Introduction to Algebra I

Kon Yi

November 7, 2025

Abstract

The Introduction to Algebra course by professor 佐藤信夫.

Contents

Chapter 1

I don't know how to parse different chapters

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).
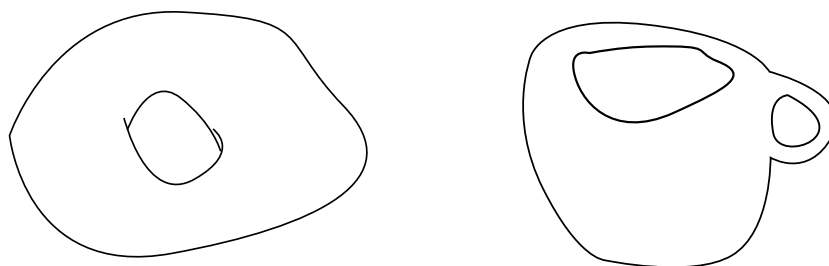
- Topology:

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

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

- $p = 7$: $\overgroup{1, 2, 4}, \overgroup{1, 2, 4}, \ldots$

> **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.
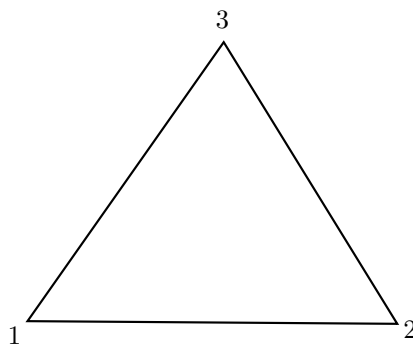
Consider the symmetry of a triangle.

Figure 1.2: Triangle

Consider the rotation:

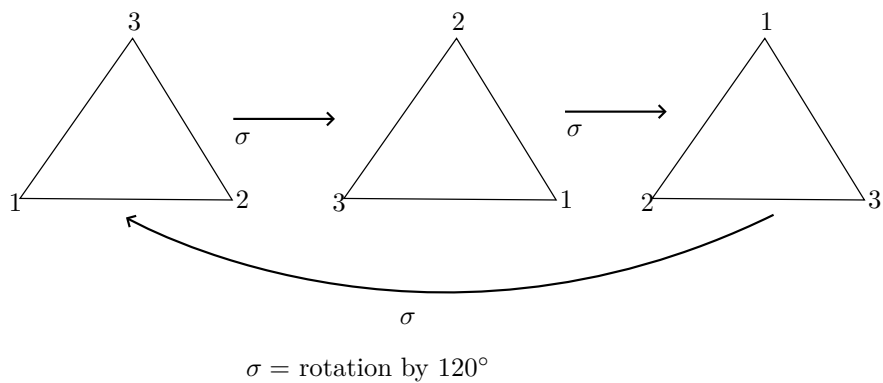

$\sigma = $ rotation by $120°$
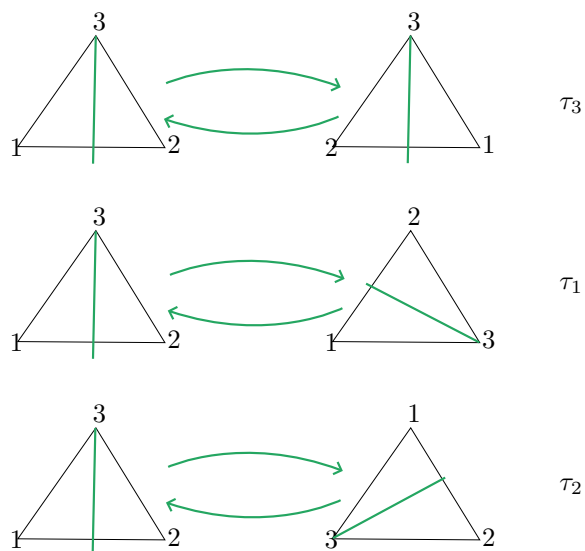
Figure 1.3: title

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

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

Observe that

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

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

Note 1.1.2. There's a fact that:

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

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.** Actually, 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. Different sets:

$$\mathbb{N} = \{1, 2, 3, \dots\}$$
$$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$$
$$\mathbb{R} = \{\text{real numbers}\}$$
$$M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$$
$$\mathrm{GL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}$$

The set of integers modulo $5 = \left\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\right\}$, 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, $(\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, +)$ 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.

$$e * g = g = g * e$$
$$e' * g = g = g * e',$$

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

2. Suppose h, h' such that

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

Then,

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

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   17 Sep. 13:20

(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.
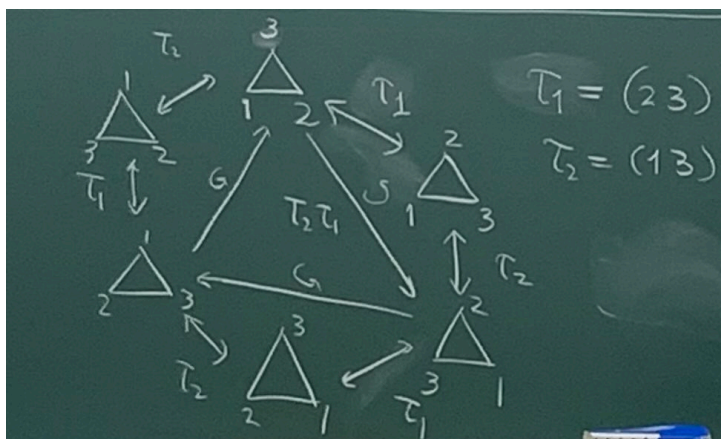

Figure 1.5: Traingle groups

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,

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

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 $1 \le i \le r$.

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 $n_1, \dots, n_r \in H$, 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. ⊛

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

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

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

- $g \in O_n(\mathbb{R}) \Leftrightarrow \langle gv, gw \rangle = \langle v, w \rangle$, where $\langle v, w \rangle = v_1 w_1 + v_2 w_2 + \cdots + v_n w_n$. 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
$$O_n(\mathbb{R}) = \mathrm{SO}_n(\mathbb{R}) \cup \varepsilon\mathrm{SO}_n(\mathbb{R})$$

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

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

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 isomorphic to S_3 because S_3 is not commutative and $C_2 \times C_3$ is. What is 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,

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

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 $g_1 g_2$ corresponds to $\phi(g_1)\phi(g_2)$. Hence, if we have $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$, 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 $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$, 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.

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

Summary

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

Lecture 5

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

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

24 Sep. 13:20

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 $\Leftrightarrow \mathrm{Im}\,\varphi = H$

- 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.

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

⊛

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

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

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 verify 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

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

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

Theorem 1.5.2.

- $|G/H| = |H \backslash G|$.

- $|gH| = |Hg|$.

given that the numbers are finite.

Proof. We first show that $|G/H| = |H \backslash G|$. We define a map $\varphi(gH) = Hg^{-1}$, we will show that it is well-defined and bijective, so we can conclude that $|G/H| = |H \backslash G|$. Suppose $g_1 H = g_2 H$, we now show that $\varphi(g_1 H) = \varphi(g_2 H)$, which is equivalent to show that $Hg_1^{-1} = Hg_2^{-1}$. Since we have $g_1 = g_2 h$ for some $h \in H$, so $g_2^{-1} = hg_1^{-1} \in Hg_1^{-1}$, so for all $h_2 \in H$, we have $h_2 g_2^{-1} = h_2 hg_1^{-1} \in Hg_1^{-1}$, which means $Hg_2^{-1} \subseteq Hg_1^{-1}$, and similarly we can show $Hg_1^{-1} \subseteq Hg_2^{-1}$, and this means $Hg_1^{-1} = Hg_2^{-1}$. Now we show that φ is bijective. Suppose $\varphi(g_1 H) = \varphi(g_2 H)$, we want to show that $g_1 H = g_2 H$. This means $Hg_1^{-1} = Hg_2^{-1}$ and we want to show $g_1 H = g_2 H$, and this can be proved by the same method above. Also, surjectivity is trivial.

Now we show that $|gH| = |Hg|$. We can build a map $\phi : gH \to H$ by $\phi(gh) = h$, then this is a well-defined bijective map (easy to show), so $|gH| = |H|$, and we can similarly show $|Hg| = |H|$, and we're done. ∎

Notation.

$$|G/H| = |H \backslash G|$$

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,

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

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

$$|H| \mid \left|(\mathbb{Z}/p\mathbb{Z})^\times\right| = p - 1.$$

In particular, consider the subset

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

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

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 $gh \leftrightarrow hg^{-1}$ 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 $|G| = [G : H] \cdot |H|$. $\blacksquare$

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

Proof. Suppose H is a subgroup of G. 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.

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

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

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

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. $\blacksquare$

Note 1.5.2. If $G \simeq \mathbb{Z}/p\mathbb{Z}$ for some $\mathbb{Z}$, then G is cyclic. This is because $G \simeq \mathbb{Z}/p\mathbb{Z}$ means there exists an isomorphism $\phi : \mathbb{Z}/p\mathbb{Z} \to G$, and since $\langle 1 \rangle = \mathbb{Z}/p\mathbb{Z}$, so we have $G = \langle \phi(1) \rangle$.

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

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

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

Hence, if we have $g_1 H$ and $g_2 H$, then we want that $(g_1 g_2)H$ is the result of operating $g_1 H$ and $g_2 H$. That is, for $h_1, h_2 \in H$, we want

$$g_1 h_1 * g_2 h_2 = (g_1 g_2) h_3$$

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

$$g_1 h_1 g_2 h_2 = g_1 g_2 h_3 \Leftrightarrow h_1 g_2 h_2 = g_2 h_3 \Leftrightarrow g_2^{-1} h_1 g_2 h_2 = h_3 \Leftrightarrow g_2^{-1} h_1 g_2 = h_3 h_2^{-1} \in H.$$

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

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

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

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

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

$$(g_1 H)(g_2 H) = (g_1 g_2) H.$$

3 Oct. 13:20

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

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 $g^{-1} h g = g^{-1} g h = h \in H$, 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 $G = \mathrm{GL}_n(\mathbb{R}) = \{$invertible $n \times n$ 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 $H \trianglelefteq G$. $\circledast$

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

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

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

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

Proof.

(1) Enough to show

    (i) For $h_1, h_2 \in \mathrm{Im}\,\phi$, $h_1 \cdot h_2 \in \mathrm{Im}\,\phi$.

    (ii) $\forall h \in \mathrm{Im}\,\phi$, $h^{-1} \in \mathrm{Im}\,\phi$.

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

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

(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

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

$$g \mapsto \overline{g} \mapsto \phi(g) \mapsto \phi(g),$$

    where the $G/\ker(\phi) \to \mathrm{Im}(\phi)$ part is an isomorphism, and we call it $\widetilde{\phi} : G/\ker\phi \to \mathrm{Im}\,\phi$. 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 $\ker\widetilde{\phi} = \{\overline{1}\} = \overline{N} \in G/N$. 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.

$$\circledast$$

Example 1.6.6. Consider
$$\det : \operatorname{GL}_n(\mathbb{R}) \to \mathbb{R}^\times \left(= (\mathbb{R} \setminus \{0\}), \cdot\right),$$
then $\operatorname{Im}\phi = \mathbb{R}^\times$, and $\ker\phi = \{g \in \operatorname{GL}_n(\mathbb{R}) \mid \det(g) = 1\}$. Hence,

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

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

$$\phi : H \times K \to G$$
$$(h, k) \mapsto hk$$

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

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

Proof.

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

$$\phi\left((h_1, k_1) \cdot (h_2, k_2)\right) = \phi((h_1 h_2, k_1 k_2)) = h_1 h_2 k_1 k_2 = h_1 k_1 h_2 k_2 = \phi(h_1 k_1)\phi(h_2 k_2)$$

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

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

Lecture 9

Theorem 1.7.2. Let m, n be coprime integers, then

$$\phi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

with $a + mn\mathbb{Z} \mapsto (a + m\mathbb{Z}, a + n\mathbb{Z})$ is an isomorphism.

8 Oct. 13:20

Example 1.7.1. $m = 2, n = 3$

$\mathbb{Z}/6\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
$\overline{0}$	$(\overline{0}, \overline{0})$
$\overline{1}$	$(\overline{1}, \overline{1})$
$\overline{2}$	$(\overline{0}, \overline{2})$
$\overline{3}$	$(\overline{1}, \overline{0})$
$\overline{4}$	$(\overline{0}, \overline{1})$
$\overline{5}$	$(\overline{1}, \overline{2})$

Table 1.1: The case $m = 2, n = 3$

proof of Theorem 1.7.2. We have to show injectivity, surjectivity, and homomorphism. Note that if we have $|G| = |H|$, then injectivity is equivalent to surjectivity since surjectivity gives $|G| \geq |H|$ and injectivity gives $|H| \geq |G|$. (Suppose the map is $G \to H$) Now since

$$|\mathbb{Z}/mn\mathbb{Z}| = mn = |\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}|,$$

so we just need to show the injectivity and group homomorphism. Now if

$$\phi\left(\overline{x}\right) = (\overline{0}, \overline{0}),$$

then $x \in m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z} = \overline{0}$, so $\ker \phi = \{\overline{0}\}$.

Exercise 1.7.1. Show the homomorphism part.

∎

Question. Now that we know ϕ is an isomorphism, can we construct ϕ^{-1}?

Answer. First, find integers a, b s.t.
$$ma + nb = 1,$$
then for $(\overline{x}, \overline{y}) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, we can set
$$\phi^{-1}(\overline{x}, \overline{y}) = \overline{may + nbx}.$$
This definition works since
$$nb \equiv 1 \mod m \quad ma \equiv 1 \mod n.$$
Check that $\phi \circ \phi^{-1}(\overline{x}, \overline{y}) = (\overline{x}, \overline{y})$. ⊛

Question. How about the step of finding such a, b?

Answer. Suppose $m \geq n$. Let $r_0 = m, r_1 = n$, then
$$\begin{aligned}
r_0 &= q_1 r_1 + r_2 \quad 0 \leq r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3 \quad 0 \leq r_3 < r_2 \\
r_2 &= q_3 r_3 + r_4 \quad 0 \leq r_4 < r_3 \\
&\vdots \\
r_{n-2} &= q_{n-1} r_{n-1} + r_n \quad 0 \leq r_n < r_{n-1} \\
r_{n-1} &= q_n r_n.
\end{aligned}$$

Now since for every r_i, $\gcd(r_i, r_{i+1}) = \gcd(m, n)$, and $\gcd(r_{n-1}, r_n) = r_n$, so it works. Since $\gcd(m, n) = 1$, so $r_n = 1$, and thus
$$\begin{aligned}
1 = r_n &= r_{n-2} - q_{n-1} r_{n-1} \\
&= r_{n-2} - q_{n-1}(r_{n-3} - q_{n-2} r_{n-2}) \\
&= -q_{n-1} r_{n-3} + (1 + q_{n-1} q_{n-2}) r_{n-2} \\
&= \dots
\end{aligned}$$
so we can recover it to $1 = a r_0 + b r_1 = am + bn$. ⊛

1.8 Group action

Lecture 10

15 Oct. 13:20

> **Definition 1.8.1** (Group Action). If G is a group and X is a set, then we say G acts on X if there exists a map
> $$G \times X \to X, \quad (g, x) \mapsto g \cdot x$$
> satisfying $g(hx) = (gh) \cdot x$ and $e \cdot x = x$, and we call this map a group action.

> **Example 1.8.1.** $X = G$ and $g \cdot x = gx$.

> **Example 1.8.2.** $X = G$ and $g \cdot x = gxg^{-1}$. We call this a conjugation.

> **Definition 1.8.2.** We say
> $$Gx = \{g \cdot x \mid g \in G\} \text{ for some } x \in X$$
> is an orbit of a group action.

Example 1.8.3. $Gx \subseteq G$ for all $x \in G$.

Example 1.8.4.
$$Gx = \{gxg^{-1} \mid g \in G\} = \{h^{-1}xh \mid h \in G\}.$$

Definition. We introduce some important subgroup of a group:

Definition 1.8.3 (Orbit). Let G be a group acting on a set X. For any $x \in X$, the *orbit* of x under the action of G is defined as
$$\mathrm{Orb}(x) = \{g(x) \mid g \in G\}.$$

Definition 1.8.4 (Stabilizer). Let G be a group acting on a set X. For any $x \in X$, the *stabilizer* of x in G is defined as
$$\mathrm{Stab}(x) = \{g \in G \mid g(x) = x\}.$$
It is a subgroup of G.

Definition 1.8.5 (Normalizer). Let H be a subgroup of a group G. The *normalizer* of H in G is defined as
$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$
It is the largest subgroup of G in which H is normal.

Definition 1.8.6 (Centralizer). Let G be a group and $g \in G$. The *centralizer* of g in G is defined as
$$C_G(g) = \{x \in G \mid xg = gx\}.$$
More generally, for a subset $S \subseteq G$,
$$C_G(S) = \{x \in G \mid xs = sx \text{ for all } s \in S\}.$$

Definition 1.8.7 (Center). Let G be a group. The *center* of G is defined as
$$Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}.$$
It consists of all elements of G that commute with every element of G.

Definition 1.8.8 (Conjuagcy classes). We call the G-orbits under the congugation actions the conjugacy classes. It is an equivalence class defined by
$$x \sim g^{-1}xg,$$
so we have
$$|G| = \sum_{C \in \mathrm{Conj}(G)} |C|,$$
where $\mathrm{Conj}(G)$ is the set of all conjugation classes of G.

Note 1.8.1. The definition of the equivalence relation in the conjugation classes is
$$x \sim y \text{ iff } \exists g \in G \text{ s.t. } x = g^{-1}yg.$$

Proposition 1.8.1.
$$|C(x)| = \frac{|G|}{|Z_G(x)|},$$
where
$$Z_G(x) = \left\{ g \in G \mid g^{-1}xg = x \right\}.$$

Remark 1.8.1. See orbit-stabalizer theorem. (HW5)

1.9 Symmetric groups

Definition 1.9.1.
$$S_n = \{\text{permutations on } n \text{ letters}\}.$$

Question. What is the conjugation classes of S_n?

Consider
$$\tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix},$$
then what is $\sigma^{-1}\tau\sigma$?

Note 1.9.1. Here we first operate σ^{-1} rather than σ, it is from left to right.

Thus, we have
$$\sigma^{-1}\tau\sigma = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n) \end{pmatrix}.$$

Example 1.9.1. If
$$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13)(2),$$
then
$$\sigma^{-1}\tau\sigma = \begin{pmatrix} \sigma(1) & \sigma(2) & \sigma(3) \\ \sigma(3) & \sigma(2) & \sigma(1) \end{pmatrix}.$$
Note that $\sigma^{-1}\tau\sigma$ can be either:
$$(13)(2), \quad (12)(3), \quad (23)(1).$$
Thus, the cycle type is preserved. Vice versa, if two permutation have the same cycle type, then they are conjugate to each other.

Theorem 1.9.1. Conjugacy classes of S_n is described by the partition of n.

For example, $7 = 1 + 2 + 4$, then it represents the conjugacy class of type
$$(a)(bc)(defg).$$

Example 1.9.2. For S_3, the conjugation classes are
$$3 \leftrightarrow (123), (132)$$
$$1 + 2 \leftrightarrow (1)(23), (2)(13), (3)(12)$$
$$1 + 1 + 1 \leftrightarrow (1)(2)(3).$$

Lecture 11

As previously seen. A group G acts on a set X means for each $g \in G$, it gives a map sends x to $g(x)$ where $g(x) \in X$ and the maps satisfy $(gh)(x) = g(h(x))$. $\Leftrightarrow$ Formally, it is $G \times X \to X$ with $(g, x) \mapsto g(x)$ s.t. $(gh)(x) = g(h(x))$. $\Leftrightarrow$ There is a group homomorphism s.t. $G \to \mathrm{Aut}(X)$.

> **Remark 1.9.1.** Last equivalence is because we can let
> $$\Phi : G \to \mathrm{Aut}(X), \quad \Phi(g) = \phi_g, \quad \text{where } \phi_g(x) = g(x).$$

Conjugation is a group action on the group itself defined by

$$G \times G \to G, \quad (g, x) \mapsto gxg^{-1},$$

and the conjugating class is a G-orbit, which means

$$C(x) = \left\{ gxg^{-1} \mid g \in G \right\} \text{ for all } g \in G.$$

> **Note 1.9.2.** G is abelian iff $C(x) = \{x\}$ for all $x \in G$.

Symmetric group has cycle representation, and conjugation class of S_n is the set of all permutations of same cycle types.

> **Theorem 1.9.2.** Conjugation classes of S_n are cycle types $(n_1, n_2, \ldots, n_k)$ with $n_1 \leq n_2 \leq \cdots \leq n_k$ and $k \geq 1$ s.t. $n_1 + n_2 + \cdots + n_k = n$, and the corresponding class consists of all elements having that cycle type.

Note that for $H \lhd G$, we know $gHg^{-1} = H$. Hence, a normal subgroup is a union of conjugating classes:

$$H = \bigcup_{x \in H} C(x).$$

Vice versa, if a subgroup $H < G$ is a union of conjugating classes, then $H \lhd G$.

> **Note 1.9.3.** For G finite, one can look at conjugating classes to classify normal subgroups.

> **Theorem 1.9.3** (Class equation)**.** Suppose C represents the congugacy classes, then
> $$|G| = \sum_C |C|,$$
>
> and
>
> (1) $\# \{C \mid |C| = 1\}$ divides $|G|$.
>
> (2) $|C|$ divides $|G|$.

Proof. Since we can define an equivalence relation s.t. $x \sim y$ iff $x = gyg^{-1}$ for some $g \in G$, and the equivalence classes corresponding to this relation are the conjugacy classes, so

$$|G| = \sum_C |C|.$$

(1) If $|C| = 1$, then there exists $x \in G$ s.t. $C(x) = \{x\}$. Hence, we know $gxg^{-1} = x$ for all $g \in G$, which means $gx = xg$ for all $g \in G$. Define

$$Z(G) = \{x \in G \mid gx = xg\},$$

which is the center of G, then this forms a subgroup of G. (This is easy to check). Now since $\bigcup_{|C|=1} C = Z(G)$, and $Z(G) \triangleleft G$, so we have

$$\#\{C \mid |C| = 1\} = |Z(G)|,$$

and by Lagrange's theorem, we know $|Z(G)| \mid |G|$, so we're done.

(2) Let $Z_G(x) = \{g \in G \mid gx = xg\}$. Then $Z_G(x)$ is a subgroup of G. (This is easy to check). Now consider $G/Z_G(x)$, we know it is the collection of equivalence classes, and for all conjugacy classes C, there is a one-to-one correspondence mapping C to $\{gxg^{-1} \mid g \in G\} = \{hxh^{-1} \mid h \in G/Z_G(x)\}$, so

$$|C(x)| = |G/Z_G(x)| = \frac{|G|}{|Z_G(x)|},$$

and we're done.

■

Here we go back to S_n. If $C = (n_1, \ldots, n_k)$ with $n_1 + \cdots + n_k = n$, then what is $|C|$? We can easily show that the answer is

$$|C\left(1^{v_1} 2^{v_2} 3^{v_3} \ldots r^{v_r}\right)| = \frac{n!}{1^{v_1}(v_1!)2^{v_2}(v_2!)3^{v_3}(v_3!)\ldots},$$

and we can find that

$$|C\left(1^{v_1} 2^{v_2} 3^{v_3} \ldots r^{v_r}\right)| = \frac{|S_n|}{|Z_{S_n}(x)|}, \quad \text{where } x \in \left(1^{v_1} 2^{v_2} \ldots\right).$$

Lecture 12

As previously seen. We have learnt that

22 Oct. 13:20

$$\{\text{Conjugacy classes of } S_n\} = \left\{\text{cycle types } (1)^{v_1}(2)^{v_2} \ldots \text{ with } 1 \cdot v_1 + 2 \cdot v_2 + \cdots = n\right\}.$$

Also, we know

$$|(1)^{v_1}(2)^{v_2} \ldots| = \frac{n!}{1^{v_1} v_1! 2^{v_2} v_2! \ldots}.$$

Besides, we have learnt that

$$H \triangleleft G \Leftrightarrow H \text{ is a union of conj classes of } G \text{ i.e. } H = \bigcup_{x \in H} C(x).$$

Figure 1.6: Possible normal subgroups of S_3 and S_4

Remark 1.9.2. Since we know H is a normal subgroup of S_n iff $H = \bigcup_{x \in H} C(x)$, where $C(x)$ is the conjugacy class of S_n, and conjugacy classes of symmetric groups are the sets of permutations of same cycle form, and since the size of a subgroup of S_n must divide $|S_n| = n!$, so we can deduce all normal subgroups of S_n.

Definition 1.9.2 (Transpositions). We say a permutation $\pi \in S_n$ is a transposition iff $\pi \in (1)^{n-2}(2)$.

Theorem 1.9.4. Every $\sigma \in S_n$ is a product of transpositions. More specifically, this argument holds with adjacent transpositions.

Proof. Since σ can be factored into independent cyclic permutations, so we just need to show any cyclic permutation is a product of transpositions. Suppose we have

$$\tau = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_2 & a_3 & \dots & a_1 \end{pmatrix},$$

then we have:

$$(a_1 a_2)(a_2 a_3) \dots (a_{n-1} a_n) I_n = \tau.$$

Note that we first operate $(a_1 a_2)$, then $(a_2 a_3)$, and so on.

Actually, if we do bubble sort on σ, then it can becomes I_n, then we can do the inverse operation to make I_n go back to σ, so σ is just the product of adjacent transpositions. ∎
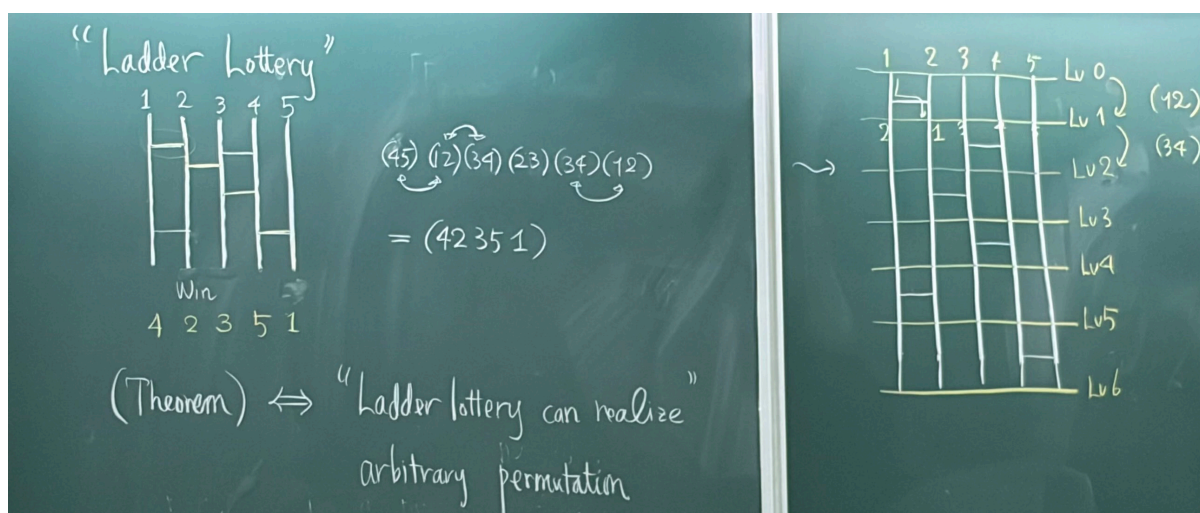

Figure 1.7: Ladder Lottery can realize arbitrary permutations

Remark 1.9.3. In ladder lottery, whenever we meet a bridge, we must go through it no matter we go left or go right, so every bridge is a (adjacent) transposition, and since every permuatation can be decomposed into adjacent transpositions, so ladder lottery can realize all permutations.

Theorem 1.9.5. For $\sigma \in S_n$, let

$$\text{inv}(\sigma) = \# \left\{ (i, j) \mid 1 \leq i < j \leq n, \sigma(i) > \sigma(j) \right\},$$

then

$$\text{inv}(\sigma \tau) \equiv \text{inv}(\sigma) + \text{inv}(\tau) \mod 2 \text{ for } \sigma, \tau \in S_n.$$

Proof. If we can show it is true for σ is a general permutation and τ is $(i, i+1)$ for all $1 \leq i \leq n$,

then for $\tau = \tau_1 \tau_2 \ldots \tau_l$, we have

$$\begin{aligned}
\mathrm{inv}(\sigma\tau) &\equiv \mathrm{inv}(\sigma\tau_1\tau_2\ldots\tau_l) \\
&\equiv \mathrm{inv}(\sigma\tau_1\ldots\tau_{l-1}) + \mathrm{inv}(\tau_l) \equiv \cdots \equiv \mathrm{inv}(\sigma) + \mathrm{inv}(\tau_1) + \mathrm{inv}(\tau_2) + \cdots + \mathrm{inv}(\tau_l) \\
&\equiv \mathrm{inv}(\sigma) + \mathrm{inv}(\tau_1\tau_2\ldots\tau_l) \equiv \mathrm{inv}(\sigma) + \mathrm{inv}(\tau).
\end{aligned}$$

Now we show that it is true for σ is a general permutation and $\tau = (i, i+1)$ for some $1 \le i \le n$.

- Case 1: $\sigma(i) > \sigma(i+1)$, then $\mathrm{inv}(\sigma\tau) = \mathrm{inv}(\sigma) - 1$ and $\mathrm{inv}(\tau) = 1$, so

$$\mathrm{inv}(\sigma\tau) \equiv \mathrm{inv}(\sigma) - 1 \equiv \mathrm{inv}(\sigma) - \mathrm{inv}(\tau) \equiv \mathrm{inv}(\sigma) + \mathrm{inv}(\tau) \mod 2.$$

- Case 2: $\sigma(i) < \sigma(i+1)$, then $\mathrm{inv}(\sigma\tau) = \mathrm{inv}(\sigma) + 1$ and $\mathrm{inv}(\tau) = 1$, so it is true in this case.

Note 1.9.4. Here we first operate σ then τ.

■

Now we can define

$$\mathrm{sgn} : S_n \to \{\pm 1\} \subseteq \mathbb{R}^\times$$

by $\mathrm{sgn}(\sigma) = (-1)^{\mathrm{inv}(\sigma)}$.

Theorem 1.9.6. For every $n \ge 2$, there exists a unique surjective group homomorphism

$$\mathrm{sgn} : S_n \to \{\pm 1\}.$$

Proof. Since

$$\mathrm{sgn}(\sigma\tau) = (-1)^{\mathrm{inv}(\sigma\tau)} = (-1)^{\mathrm{inv}(\sigma)}(-1)^{\mathrm{inv}(\tau)} = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\tau),$$

so the existence is true. (This uses previous theorem, and surjectivity is trivial since transpositions give -1 and composition of transpositions give 1). Now if

$$\varphi : S_n \to \{\pm 1\}$$

is a surjective group homomorphism, then since $\{\pm 1\}$ is an abelian group, so

$$\varphi(\tau\sigma\tau^{-1}) = \varphi(\tau)\varphi(\sigma)\varphi(\tau)^{-1} = \varphi(\sigma),$$

so conjugates elements are mapped to same sign. Now that transpositions are all conjugate (same cycle types so conjugate), so all transpositions have same sign. If $\varphi((ij)) = 1$ for some i, j, then since for all $\sigma \in S_n$, σ can be written to a product of transpositions, so $\varphi(\sigma) = \prod \varphi((ij)) = 1$, then φ is not surjective, so $\varphi((ij)) = -1$. Hence, φ is uniquely defined. (See next proposition) ■

Lemma 1.9.1. For a transposition $t \in S_n$, $\mathrm{inv}(t)$ is odd.

Proof. Suppose $t = (i, i+k)$ for some $1 \le i \le n$ s.t. $i + k \le n$ and $k > 0$, then since $t(i) = i + k$, so $t(i) > t(i+j) = i + j$ for all $1 \le j \le k$. Hence, we know there are k inverse pairs, also since for all $i + 1 \le j \le i + k - 1$, we know $j = t(j) > t(i+k) = i$, so there are $k - 1$ inverse pairs, and thus there are $2k - 1$ inverse pairs, and thus $\mathrm{inv}(t)$ is odd. ■

Proposition 1.9.1. If π can be decomposed into $c_1 c_2 \ldots c_n$ and $c_1' c_2' \ldots c_m'$, where c_i's and c_i''s are transpositions, then $2 \mid n - m$.

Proof. If $2 \nmid n - m$, then since

$$0 \equiv \mathrm{inv}(\pi\pi^{-1}) \equiv \mathrm{inv}(\pi) + \mathrm{inv}(\pi^{-1}) \equiv \sum_{i=1}^{n} \mathrm{inv}(c_i) + \sum_{i=1}^{m} \mathrm{inv}(c_{m+1-i}') \mod 2,$$

and since $\text{inv}(t)$ is odd for all transpositions t, and $n + m$ is odd, so we know $\sum_{i=1}^{n} \text{inv}(c_i) + \sum_{i=1}^{m} \text{inv}(c'_{m+1-i})$ is a sum of $n + m$ of odd numebers, which is the sum of odd numbers many of odds, and it is still an odd, so it is a contradiction. ■

Definition 1.9.3 (Alternating group of degree n)**.** We define

$$A_n = \ker(\text{sgn}) = \{\sigma \in S_n \mid \text{sgn}(\sigma) = 1\}$$
$$= \{\text{all elements expressed as a product of even number of transpositions}\}$$
$$= \bigcup_{(1-1)v_1 + (2-1)v_2 + \ldots \text{ is even}} (1)^{v_1}(2)^{v_2} \ldots$$

since $\text{sgn}((a_1 a_2 \ldots a_n)) = (-1)^{n-1}$ (It is the product of $n - 1$ transpositions).

Proposition 1.9.2. $\sigma = (1)^{v_1}(2)^{v_2} \ldots$ is an even permutation ($\sigma \in A_n$) iff $v_2 + v_4 + \ldots$ is even.

Proof. We know $\sigma \in A_n$ iff

$$(1-1)v_1 + (2-1)v_2 + \cdots \equiv 0 \quad \mod 2 \Leftrightarrow v_2 + 3v_4 + \cdots \equiv 0 \quad \mod 2 \Leftrightarrow v_2 + v_4 + \cdots \equiv 0 \quad \mod 2.$$

■

Definition 1.9.4 (Simple group)**.** A group G is said to be simple if G has no proper($\{1\}$ nor G) normal subgroup.

Note 1.9.5. $G \triangleright H$ means G/H is a subgroup, and we say G can be described by H and G/H (as a semi-direct product).

Example 1.9.3. $\mathbb{Z}/n\mathbb{Z}$ is simple iff n is prime.

Proof. If $\mathbb{Z}/n\mathbb{Z}$ is simple but $n = ms$ for some $m, s > 1$ s.t. $\gcd(m, s) = 1$, then if $\mathbb{Z}/n\mathbb{Z} = \langle g \rangle$, then we know $\langle g^m \rangle$ is a proper normal subgroup of $\mathbb{Z}/n\mathbb{Z}$, which is a contradiction. Now if n is a prime, then $\mathbb{Z}/n\mathbb{Z}$ has no proper subgroup by Lagrange's theorem, so $\mathbb{Z}/n\mathbb{Z}$ is simple. ⊛

Example 1.9.4. S_n is not a simple group for all $n \geq 3$ because $A_n \triangleleft S_n$ is proper and normal.

Example 1.9.5. $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$ is simple but $V_4 = \{e, (12)(34), (13)(24), (14)(23)\} \triangleleft A_4 = V_4 = A_4 \cup \{\text{permutuations of a cycle of size 4}\}$ is proper normal, so A_4 is not simple.

Proof. V_4 is the union of some conjugacy classes, so it is normal. ⊛

Theorem 1.9.7. A_n is a simple group for all $n \geq 5$.

Lecture 13

1.10   Sylow's theorem

5 Nov. 13:20

Definition 1.10.1 (Sylow p-group)**.** Let G be a finite group with $|G| = p^m a$ where $p \nmid a$ and p is prime. A subgroup $H < G$ with $|H| = p^m$ is called Sylow p-group.

Theorem 1.10.1 (Sylow's theorem)**.**

(1) Sylow p-subgroup exists.

(2) If $K < G$ has the order $|K| = p^l$ with $l \le m$, then there exists Sylow p-subgroup containing K.

(3) Sylow p-subgroup are conjugate to each other i.e. if P_1, P_2 are Sylow p-subgroup, then there exists $g \in G$ s.t. $P_2 = gP_1g^{-1}$.

(4) Let $n_p := \#\{\text{Sylow } p\text{-subgroups}\}$, then $n_p \equiv 1 \mod p$.

Application of Sylow's theorem

Proposition 1.10.1. Let G be a group of order pq with p, q distinct and both prime s.t. $q \not\equiv 1$ mod p, then
$$G \simeq \mathbb{Z}/pq\mathbb{Z}.$$
i.e. The group of order pq is unique.

Proof. Since $|G| = pq$, we know $n_q \equiv 1 \mod q$ and $n_q \mid p$, so $n_q = 1, p$. Note that $n_q = 1$. Thus, we know Sylow q-subgroup is a unique Q, and it is normal. Similarly we can show $n_p = 1$ and thus Sylow p-subgroup is a normal P. Hence, $|P| = p$ and $|Q| = q$, and since $P \cap Q = \{1\}$, so we have
$$P \times Q \simeq PQ = G.$$
This proves $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ and since p, q are distinct prime, so
$$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \simeq \mathbb{Z}/pq\mathbb{Z}.$$
■

Example 1.10.1. If $|G| = 15$, then $G \simeq \mathbb{Z}/15\mathbb{Z}$, but if $|G| = 21$, then G may be non-abelian since $7 \equiv 1 \mod 3$.

Proposition 1.10.2. If $|G| = pq$ with p, q distinct primes s.t. $q \equiv 1 \mod p$, then there are two possibilities:

- $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

- $G \simeq \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$, where $\rtimes$ is the semi-direct product.

Definition 1.10.2 (Semi-direct product)**.** Let G be a group, then $G = N \rtimes H$ means $N \triangleleft G$ and $H < G$ and $N \cap H = \{1\}$, and there exists $\varphi : H \to \operatorname{Aut}(N)$ s.t.
$$\varphi(h)(n) = hnh^{-1}.$$
Then, we can define a product structure on $N \times H$ as
$$(n, h) \cdot (n', h') = (nhn^{-1}n', hh')$$
since for
$$g = nh(n \in N, h \in H) \quad g' = n'h'(n' \in N, h' \in H),$$
and
$$gg' = nhn'h' = nhn'h^{-1}hh' \in N \cdot H(\text{Note that } n \in N, hn'h^{-1} \in N, hh' \in H).$$

The upshot is suppose G is a group and $N \triangleleft G$ and there exists $H < G$ s.t. $H \simeq G/N$ with $h \mapsto hN$. Then, G can be reconstructed by the information of H, N and φ, which is a group action of H acts on N.

Lecture 14

Let G be finite group and p prime. Suppose $|G| = p^e m$, and $\gcd(p, m) = 1$, then

$$\mathrm{Syl}_p(G) = \{H < G \mid |H| = p^e\},$$

and for $H \in \mathrm{Syl}_p(G)$, we call it a Sylow p-subgroup.

Theorem 1.10.2 (Sylow's theorem).

(1) $\mathrm{Syl}_p(G)$ is non-empty i.e. Sylow p-subgroup exists.

(2) Suppose $H < G$ has $|H| = p^i$ for some $0 \leq i \leq e$, then there exists $P \in \mathrm{Syl}_p(G)$ s.t. $H < P$.

(3) For $P, P' \in \mathrm{Syl}_p(G)$, there exists $g \in G$ s.t. $P' = gPg^{-1}$ i.e. all Sylow p-subgroups are conjugate in G.

(4) Let $n_p := \big|\mathrm{Syl}_p(G)\big|$, then $n_p \equiv 1 \mod p$ and $n_p \mid |G|$.

Proposition 1.10.3. With the same setting, let $r \leq e$, then there exists $H < G$ s.t. $|H| = p^r$.

Proof. First consider all subsets of size p^r. Let $\mathscr{S} := \{S \subseteq G \mid |S| = p^r\}$. At least, $h \in \mathscr{S}$ if exists. Suppose $|G| = p^e m = p^r M$. First observe that

$$|\mathscr{S}| = \binom{p^r M}{p^r} = \frac{p^r M \, (p^r M - 1) \dots (p^r M - (p^r - 1))}{p^r \, (p^r - 1) \dots 1},$$

and note that all factors p in the denominators are cancelled since

$$p^r M - i \equiv p^r - i \mod p^r \quad \forall 1 \leq i \leq p^r - 1.$$

Hence, $\mathrm{ord}_p |\mathscr{S}| = \mathrm{ord}_p(M) = s$. Now consider a group action of G on $\mathscr{S}$ given by

$$G \times \mathscr{S} \to \mathscr{S}, \quad (g, S) \mapsto g \cdot S \text{ (left-multiplication)}.$$

Let $\mathscr{S} = \cup_i \mathscr{S}_i$ be the decomposition into orbits (cosets). Thus,

$$|\mathscr{S}| = \sum_i |\mathscr{S}_i|,$$

and $|\mathscr{S}|$ is divisible by p exactly s times, and thus at least one of $\mathscr{S}_i$ has $p^{s+1} \nmid |\mathscr{S}_i|$. WLOG, suppose $p^{s+1} \nmid |\mathscr{S}_1|$. Let $S_1 \in \mathscr{S}_1$. Note that $\mathscr{S}_1 = \{g \cdot S_1 \mid g \in G\}$. Now define $H = \{h \in G \mid h \cdot S_1 = S_1\}$. Then, $H < G$. We will show $|H| = p^r$:

- As G acts on $\mathscr{S}_1$ transitively,

$$G/H \to \mathscr{S}_1, \quad gH \mapsto g \cdot S_1$$

  is bijective. Thus, $|\mathscr{S}_1| = \frac{|G|}{|H|}$. Hence, $|H| = \frac{|G|}{|\mathscr{S}|}$, and since $|G| = p^r M = p^r p^s m$, and $p^{s+1} \nmid |\mathscr{S}|$, so $|\mathscr{S}_1| \mid M$. Hence, $|H|$ is a multiple of p^r, which means $|H| \geq p^r$.

- Next, fix $x \in S_1$, then

$$\varphi : H \to S_1, \quad h \mapsto h \cdot x$$

  is injective. Thus, $|H| \leq |S_1| = p^r$.

Thus, $|H| = p^r$. $\blacksquare$

Remark 1.10.1. Our goal is to find $H < G$ s.t. $|H| = p^r$.

Now we show the Sylow's theorem:

proof of (1). By previous proposition, it is true. ∎

proof of (2). Let $P \in \mathrm{Syl}_p(G)$, and

$$A_p = \left\{ gPg^{-1} \mid g \in G \right\} \subseteq \mathscr{S}.$$

Let $N_G(P) := \left\{ g \in G \mid gPg^{-1} = P \right\} < G$. Note: $P \triangleleft N_G(P)$. Hence,

$$|A_p| = \frac{|G|}{|N_G(P)|} = [G : N_G(P)].$$

This means

$$|A_p| = \frac{\left(\frac{|G|}{|P|}\right)}{\left(\frac{|N_G(P)|}{|P|}\right)} \Rightarrow |A_p| \mid \frac{|G|}{|P|} = \frac{p^e m}{p^e} = m.$$

Hence, $p \nmid |A_p|$. Next, consider the group action of H on A_p by

$$H \times A_p \to A_p, \quad (h, Q) \mapsto hQh^{-1},$$

and let $A_p = \bigcup_{i=1} A_p^{(i)}$ be the decomposition into the orbits with $A_p^{(1)} = \left\{ hPh^{-1} \mid h \in H \right\}$. let P_i be a representative of $A_p^{(i)}$ i.e.

$$A_p^{(i)} = \left\{ hP_i h^{-1} \mid h \in H \right\},$$

and we know

$$\left| A_p^{(i)} \right| = \frac{|H|}{|N_H(P_i)|} = \frac{|H|}{|H \cap N_G(P_i)|}$$

is a power of p. By the previous argument, we know $p \nmid |A_p|$. Thus, there exists j s.t. $p \nmid \left| A_p^{(j)} \right|$, which means $\left| A_p^{(j)} \right| = 1$. Thus, $|H| = |H \cap N_G(P_j)|$, so $H \subseteq N_G(P_j)$, which means $H < N_G(P_j)$. Now recall the second isomorphism theorem:

Theorem 1.10.3 (Second Isomorphism Theorem). Suppose $H < G$ and $N \triangleleft G$, then

- $HN < G$

- $N \triangleleft HN$

- $H \cap N \triangleleft H$

- $HN/N \simeq H/(H \cap N)$.

Since we know $H < N_G(P_j)$ and $P_j \triangleleft N_G(P_j)$, so

$$\frac{|HP_j|}{|P_j|} = \frac{|H|}{|H \cap P_j|},$$

Thus, we have

$$\text{L.H.S. } \Big| \ \frac{|G|}{|HP_j|} \cdot \frac{|HP_j|}{|P_j|} = \frac{|G|}{|P_j|} = \frac{p^e m}{p^e} = m$$

$$\text{R.H.S. } \Big| \ |H|, \text{ which is the power of } p,$$

so we know L.H.S. and R.H.S. are equal to 1. Thus, $H = H \cap P_j$, and thus $H \subseteq P_j$, so $H < P_j$, where $P_j \in A_p \subseteq \mathrm{Syl}_p(G)$. ∎

proof of (3). Let $P, H \in \mathrm{Syl}_p(G)$, then by (2) we know $H \subseteq P_j \in A_p$ for some j. Since $|H| = |P_j| = p^e$, so $H = P_j \in A_p$: conjugation of P in G. So (3) is true. ∎

proof of (4). Let $P \in \mathrm{Syl}_p(G)$. By changing H as P in (2), we know $A_p^{(1)} = \{P\}$, whereas $\left|A_p^{(i)}\right| > 1$ if $i \geq 2$. (If $\{P_i\} = |A_p^{(i)}| = 1$, then $P = H \subseteq P_i$, and thus $P_i = P$, which means $i = 1$.) Therefore,

$$\left|\mathrm{Syl}_p(G)\right| = |A_p| = \sum_i \left|A_p^{(i)}\right| = \left|A_p^{(1)}\right| + \sum_{i \geq 2} \left|A_p^{(i)}\right| = 1 + \sum_i p^{l_i} \equiv 1 \mod p.$$

Also,

$$\left|\mathrm{Syl}_p(G)\right| = |A_p| = \frac{|G|}{|N_G(p)|} = [G : N_G(p)]$$

is a divisor of $|G|$. ∎

Appendix