Introduction to Algebra I

Kon Yi

September 17, 2025

Abstract

The Introduction to Algebra course by professor 佐藤信夫.

Contents

Chapter 1

Introduction

Lecture 1

1.1 Why study groups?

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:

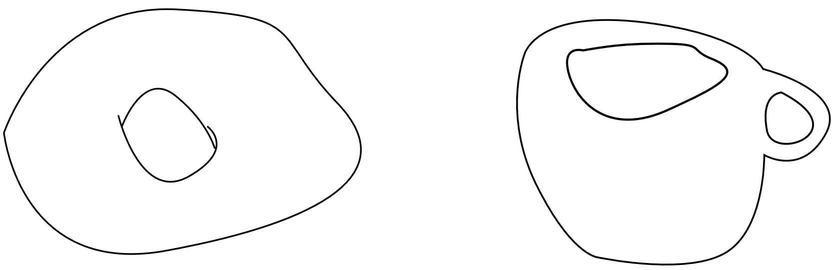


Figure 1.1: Fundamental Groups

- 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.

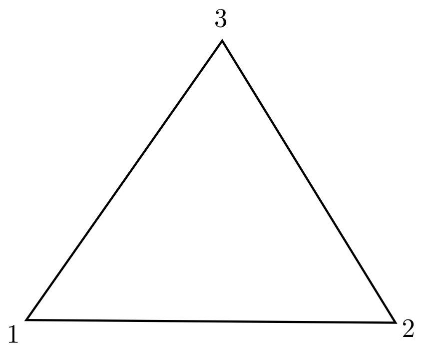
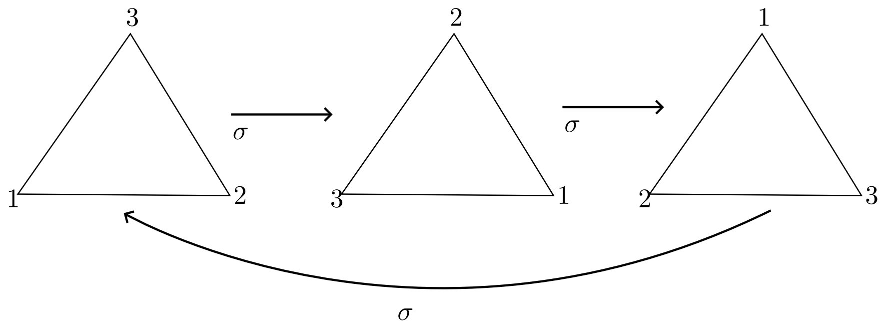


Figure 1.2: Triangle

Consider the rotation:



σ = rotation by 120°

Figure 1.3: title

and reflection

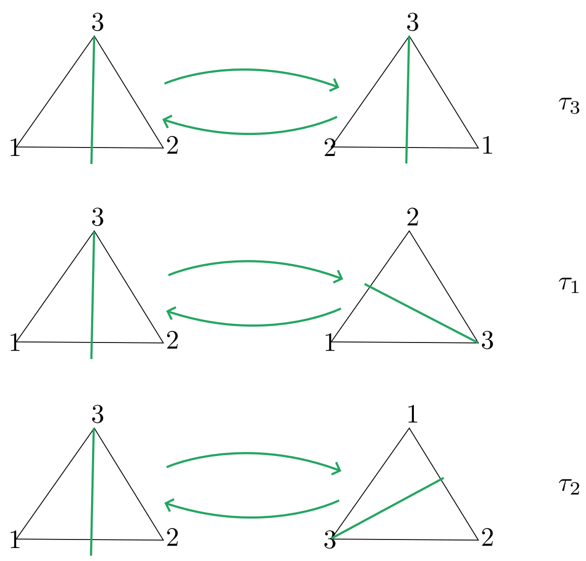


Figure 1.4: title

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

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

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

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.

■

Appendix