Introduction to Algebra I

Kon Yi

September 24, 2025

Abstract

The Introduction to Algebra course by professor 佐藤信夫.

Contents

1 Introduction **2**

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

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:

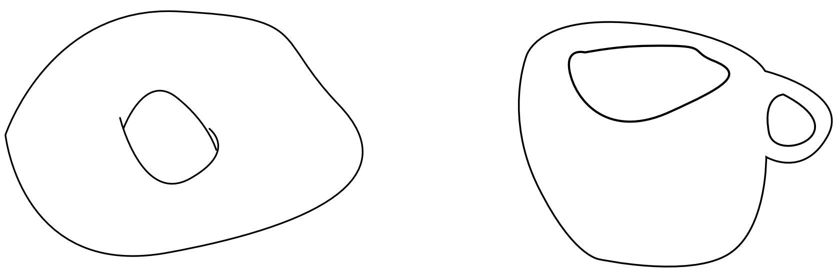

Figure 1.1: Fundamental Groups

- Physics/Chemistry: crystal symmetries and Gauge theory.

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

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

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

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.

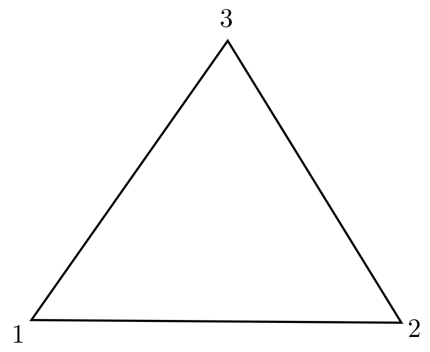

Figure 1.2: Triangle

Consider the rotation:

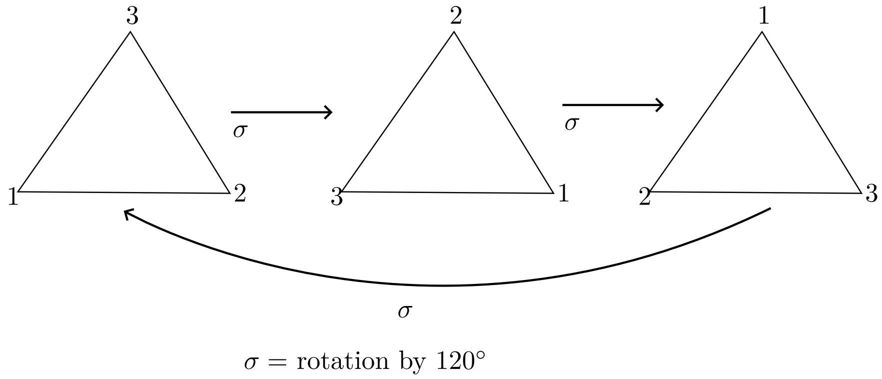

Figure 1.3: title

and reflection

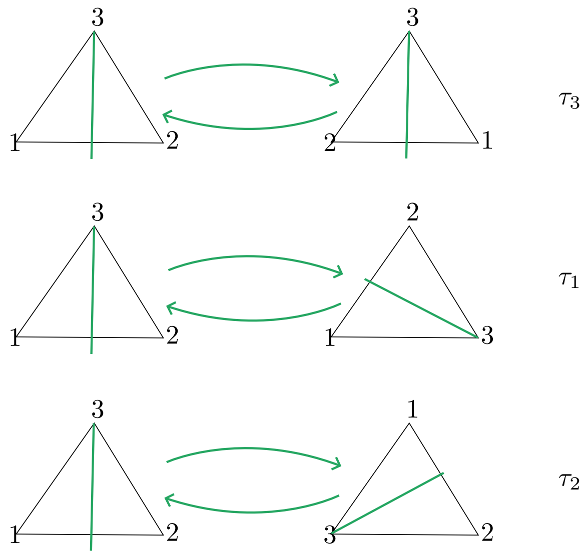

Figure 1.4: title

Hence, symmetrices 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

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

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 $\mod p$,
- 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 $X \to X$ (self map) with composition $\left(\varphi_1 \star \varphi_2\right)(x) = \varphi_1\left(\varphi_2(x)\right)$.
- 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 (Abedian Group). Has all the 4 properties.

Note 1.1.3. Actuallu, in these algebra structure, we also need clousre under operations.

Lecture 2

Set is a collection of elements. 12 Sep. 13:20

Example 1.1.2. The set of natural numbers

$$\begin{gathered}
\mathbb{N} = \{1, 2, 3, \dots\} \\
\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\} \\
\mathbb{R} = \{\text{real numbers}\} \\
M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\} \\
\mathrm{GL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\} \\
\text{The set of integers modulo } 5 = \left\{ \overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4} \right\}, \text{ where } \overline{i} = \{5k + i \mid k \in \mathbb{N} \cup \{0\}\}.
\end{gathered}$$

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 $f : X \to Y$. 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. $\mathcal{S}_n = \{\text{Permutations on } n \text{ letters}\}$ is a group, and non-abelian if $n \geq 3$ and abelian if $n = 1, 2$.

Example 1.1.6. Suppose $\mathrm{GL}_n(\mathbb{R}) = \{\text{real invertible } n \times n \text{matrices}\}$, then $(\mathrm{GL}(\mathbb{R}), \cdot)$ 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 $g \in G$, $\left(g^{-1}\right)^{-1} = g$.

Proof.

1. Suppose e, e' are identites, 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,
$$h' = e * h' = h * g * h' = he = h.$$
3. Since the inverse is unique, it sufficies to show that $h^{-1}g^{-1}$ is the inverse of gh, so $h^{-1}g^{-1} = (gh)^{-1}$.
4. Trivial.

■

Lecture 3

17 Sep. 13:20

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.

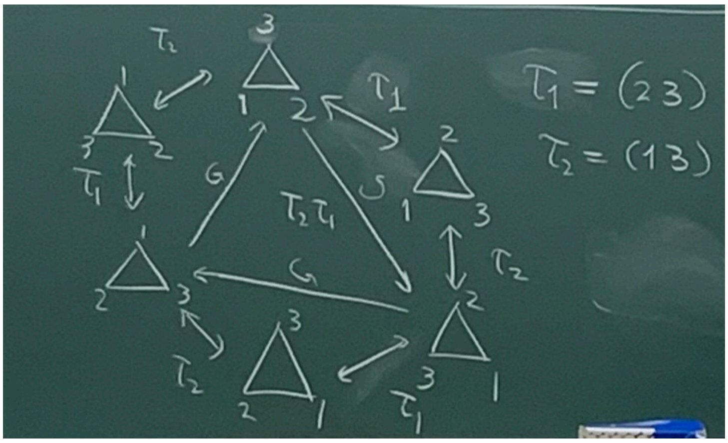

Figure 1.5: Traingle groups

Example 1.2.1. Consider the case when

$$G = \{\text{permutations on } \{1, 2, 3\}\} = \mathcal{S}_3,$$

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,

$$\begin{aligned} H = &\{id\}, \{id, \tau_1\}, \{id, \tau_2\}, \{id, \tau_1\tau_2\tau_1\}, \\ &\{id, \tau_1\tau_2, \tau_2\tau_1\}, G \end{aligned}$$

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 $n_1, \ldots, n_r \in H$, then

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

where $d = \gcd(n_1, n_2, \ldots, n_r)$. 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. ⊛

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. ⊛

Example 1.2.4. Suppose

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

then what are the subgroups?

Proof. Consider

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

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

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

Exercise 1.2.1. Show that

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

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

Lecture 4

19 Sep. 13:20

As previously seen.

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

$$\begin{aligned}
C_1 &= \{1\} \\
C_2 &= \{1, \sigma\} \text{ with } \sigma^2 = 1 \\
C_3 &= \left\{1, \sigma, \sigma^2\right\} \text{ with } \sigma^3 = 1. \\
C_4 &= \left\{1, \sigma, \sigma^2, \sigma^3\right\} \text{ with } \sigma^4 = 1. \\
C_5 &= \left\{1, \sigma, \sigma^2, \sigma^3, \sigma^4\right\} \text{ with } \sigma^5 = 1. \\
C_6 &= \left\{1, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5\right\} \text{ with } \sigma^6 = 1.
\end{aligned}$$

  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. $S_3 = \left\{1, \sigma, \sigma^2, \tau, \tau\sigma, \theta\sigma^2\right\}$.

- $g \in O_n(\mathbb{R}) \Leftrightarrow \langle gv, gw \rangle = \langle v, w \rangle$, 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
$$\mathrm{SO}_n(\mathbb{R}) = \{g \in O_n(\mathbb{R}) \mid \det g = 1\},$$
and
$$\mathrm{O}_n(\mathbb{R}) = \mathrm{SO}_n(\mathbb{R}) \cup \varepsilon \mathrm{SO}_n(\mathbb{R})$$
where $\varepsilon \in \mathrm{O}_n(\mathbb{R})$ 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
$$\begin{aligned} C_2 &= \{1, \tau\} \text{ with } \tau^2 = 1 \\ C_3 &= \left\{1, \sigma, \sigma^2\right\} \text{ with } \sigma^3 = 1. \end{aligned}$$
Then,
$$C_2 \times C_3 = \left\{(1,1), (1,\sigma), (1,\sigma^2), (\tau,1), (\tau,\sigma), (\tau,\sigma^2)\right\}.$$
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 is the subgroups?

Proof.
$$\begin{aligned} (\tau,\sigma)^2 &= (1,\sigma^2) \\ (\tau,\sigma)^3 &= (\tau,1) \\ (\tau,\sigma)^4 &= (1,\sigma) \\ (\tau,\sigma)^5 &= (\tau,\sigma^2) \\ (\tau,\sigma)^6 &= (1,1) \end{aligned}$$
Letting $\mu = (\tau, \sigma)$, then we know that
$$C_2 \times C_3 = \left\{1, \mu, \mu^2, \mu^3, \mu^4, \mu^5\right\} \simeq C_6.$$
⊛

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

1.3 Group homomorphisms/isomorphisms

The idea of isomorphisms is: Suppose G, H are groups and $\phi : G \to H$ 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
$$\phi : G \to \{1\},$$
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 ϕ 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 $\phi : G \to H$ 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 $\phi : G \to H$ is said to be an isomorphism if ϕ is said to be an isomorphism if it is injective and surjective.

Definition 1.3.3 (Another definition of homomorphism)**.**

$$\left.\begin{array}{l}\exists\phi : G \to H \\ \exists\psi : H \to G\end{array}\right\} \text{(group) homomorphism}$$

i.e.

$$\begin{cases}\phi(g_1 g_2) = \phi(g_1)\phi(g_2) \ (g_1, g_2 \in G) \\ \psi(h_1 h_2) = \psi(h_1)\psi(h_2) \ (h_1, h_2 \in H)\end{cases} + \begin{cases}\psi \circ \phi(g) = g \text{ for } g \in G \\ \phi \circ \psi(h) = h \text{ for } h \in H.\end{cases}$$

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

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

1.4 Properties of homomorphism

Definition 1.4.1. Let $\phi : G \to H$ 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.
- $\operatorname{Im} \phi = \{\phi(g) \mid g \in G\}$, which can be used to measure how far it is from being surjective.

Summary

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

Lecture 5

24 Sep. 13:20

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

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

Thus, we have

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

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

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

are identity groups. Note that

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

Also, we know

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

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

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

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

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

1.5 Equivalenec 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 $C(x) \cap C(y) \neq \varnothing$, then $C(x) = C(y)$.

Appendix