Introduction to Algebra I

Kon Yi

October 3, 2025

Abstract

The Introduction to Algebra course by professor 佐藤信夫.

Contents

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:

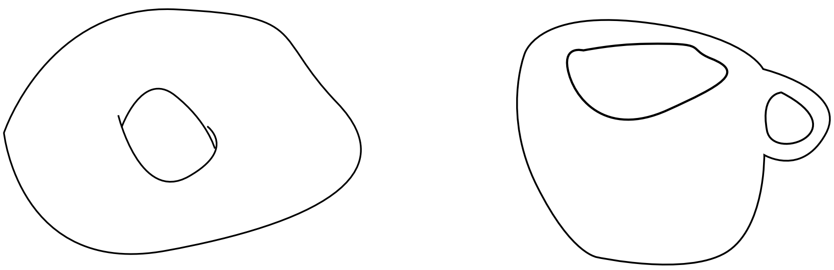


Figure 1.1: Fundamental Groups

- 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.

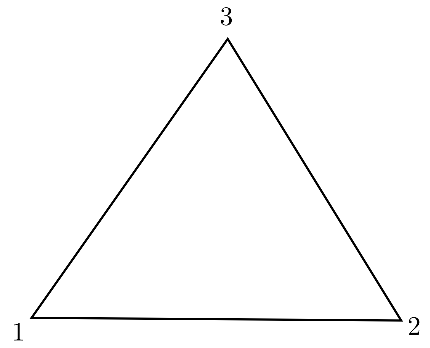
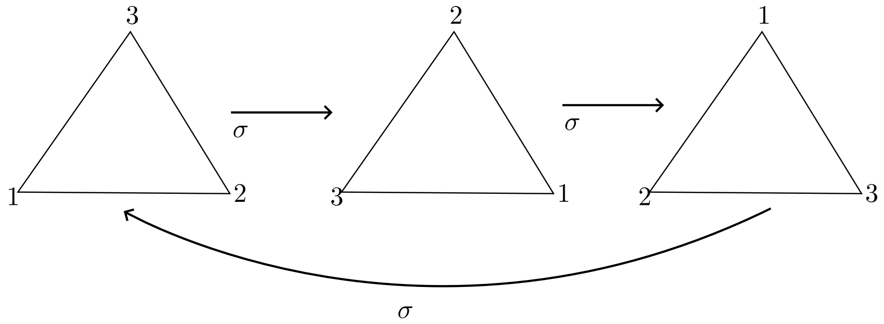


Figure 1.2: Triangle

Consider the rotation:



σ = rotation by 120°

Figure 1.3: title

and reflection

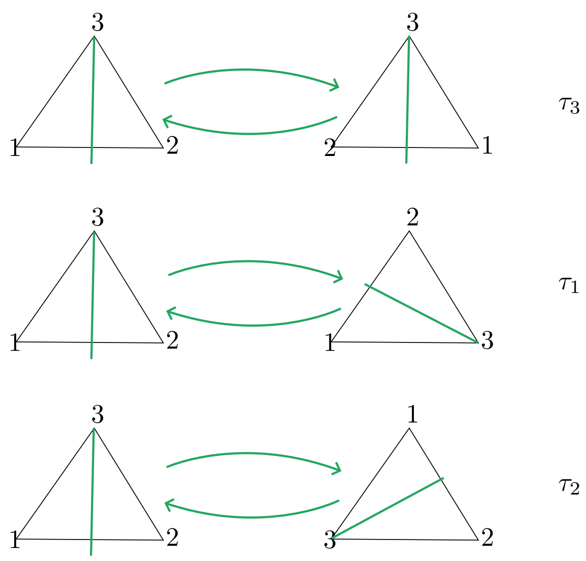


Figure 1.4: title

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. $\varphi_1, \varphi_2, \ldots, \varphi_6$ are closed under composition.

Note 1.1.2. There's a fact that:

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

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 $(\varphi_1 \star \varphi_2)(x) = \varphi_1(\varphi_2(x))$.
- 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 (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

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

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 $f : X \to Y$. 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.

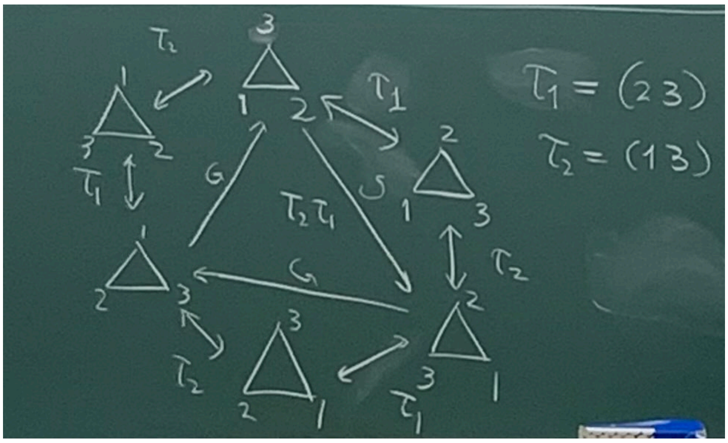


Figure 1.5: Traingle groups

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 $1 \le i \le r$.

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 Isomorphism)**.** A map $\phi : G \to H$ 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, $\phi : G \to H$ and $\psi : H \to G$, 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. $\exp : \mathbb{R} \to \mathbb{R}_{>0}$.. 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 $g_1 = g_2$. ■

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 $C(x) = C(y)$.

Lecture 6

26 Sep. 13:20

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 $\{1, 2, \ldots, 10\}$ and the relation is $\equiv \mod 2$, then

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

Example 1.5.4.

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

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

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

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:

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

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

Example 1.5.7. $\{0, 1, 2, \ldots, N\}$ is NOT a CSR because 0 and N are two representatives of the same class. Also, $\{0, 2, 3, \ldots, N\}$ 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

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

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 $H \setminus G$ 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 $\overline{g}$.

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,

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

forms a (commutative) group by "$\cdot$"(multiplicaiton), 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

$$H = \left\{\overline{1}, \overline{2}, \overline{2^2}, \dots\right\},$$

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

Lecture 7

1 Oct. 13:20

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

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

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

Proof. Consider the map $H \to gH$ by $h \mapsto gh$, we say this map is ψ, then ψ 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 ψ is injective. Thus, ψ 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.

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

Since $\langle g \rangle \subseteq G$ and $|G| < \infty$, so $\langle g \rangle$ is also finite, so there eixsts $i > j \in \mathbb{Z}$ 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

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

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.

Lecture 8

3 Oct. 13:20

As previously seen. We want to solve a question: For what $H < G$, does G/H form a group by

$$(g_1H)(g_2H) = (g_1g_2)H.$$

Note 1.6.1. $g^{-1}Hg = H$ for all $g \in G$ iff $\forall g \in G$ and $h \in H$, $g^{-1}hg \in H$.

We have the answer is Theorem 1.6.1.

Example 1.6.2. If G is abelian, then every subgroup is normal.

Proof. Let $H < G$ and $h \in H$, $g \in G$, then $g^{-1}hg = g^{-1}gh = h \in H$, so $H \trianglelefteq G$. ⊛

Example 1.6.3. If $G = S_3$, show that $V_3 = \{(1), (123), (132)\}$ form a normal subgroup, where

$$\{(1), (12)\}, \ \{(1), (13)\}, \ \{(1), (23)\}$$

are not normal subgroups.

Example 1.6.4. If $G = \mathrm{GL}_n(\mathbb{R}) = \{\text{invertible } n \times n \text{ real matrices}\}$, then

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

forms a normal subgroup of G.

Proof. It is enough to show

$$\forall g \in G, h \in H \Rightarrow g^{-1}hg \in H.$$

Since $h \in SL_n(\mathbb{R})$ and $\det h = 1$, then

$$\det\left(g^{-1}hg\right) = \det\left(g^{-1}\right)\det(h)\det(g) = \det\left(g^{-1}g\right)\det(h) = 1 \cdot 1 = 1.$$

Thus, $g^{-1}hg \in H$, and thus $H \trianglelefteq G$. ⊛

Example 1.6.5 (First isomorphism theorem). Let $\phi : G \to H$ be a group homomorphism, then

(1) $\operatorname{Im}\phi < H$.

(2) $\ker\phi \trianglelefteq G$.

(3) $G/\ker\phi \simeq \operatorname{Im}\phi$.

Proof.

(1) Enough to show

 (i) For $h_1, h_2 \in \operatorname{Im}\phi$, $h_1 \cdot h_2 \in \operatorname{Im}\phi$.
 (ii) $\forall h \in \operatorname{Im}\phi$, $h^{-1} \in \phi$.

 For (i), $\exists g_1, g_2 \in G$ s.t. $h_1 = \phi(g_1)$ and $h_2 = \phi(g_2)$, then $h_1h_2 = \phi(g_1)\phi(g_2) = \phi(g_1g_2)$, so $h_1h_2 \in \operatorname{Im}\phi$. For (ii), for $h \in H$, $\exists g \in G$ s.t. $h = \phi(g)$, so

$$h^{-1} = \phi(g)^{-1} = \phi(g^{-1}) \in \operatorname{Im}\phi.$$

(2) Enough to show

 (i) $\ker\phi < G$

(ii) $g \in G, h \in \ker \phi$, $g^{-1}hg \in \ker \phi$.

We first show (i). Let $g_1, g_2 \in \ker \phi$, then $\phi(g_1) = \phi(g_2) = 1$. Thus, $\phi(g_1 g_2) = \phi(g_1)\phi(g_2) = 1$, and thus $g_1 g_2 \in \ker \phi$. Now for $g \in \ker \phi$, we have $\phi(g) = 1$. Thus, $\phi\left(g^{-1}\right) = \phi(g)^{-1} = e_H^{-1} = e_H$, so $g^{-1} \in \ker \phi$. Now we show (ii). Let $g \in G$ and $h \in \ker \phi$, then $\phi(h) = 1$. Now since

$$\phi\left(g^{-1}hg\right) = \phi\left(g^{-1}\right)\phi(h)\phi(g) = \phi\left(gg^{-1}\right)\phi(h) = 1 * 1 = 1,$$

so $g^{-1}hg \in \ker \phi$.

(3) Let $N = \ker \phi$, and note that the map we want is something like $g \mapsto \phi(g)$. We can think of decomposing ϕ to

$$\underbrace{G \to G/\ker(\phi)}_{\text{surj}} \to \underbrace{\operatorname{Im}\phi \to H}_{\text{inj}}.$$
$$g \mapsto \overline{g} \mapsto \phi(g) \mapsto \phi(g),$$

where the $G/\ker(\phi) \to \operatorname{Im}(\phi)$ part is an isomorphism, adn we call it $\widetilde{\phi} : G/\ker \phi \to \operatorname{Im}\phi$. We have to show that the map is well-defined first, suppose

$$\overline{g} = \{g_1, g_2, g_3, \dots\},$$

then we want to show $\phi(g_1) = \phi(g_2) = \phi(g_3)$. More precisedly, we have to check that if $g_1 N = g_2 N$, then $\phi(g_1) = \phi(g_2)$. Since $g_1 N = g_2 N$, so $g_2 = g_1 N$ for some $n \in N$. Thus,

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

Thus, the map is well-defined. Then, we have to show that the $\overline{g} \mapsto \phi(g)$ part is bijective and it is an homomorphism. For surjectivity. Let $h \in \operatorname{Im}\phi$, then $\exists g \in G$ s.t. $h = \phi(g)$. By well-definedness of $\widetilde{\phi}$, we know $h = \widetilde{\phi}(gN) \in \operatorname{Im}\widetilde{\phi}$. Next we show the injectivity. Assuming the homomorphy of $\widetilde{\phi}$, it is enough to show $\ker \widetilde{\phi} = \left\{\overline{1}\right\} = \overline{N} \in G/N$. Hence, we want to show that if $gN \in \ker \widetilde{\phi}$, then $gN = N$. Suppose $gN \in \ker \widetilde{\phi}$, then $\phi(g) = \widetilde{\phi}(gN) = 1$. Thus, $g \in \ker \phi = N$. Hence, $gN = N$. (Since $g^{-1} \in \ker \phi$) Next, we show the homomorphy:

$$\widetilde{\phi}(g_1 N * g_2 N) = \widetilde{\phi}((g_1 * g_2)N) = \phi(g_1 * g_2) = \phi(g_1)\phi(g_2) = \widetilde{\phi}(g_1 N)\widetilde{\phi}(g_2 N)$$

since N is normal, so $\widetilde{\phi}$ is an homomorphism.

Combining the well-definedness, surjectivity, injectivity, and group homomorphism, we know $\widetilde{\phi}$ is an isomorphism.

⊛

Example 1.6.6. Consider

$$\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^{\times} \left(= \left(\mathbb{R} \setminus \{0\}\right), \cdot\right),$$

then $\operatorname{Im}\phi = \mathbb{R}^{\times}$, and $\ker \phi = \{g \in \mathrm{GL}_n(\mathbb{R}) \mid \det(g) = 1\}$. Hence,

$$G/\ker \phi = \mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) = \{g \cdot \mathrm{SL}_n(\mathbb{R}) \mid g \in \mathrm{GL}_n(\mathbb{R})\},$$

which means each equivalence class contains matrices with same determinant, and it is isomorphic to $\mathbb{R}^{\times}$.

1.7 Direct Product (= Cartesian Product)

Proposition 1.7.1. *Let G be a group and $H, K \trianglelefteq G$ s.t. $H \cap K = \{1\}$, then for $h \in H$ and $k \in K$, $hk = kh$.*

Proof. The goal is $hk = kh$, which means $h^{-1}k^{-1}hk = 1$. Note that $h^{-1}k^{-1}h \in K$ and $k \in K$, so $h^{-1}k^{-1}hk \in K$. Also, $h^{-1} \in H$ and $k^{-1}hk \in H$, so $h^{-1}k^{-1}hk \in H$. Hence, $h^{-1}k^{-1}hk \in H \cap K = \{1\}$. ■

Proposition 1.7.2. Suppose $H, K \trianglelefteq G$ satisfy

$$\begin{cases} H \cap K = \{1\} \\ H \cdot K = \{h \cdot k \mid h \in H, k \in K\} = G, \end{cases}$$

then

$$\begin{aligned} \phi : H \times K &\to G \\ (h, k) &\mapsto hk \end{aligned}$$

is an isomorphism. Note that in $H \times K$, for $(h_1, k_1), (h_2, k_2) \in H \times K$, we have

$$(h_1, k_1) \cdot (h_2, k_2) = (h_1h_2, k_1k_2).$$

Proof.

(1) Homomorphy: Let $(h_1, k_1), (h_2, k_2) \in H \times K$, then

$$\phi\left((h_1, k_1) \cdot (h_2, k_2)\right) = \phi((h_1h_2, k_1k_2)) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = \phi(h_1k_1)\phi(h_2k_2)$$

by Proposition 1.7.1.

(2) Surjectivity: Trivial.

(3) Injectivity: Need to show $\ker \phi = \{1\}$. Let $(h, k) \in \ker \phi$, then $hk = 1$. Thus, $h = k^{-1} \in K$, and $h \in H$, so $h \in H \cap K = \{1\}$, so $h = k = 1$.

By (1), (2), (3), we know ϕ is an isomorphism. ■

Theorem 1.7.1. If $(m, n) = 1$, then

$$\mathbb{Z}/(mn)\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Appendix