{\text{real invertible } n \times n \text{ matrices}\}$ , then  $(\text{GL}(\mathbb{R}), \cdot)$  is a non-abelian group for  $n \geq 2$ , and abelian for  $n = 1$ .

## 1.2 Basis Properties of Groups

**Theorem 1.2.1.** Suppose  $G = (G, *)$  is a group, then

1. Identity element is unique.
2. For  $g \in G$ ,  $g^{-1}$  is unique.
3. For  $g, h \in G$ , then  $(g * h)^{-1} = h^{-1} * g^{-1}$ .
4. For  $g \in G$ ,  $(g^{-1})^{-1} = g$ .

**Proof.**

1. Suppose  $e, e'$  are identities, i.e.

$$\begin{aligned} e * g &= g = g * e \\ e' * g &= g = g * e', \end{aligned}$$

then  $e = e * e' = e'$ .

2. Suppose  $h, h'$  such that

$$\begin{aligned} g * h &= h * g = e \\ h' * g &= g * h' = e. \end{aligned}$$

Then,

$$h' = e * h' = h * g * h' = h e = h.$$

3. Since the inverse is unique, it suffices to show that  $h^{-1}g^{-1}$  is the inverse of  $gh$ , so  $h^{-1}g^{-1} = (gh)^{-1}$ .
4. Trivial.

■

## Lecture 3



**As previously seen.**  $G = (G, *)$  is called a group if

- (1)  $(a * b) * c = a * (b * c)$
- (2)  $\exists e \in G$  s.t.  $a * e = a = e * a$ .
- (3) For  $a \in G$ ,  $\exists a^{-1} \in G$  s.t.  $a * a^{-1} = e = a^{-1} * a$ .

Also, we have shown that  $e$  is unique and for every  $a \in G$ ,  $a^{-1}$  is also unique.

**Definition 1.2.1 (Subgroup).** Suppose  $G = (G, *)$  is a group, and  $H \subseteq G$ , then  $H$  is called a subgroup if  $(H, *)$  is a group.

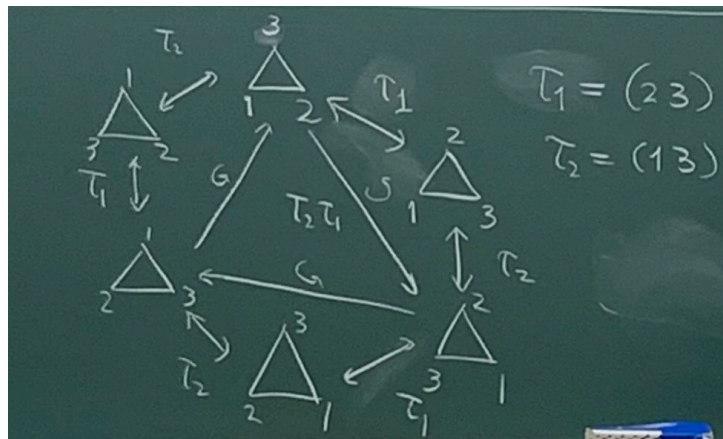


Figure 1.5: Traingle groups

**Example 1.2.1.** Consider the case when

$$G = \{\text{permutations on } \{1, 2, 3\}\} = S_3,$$

then what is the subgroup of  $G$ ?

**Proof.** Note that

$$G = \{id, \tau_1, \tau_2, \tau_1\tau_2\tau_1, \tau_1\tau_2, \tau_2, \tau_1\}.$$

Then,

$$H = \{id\}, \{id, \tau_1\}, \{id, \tau_2\}, \{id, \tau_1\tau_2\tau_1\}, \\ \{id, \tau_1\tau_2, \tau_2\tau_1\}, G$$

These 6 subgroups are all subgroups of  $G$ . In general, identity  $\{id\}$  and  $G$  itself are always subgroups. \*

**Note 1.2.1.** We will talk about Sylow's theorem later, which claims that if

$$|G| = p_1^{e_1} \dots p_r^{e_r},$$

then  $G$  has subgroups of order  $p_i^{e_i}$  for  $1 \leq i \leq r$ .

**Example 1.2.2.** If  $G = (\mathbb{Z}, +)$ , what is the subgroup of  $G$ ?

**Proof.** Suppose  $n \in H$ , then  $n + n = 2n \in H$ , and  $-n \in H$ , and then  $3n = 2n + n \in H$ . Hence, all

multiples of  $n \in H$ , which means  $n\mathbb{Z} \subseteq H$ . If  $n_1, \dots, n_r \in H$ , then

$$\underbrace{n_1\mathbb{Z} + n_2\mathbb{Z} + \dots + n_r\mathbb{Z}}_{d\mathbb{Z}} \subseteq H,$$

where  $d = \gcd(n_1, n_2, \dots, n_r)$ . Hence, the only subgroups are of the form  $d\mathbb{Z}$ . In particular,  $0\mathbb{Z} = \{0\}$ , which is the identity subgroup, and  $1\mathbb{Z} = \mathbb{Z}$  is  $G$  itself.  $\circledast$

**Example 1.2.3.** If  $G = \mathbb{R}^\times = (\mathbb{R} \setminus \{0\}, \times)$ , what are the finite subgroups of  $G$ ?

**Proof.** Consider  $H = \{1\}, \{1, -1\}$ , and these are all finite subgroups.  $\circledast$

**Example 1.2.4.** Suppose

$$G = \text{GL}_n(\mathbb{R}) = (\{n \times n \text{ invertible matrices}\}, \times),$$

then what are the subgroups?

**Proof.** Consider

$$\text{SL}_n(\mathbb{R}) = \{g \in \text{GL}_n(\mathbb{R}) \mid \det g = 1\},$$

then since  $\det g \det h = \det(gh)$ , so  $\text{SL}_n(\mathbb{R})$  is a subgroup. Also, consider the set of all diagonal  $n \times n$  real matrices, then it is also a subgroup of  $\text{GL}_n(\mathbb{R})$ .  $\circledast$

**Remark 1.2.1.** We define orthogonal subgroup to be the subgroup preserving distances. For example, suppose  $g \in \text{GL}_n(\mathbb{R})$ , and if we have norm here, then  $|gv| = |v|$  if and only if  $g^t g = I$ .

**Exercise 1.2.1.** Show that

$$O_n(\mathbb{R}) = \{g \in \text{GL}_n(\mathbb{R}) \mid g^t g = I\}$$

forms a subgroup of  $\text{GL}_n(\mathbb{R})$ .

## Lecture 4

As previously seen.

19 Sep. 13:20

- $\mathbb{Z} = (\mathbb{Z}, +)$  is a infinite cyclic group s.t. its subgroup is  $d\mathbb{Z}$  with all  $d = 0, 1, 2, \dots$
- $C_n = (\mathbb{Z}/n\mathbb{Z}, +)$  is a cyclic group of order  $n$ .

$$C_1 = \{1\}$$

$$C_2 = \{1, \sigma\} \text{ with } \sigma^2 = 1$$

$$C_3 = \{1, \sigma, \sigma^2\} \text{ with } \sigma^3 = 1.$$

$$C_4 = \{1, \sigma, \sigma^2, \sigma^3\} \text{ with } \sigma^4 = 1.$$

$$C_5 = \{1, \sigma, \sigma^2, \sigma^3, \sigma^4\} \text{ with } \sigma^5 = 1.$$

$$C_6 = \{1, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5\} \text{ with } \sigma^6 = 1.$$

Observe that the subgroups of  $C_n$  are of the form  $C_d$  with  $d \mid n$  (+ unique for each  $d$ ).

**Exercise 1.2.2.** Prove it.

- $S_n$ : the symmetric group of degree  $n$ .  $S_3 = \{1, \sigma, \sigma^2, \tau, \tau\sigma, \theta\sigma^2\}$ .

- $g \in O_n(\mathbb{R}) \Leftrightarrow \langle gv, gw \rangle = \langle v, w \rangle$ , where  $\langle v, w \rangle = v_1w_1 + v_2w_2 + \cdots + v_nw_n$ . Also,

$$\langle gv, gw \rangle = \langle v, w \rangle \Leftrightarrow \|gv\| = \|v\|.$$

Note that

$$SO_n(\mathbb{R}) = \{g \in O_n(\mathbb{R}) \mid \det g = 1\},$$

and

$$O_n(\mathbb{R}) = SO_n(\mathbb{R}) \cup \varepsilon SO_n(\mathbb{R})$$

where  $\varepsilon \in O_n(\mathbb{R})$  s.t.  $\det \varepsilon = -1$ .

- Suppose  $G, H$  are groups and

$$G \times H = \{(g, h) \mid g \in G, h \in H\},$$

then  $G \times H$  is a group since we can define

$$(g_1, h_1) * (g_2, h_2) = (g_1g_2, h_1h_2).$$

**Example 1.2.5.** Suppose

$$C_2 = \{1, \tau\} \text{ with } \tau^2 = 1$$

$$C_3 = \{1, \sigma, \sigma^2\} \text{ with } \sigma^3 = 1.$$

Then,

$$C_2 \times C_3 = \{(1, 1), (1, \sigma), (1, \sigma^2), (\tau, 1), (\tau, \sigma), (\tau, \sigma^2)\}.$$

Note that  $C_2 \times C_3$  is not  $S_3$  because  $S_3$  is not commutative and  $C_2 \times C_3$  is. What are the subgroups?

**Proof.**

$$(\tau, \sigma)^2 = (1, \sigma^2)$$

$$(\tau, \sigma)^3 = (\tau, 1)$$

$$(\tau, \sigma)^4 = (1, \sigma)$$

$$(\tau, \sigma)^5 = (\tau, \sigma^2)$$

$$(\tau, \sigma)^6 = (1, 1)$$

Letting  $\mu = (\tau, \sigma)$ , then we know that

$$C_2 \times C_3 = \{1, \mu, \mu^2, \mu^3, \mu^4, \mu^5\} \simeq C_6.$$

⊛

As groups,

$$\begin{aligned} S_3 &\simeq (\{f_1, f_2, f_3, f_4, f_5, f_6\}, \circ) \text{ where } f_1(x) = x, f_2(x) = 1 - x, f_3(x) = \frac{1}{x} \dots \\ &\simeq \text{symmetry of triangle} \\ &\simeq C_6 \end{aligned}$$

### 1.3 Group homomorphisms/isomorphisms

The idea of isomorphisms is: Suppose  $G, H$  are groups and  $\phi : G \rightarrow H$  is defined by  $g \mapsto \phi(g)$ . Now if  $g_1, g_2 \in G$ , we want that  $g_1g_2$  corresponds to  $\phi(g_1)\phi(g_2)$ . Hence, if we have  $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$ , then it would be a great property, and it seems that  $G, H$  have same structure. But, consider the map

$$\phi : G \rightarrow \{1\},$$

then this map satisfies  $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$ , but obviously  $G$  and  $\{1\}$  do not have same structure, so we have to give further restriction. Hence, we should restrict that

- Any two elements of  $G$  should not be mapped to the same element.

Hence, if we have a map from  $G$  to  $G \times H$  with

$$g \mapsto (g, 1),$$

then it also satisfies  $\phi(g_1 g_2) = \phi(g_1) \phi(g_2)$ . However, it is not enough, we need the surjection so that we can say any two isomorphic things have same structure.

- The image of  $\phi$  should cover  $H$ .

### Summary

- The first restriction  $\Leftrightarrow \forall g_1 \neq g_2 \in G$ , we must have  $\phi(g_1) \neq \phi(g_2)$ .
- The second restriction  $\Leftrightarrow \forall h \in H$ ,  $\exists g \in G$  s.t.  $h = \phi(g)$ .

**Definition 1.3.1.** A map  $\phi : G \rightarrow H$  is said to be a homomorphism if

$$\phi(g_1 g_2) = \phi(g_1) \phi(g_2)$$

for all  $g_1, g_2 \in G$ .

**Definition 1.3.2.** A homomorphism  $\phi : G \rightarrow H$  is said to be an isomorphism if  $\phi$  is said to be an isomorphism if it is injective and surjective.

**Definition 1.3.3 (Another definition of Isomorphism).** A map  $\phi : G \rightarrow H$  is an **isomorphism** if it is a group homomorphism that is also a bijection. An equivalent, and often more formal, definition is: Two groups  $G$  and  $H$  are said to be **isomorphic** ( $G \cong H$ ) if there exist two group homomorphisms,  $\phi : G \rightarrow H$  and  $\psi : H \rightarrow G$ , such that they are mutual inverses:

$$\begin{cases} \phi(g_1 g_2) = \phi(g_1) \phi(g_2) & \text{for } g_1, g_2 \in G \\ \psi(h_1 h_2) = \psi(h_1) \psi(h_2) & \text{for } h_1, h_2 \in H \end{cases}$$

AND

$$\begin{cases} \psi \circ \phi(g) = g & \text{for all } g \in G \\ \phi \circ \psi(h) = h & \text{for all } h \in H. \end{cases}$$

**Exercise 1.3.1.** Check that two definitions agree.

Note that  $(\mathbb{Z}/3\mathbb{Z}, +) \simeq C_3$ , and  $(\mathbb{Z}/3\mathbb{Z})^\times \simeq C_2 \simeq (\mathbb{Z}/2\mathbb{Z}, +)$ . Also,  $(\mathbb{Z}/5\mathbb{Z})^\times \simeq C_4 \simeq (\mathbb{Z}/4\mathbb{Z}, +)$ . Thus, more generally, we can see that

$$(\mathbb{Z}/p\mathbb{Z})^\times \simeq C_{p-1} \simeq (\mathbb{Z}/(p-1)\mathbb{Z}, +)$$

for all prime  $p$ .

**Example 1.3.1.**  $\exp : \mathbb{R} \rightarrow \mathbb{R}_{>0}$ . Note that it satisfies  $\exp(x + y) = \exp(x) \exp(y)$ . In terms of the group structure,  $\exp$  gives a group homomorphism

$$(\mathbb{R}, +) \rightarrow (\mathbb{R}_{>0}, \cdot)$$

## 1.4 Properties of homomorphism

**Definition 1.4.1.** Let  $\phi : G \rightarrow H$  to be a group homomorphism.

- $\ker \phi = \{g \in G \mid \phi(g) = 1\}$ , which can be used to measure how far it is from being injective.
- $\text{Im } \phi = \{\phi(g) \mid g \in G\}$ , which can be used to measure how far it is from being surjective.

### Summary

$$\begin{cases} \ker \phi = \{1\} \Leftrightarrow \phi \text{ is injective} \\ \text{Im } \phi = H \Leftrightarrow \phi \text{ is surjective.} \end{cases}$$

## Lecture 5

**As previously seen.** Group homomorphism means there exists  $\varphi : (G, *) \rightarrow (H, \circ)$  with

24 Sep. 13:20

$$\varphi(g_1 * g_2) = \varphi(g_1) \circ \varphi(g_2).$$

Thus, we have

$$\begin{cases} \varphi(1_G) = 1_H \\ \varphi(g^{-1}) = \varphi(g)^{-1} \end{cases}.$$

Group isomorphism means  $\varphi : G \rightarrow H$  is an homomorphism and there exists another group homomorphism  $\psi : H \rightarrow G$  s.t.

$$\begin{cases} \psi \circ \varphi : G \rightarrow G \\ \varphi \circ \psi : H \rightarrow H \end{cases}$$

are identity groups. Note that

- $\varphi$  is surjective if  $\varphi(G) = H$ .
- $\varphi$  is injective if  $\forall g_1 \neq g_2 \in G, \varphi(g_1) \neq \varphi(g_2)$ .

Also, we know

- surjective  $\Leftrightarrow \text{Im } \varphi = H$
- injective  $\Leftrightarrow \ker \varphi = \{1\}$ .

**why  $\ker \varphi = \{1\}$  means injective?** Suppose  $\varphi(g_1) = \varphi(g_2)$ , then

$$1_H = \varphi(g_1)^{-1} \varphi(g_1) = \varphi(g_1)^{-1} \varphi(g_2) = \varphi(g_1^{-1}) \varphi(g_2) = \varphi(g_1^{-1} g_2).$$

Hence, we have  $g_1^{-1} g_2 = 1_G$ , and thus  $g_1 = g_2$ . ■

**Theorem 1.4.1.** Let  $\varphi : G \rightarrow H$  be a group homomorphism, then  $\varphi$  is an isomorphism iff  $\ker \varphi = \{1\}$  and  $\text{Im } \varphi = H$ .

## 1.5 Equivalence relation

**Definition 1.5.1 (relation).** Let  $S$  be a set. A subset  $R \subseteq S \times S$  is called a relation.

**Example 1.5.1.** Suppose  $S = \{1, 2, 3, 4\}$ , then

$$R = \{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$$

is the relation  $<$ .

**Notation.**  $(a, b) \in R$  is commonly denoted as  $a \cdot b$  with some symbol  $\cdot$ .

**Definition 1.5.2 (Equivalence relation).** Let  $S$  be a set and  $\sim$  is a relation on  $S$ , then  $\sim$  is called an equivalence relation if it satisfies:

- Reflexive:  $x \sim x$
- Symmetric: If  $x \sim y$ , then  $y \sim x$ .
- Transitive: If  $x \sim y$  and  $y \sim z$ , then  $x \sim z$ .

**Definition 1.5.3 (Equivalence class).** Suppose  $S$  is a set and  $\sim$  is an equivalence relation on  $S$ . We define

$$C(x) = \{y \in S \mid x \sim y\}.$$

**Example 1.5.2.** Suppose  $S = \{1, 2, 3, 4, 5, 6\}$ , and  $x \sim y$  if  $x - y \in 3\mathbb{Z}$ , then  $\sim$  is an equivalence relation. List all the equivalence classes.

**Proof.**

$$\begin{aligned} C(1) &= C(4) = \{1, 4\} \\ C(2) &= C(5) = \{2, 5\} \\ C(3) &= C(6) = \{3, 6\}. \end{aligned}$$

⊛

**Theorem 1.5.1.**

- If  $y, z \in C(x)$ , then  $y \sim z$ .
- If  $y \in C(x)$ , then  $C(x) = C(y)$ .
- If  $C(x) \cap C(y) \neq \emptyset$ , then  $C(x) = C(y)$ .

## Lecture 6

**Definition 1.5.4 (Quotient Group).** Let  $G$  be a group and  $H \trianglelefteq G$  a normal subgroup. The *quotient group* of  $G$  by  $H$ , denoted  $G/H$ , is the set of left cosets of  $H$  in  $G$ :

$$G/H = \{gH : g \in G\}.$$

The group operation on  $G/H$  is defined by

$$(gH)(kH) = (gk)H, \quad \text{for all } g, k \in G.$$

This operation is well-defined because  $H$  is normal in  $G$ .

**Definition 1.5.5 (Quotient Set).** Let  $S$  be a set, and let  $\sim$  be an equivalence relation on  $S$ . Then, the quotient set is defined to be

$$S/\sim := \{\text{equivalence classes}\}$$

**Example 1.5.3.** Consider the set  $\{1, 2, \dots, 10\}$  and the relation is  $\equiv \pmod{2}$ , then

$$\{1, 2, \dots, 10\} / (\equiv \pmod{2}) = \{\{1, 3, 5, 7, 9\}, \{2, 4, 6, 8, 10\}\}.$$

26 Sep. 13:20

**Example 1.5.4.**

$$\mathbb{Z}/N\mathbb{Z} = \{\text{Congruence classes to } N\mathbb{Z} \text{ under the operation } \pmod{N}\}$$

**Definition 1.5.6 (Quotient map).** We say  $\pi : S \rightarrow S/n$  is a "quotient map" if  $\pi(x) = \bar{x}$ .

**Example 1.5.5.**  $\pi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ .

**Definition 1.5.7 (Representative elements).** Representative element is whatever element of an equivalence class.

**Definition 1.5.8 (Complete system of representative (CSR)).**  $R \subseteq S$  is called complete system of representative if  $R$  contains all elements that represent the quotient set without redundancy.

**Example 1.5.6.** For the quotient group  $\mathbb{Z}/N\mathbb{Z}$ , several complete systems of representatives are possible:

$$\{0, 1, \dots, N-1\}, \quad \{1, 2, \dots, N\}, \quad \{2N, 2N+1, \dots, 3N-1\}, \quad \text{etc.}$$

In general, any set of  $N$  consecutive integers forms a complete system of representatives.

**Example 1.5.7.**  $\{0, 1, 2, \dots, N\}$  is NOT a CSR because 0 and  $N$  are two representatives of the same class. Also,  $\{0, 2, 3, \dots, N\}$  is NOT a CSR because there no representative for  $1 + N\mathbb{Z}$ .

Now we talk about the quotient of group by an equivalence relation defined by its subgroup.

**Definition 1.5.9.** For a group  $G$  and its subgroup  $H$ , we define the set of all left cosets as

$$G/H := G/\sim$$

where  $g_1 \sim g_2$  if  $\exists h \in H$  s.t.  $g_1 = g_2 h$ . In the same way, the set of all right cosets is defined as

$$H \backslash G := G/\sim$$

where  $g_1 \sim g_2$  if  $\exists h \in H$  s.t.  $g_1 = h g_2$ .

We first need to check  $\sim$  is an equivalence relation on  $G$ .

- Reflexive:  $g = g \cdot 1_G$
- Symmetry:  $g_1 \sim g_2$  iff  $\exists h \in H$  s.t.  $g_1 = g_2 h$  and this holds if and only if  $\exists h' \in H$  s.t.  $g_2 = g_1 h'$ . Here  $h' = h^{-1}$  which exists because  $H$  is a subgroup.
- Transitivity: If  $g_1 \sim g_2$  and  $g_2 \sim g_3$ , then  $g_1 = g_2 h_1$  and  $g_2 = g_3 h_2$  for some  $h_1, h_2 \in H$ , then

$$g_1 = (g_3 h_2) h_1 = g_3 (h_2 h_1),$$

which shows  $g_1 \sim g_3$ .

Thus, we verifies the well-definedness of the quotient  $G/H$ , and similarly we can show  $H \backslash G$  is well-defined.

**Notation.** The element of  $G/H$  is commonly denoted as  $gH$ , and the right coset is denoted by  $Hg$ .

**Note 1.5.1.** If  $H$  is clear from the context, then  $gH$  may be denoted more simply as  $\bar{g}$ .

**Example 1.5.8.** If we have  $G = (\mathbb{Z}, +)$  and  $H = (N\mathbb{Z}, +)$ , then

$$G/H = \{0 + N\mathbb{Z}, 1 + N\mathbb{Z}, \dots, (N-1) + N\mathbb{Z}\}.$$

**Remark 1.5.1.** For a finite set  $S$ , we denote by  $|S| = \#$  of elements of  $S$ .

**Theorem 1.5.2.**

- $|G/H| = |H/G|$ .
- $|gH| = |Hg|$ .

given that the numbers are finite.

**Notation.**

$$|G/H| = |H \setminus G|$$

is called the index of  $H \subseteq G$ , and denoted as  $(G : H)$ .

**Theorem 1.5.3.**

$$|G| = (G : H) \cdot |H|.$$

**Corollary 1.5.1** (Lagrange's theorem). For any subgroup  $H$  of  $G$ ,  $H$  divides  $|G|$ .

**Example 1.5.9.** For a prime  $p$ ,

$$(\mathbb{Z}/p\mathbb{Z}) \setminus \{\bar{0}\} = \{\bar{1}, \bar{2}, \dots, \overline{p-1}\}$$

forms a (commutative) group by " $\cdot$ " (multiplication), where we called it  $(\mathbb{Z}/p\mathbb{Z})^\times$ . In this case, if we have a subgroup  $H \subseteq (\mathbb{Z}/p\mathbb{Z})^\times$ , then we have

$$|H| \mid |\mathbb{Z}/p\mathbb{Z}| = p - 1.$$

In particular, consider the subset

$$H = \{\bar{1}, \bar{2}, \bar{2}^2, \dots\},$$

then it forms a subgroup. Also, if  $r$  is the smallest positive integer s.t.  $\bar{2}^r = \bar{1}$ , then we know  $|H|$  is the period of  $2^n \bmod p$ , and thus this period divides  $p - 1$ .

## Lecture 7

**As previously seen.**

$$G/\sim = \{gH : g \in G\}.$$

Note that if  $g \in G$  belongs to a coset, then  $gh$  must belong to the same coset.

Note that

$$|G/H| = |H \setminus G|$$

since  $gH \leftrightarrow Hg^{-1}$  is a well-defined bijective map between these two sets. (since  $gh \leftrightarrow h^{-1}g$  is a bijective map).

**Theorem 1.5.4.** Suppose  $G$  is finite, then

$$|G| = [G : H] \cdot |H|,$$

1 Oct. 13:20



where  $[G : H] = |G/H|$ .

**Proof.** Consider the map  $H \rightarrow gH$  by  $h \mapsto gh$ , we say this map is  $\psi$ , then  $\psi$  is obviously surjective, and injectivity can be checked as follows: If  $\psi(h_1) = \psi(h_2)$ , then  $gh_1 = gh_2$ , and thus  $h_1 = h_2$ , which shows  $\psi$  is injective. Thus,  $\psi$  is bijective. Hence,  $|H| = |gH|$ . Now we know the number of cosets is  $[G : H]$ , and since we can partition  $G$  by the equivalence relation given by  $G/H$ , and thus we know  $|G| = [G : H] \cdot |H|$ . ■

**Proposition 1.5.1.** If  $|G|$  is a prime  $p$ , then  $G \simeq \mathbb{Z}/p\mathbb{Z}$  (cyclic subgroup of order  $p$ ).

**Proof.** Since  $|H|$  divides  $|G|$ , so  $H = \{1\}$  or  $G$ . Suppose  $G$  is not cyclic, then for  $g \in G$ , consider the subgroup generated by  $g$  i.e.

$$\langle g \rangle = \{ \dots, g^{-1}, 1, g, g^2, \dots \}.$$

Since  $\langle g \rangle \subseteq G$  and  $|G| < \infty$ , so  $\langle g \rangle$  is also finite, so there exists  $i > j \in \mathbb{Z}$  s.t.  $g^i = g^j$ , so  $g^{j-i} = 1$ . Thus, there exists  $N \in \mathbb{Z}_{>0}$  s.t.  $g^N = 1$ , pick the smallest such  $N$ , then

$$\langle g \rangle = \{1, g, \dots, g^{N-1}\} \simeq \mathbb{Z}/N\mathbb{Z},$$

which is a cyclic group. However, it is a subgroup of  $G$ , so  $\langle g \rangle = \{1\}$  or  $G$ . If  $\langle g \rangle = \{1\}$ , then  $o(g) = 1$ , which means  $g = 1$ . If  $g \neq 1$ , then  $\langle g \rangle = G$ , but it shows  $G$  is cyclic, which gives a contradiction. Hence,  $g = 1$  is the only element of  $G$ , but  $|G|$  is prime, so  $|G| > 1$ , and thus it is impossible. ■

## 1.6 Normal subgroups

**Question.** When does  $G/H$  admit a group structure (inherited from  $G$ ).

**Example 1.6.1.**  $G = (\mathbb{Z}, +)$  and  $H = (n\mathbb{Z}, +)$ , then

$$G/H = \{n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}\}.$$

In this case,  $G/H$  with addition naturally forms a group.

Hence, if we have  $g_1H$  and  $g_2H$ , then we want that  $(g_1g_2)H$  is the result of operating  $g_1H$  and  $g_2H$ . That is, for  $h_1, h_2 \in H$ , we want

$$g_1h_1 * g_2h_2 = (g_1g_2)h_3$$

for some  $h_3 \in H$ . Fix  $g_1, g_2$ , then for any  $h_1, h_2 \in H$  there must be  $h_3 \in H$  s.t. the equation holds. Note that

$$g_1h_1g_2h_2 = g_1g_2h_3 \Leftrightarrow h_1g_2h_2 = g_2h_3 \Leftrightarrow g_2^{-1}h_1g_2h_2 = h_3 \Leftrightarrow g_2^{-1}h_1g_2 = h_3h_2^{-1} \in H.$$

Thus, the requirement is that  $g^{-1}Hg \subseteq H$  for all  $g \in G$ , which means  $H \subseteq gHg^{-1}$  for all  $g \in G$ . This gives  $H \subseteq g^{-1}Hg$  by replacing  $g^{-1}$  with  $g$ . This gives  $g^{-1}Hg = H$ .

**Definition 1.6.1.** Suppose  $H \subseteq G$ ,  $H$  is called a normal subgroup if

$$g^{-1}Hg = H \quad \forall g \in G.$$

**Theorem 1.6.1.** The quotient  $G/H$  inherits the group structure of  $G$  if and only if  $H$  is a normal subgroup.

# Appendix