Introduction to Algebra I

Kon Yi

December 12, 2025

Abstract

The Introduction to Algebra course by professor 佐藤信夫.

Contents

Chapter 1

Group theory

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:

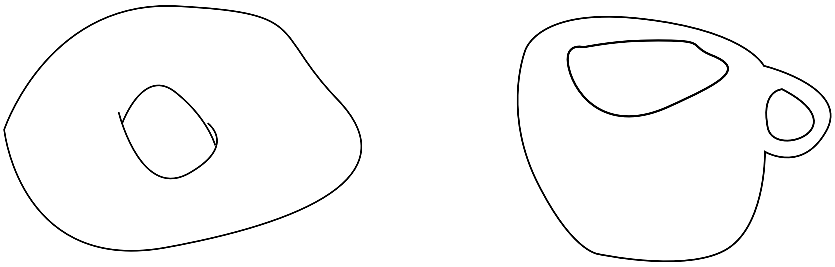


Figure 1.1: Fundamental Groups

- 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.

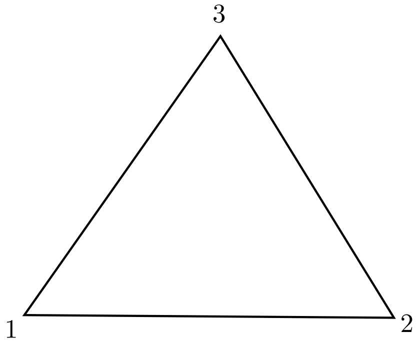
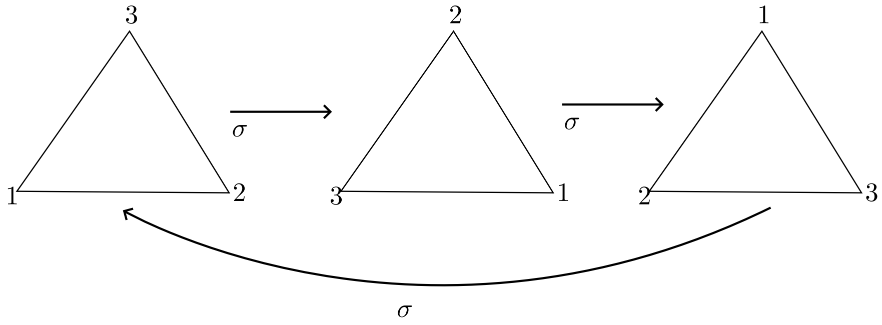


Figure 1.2: Triangle

Consider the rotation:



σ = rotation by 120°

Figure 1.3: title

and reflection

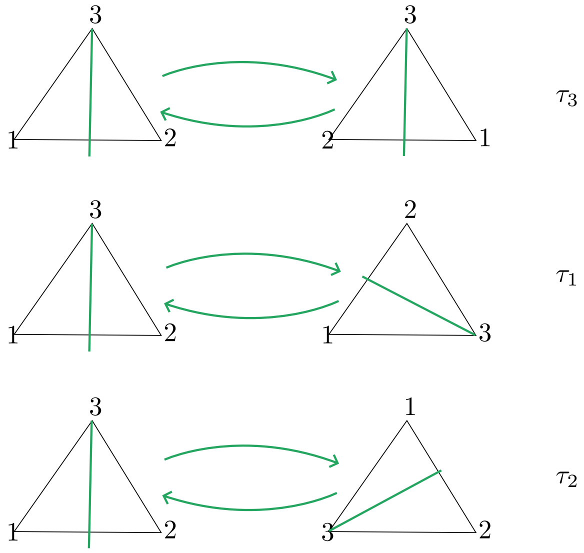


Figure 1.4: title

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

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

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 suffices 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.

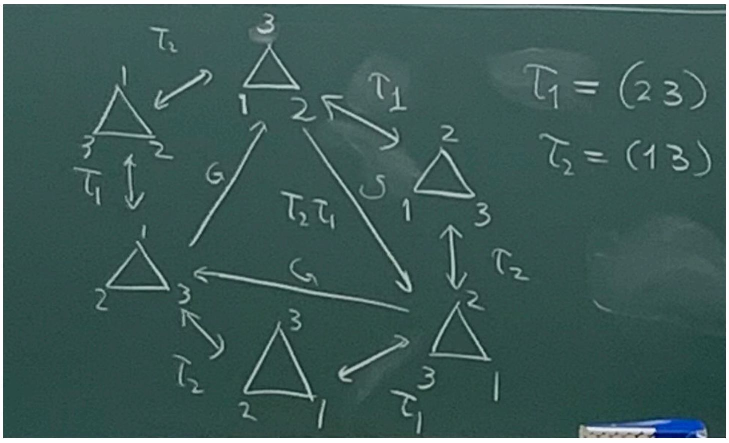


Figure 1.5: Traingle groups

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

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

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

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

Proof. Suppose $n \in H$, then $n + n = 2n \in H$, and $-n \in H$, and then $3n = 2n + n \in H$. Hence, all multiples of $n \in H$, which means $n\mathbb{Z} \subseteq H$. If $n_1, \ldots, n_r \in H$, then

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

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

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

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

Example 1.2.4. Suppose

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

then what are the subgroups?

Proof. Consider

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

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

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

Exercise 1.2.1. Show that

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

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

Lecture 4

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 $d = 0, 1, 2, \ldots$.
- $C_n = (\mathbb{Z}/n\mathbb{Z}, +)$ 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. $S_3 = \left\{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\right\}$.

- $g \in O_n(\mathbb{R}) \Leftrightarrow \langle gv, gw \rangle = \langle v, w \rangle$, 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 isomorphic to 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 $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$. 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

$$\phi(g_1g_2) = \phi(g_1)\phi(g_2)$$

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:

$$\begin{cases} \phi(g_1g_2) = \phi(g_1)\phi(g_2) & \text{for } g_1, g_2 \in G \\ \psi(h_1h_2) = \psi(h_1)\psi(h_2) & \text{for } h_1, h_2 \in H \end{cases}$$

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:

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

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

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

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

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

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

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

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

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 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 $\overline{g}$.

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.

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

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 $g_1H=g_2H$, we now show that $\varphi(g_1H)=\varphi(g_2H)$, which is equivalent to show that $Hg_1^{-1}=Hg_2^{-1}$. Since we have $g_1=g_2h$ 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 $h_2g_2^{-1}=h_2hg_1^{-1}\in Hg_1^{-1}$, 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 $\varphi(g_1H)=\varphi(g_2H)$, we want to show that $g_1H=g_2H$. This means $Hg_1^{-1}=Hg_2^{-1}$ and we want to show $g_1H=g_2H$, 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,

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

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

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

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

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.

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

Since $\langle g \rangle \subseteq G$ and $|G| < \infty$, so $\langle g \rangle$ is also finite, so there 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. ■

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

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

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

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

Thus, the requirement is that $g^{-1}Hg \subseteq H$ 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

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

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) $\forall h \in \operatorname{Im}\phi$, $h^{-1} \in \operatorname{Im}\phi$.

For (i), $\exists g_1, g_2 \in G$ s.t. $h_1 = \phi(g_1)$ and $h_2 = \phi(g_2)$, then $h_1h_2 = \phi(g_1)\phi(g_2) = \phi(g_1g_2)$, 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, $\phi(g_1g_2) = \phi(g_1)\phi(g_2) = 1$, and thus $g_1g_2 \in \ker\phi$. 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, and 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 $g_1N = g_2N$, then $\phi(g_1) = \phi(g_2)$. Since $g_1N = g_2N$, so $g_2 = g_1n$ for some $n \in N$. Thus,

$$\phi(g_2) = \phi(g_1n) = \phi(g_1)\phi(n) = \phi(g_1).$$

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:

$$\widetilde{\phi}(g_1N * g_2N) = \widetilde{\phi}((g_1 * g_2)N) = \phi(g_1 * g_2) = \phi(g_1)\phi(g_2) = \widetilde{\phi}(g_1N)\widetilde{\phi}(g_2N)$$

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

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

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

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

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

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

Lecture 9

8 Oct. 13:20

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.

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 $\ker \phi = \left\{\overline{0}\right\}$.

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

$$\phi^{-1}\left(\overline{x}, \overline{y}\right) = \overline{may + nbx}.$$

This definition works since

$$nb \equiv 1 \mod m \quad ma \equiv 1 \mod n.$$

Check that $\phi \circ \phi^{-1}\left(\overline{x}, \overline{y}\right) = (\overline{x}, \overline{y})$. ⊛

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

$$\begin{aligned} 1 = r_n &= r_{n-2} - q_{n-1} r_{n-1} \\ &= r_{n-2} - q_{n-1}\left(r_{n-3} - q_{n-2} r_{n-2}\right) \\ &= -q_{n-1} r_{n-3} + (1 + q_{n-1} q_{n-2}) r_{n-2} \\ &= \ldots \end{aligned}$$

so we can recover it to $1 = ar_0 + br_1 = am + bn$. ⊛

1.8 Group action

Lecture 10

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 15 Oct. 13:20

$$G \times X \to X, \quad (g, x) \mapsto g \cdot x$$

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.

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

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

$$\begin{aligned} 3 &\leftrightarrow (123), (132) \\ 1+2 &\leftrightarrow (1)(23), (2)(13), (3)(12) \\ 1+1+1 &\leftrightarrow (1)(2)(3). \end{aligned}$$

Lecture 11

17 Oct. 13:20

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 $(n_1, n_2, \dots, n_k)$ 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 $Z(G) \lhd G$, 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 $\left\{gxg^{-1} \mid g \in G\right\} = \left\{hxh^{-1} \mid h \in G/Z_G(x)\right\}$, 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

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

and we can find that

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

Lecture 12

22 Oct. 13:20

As previously seen. We have learnt that

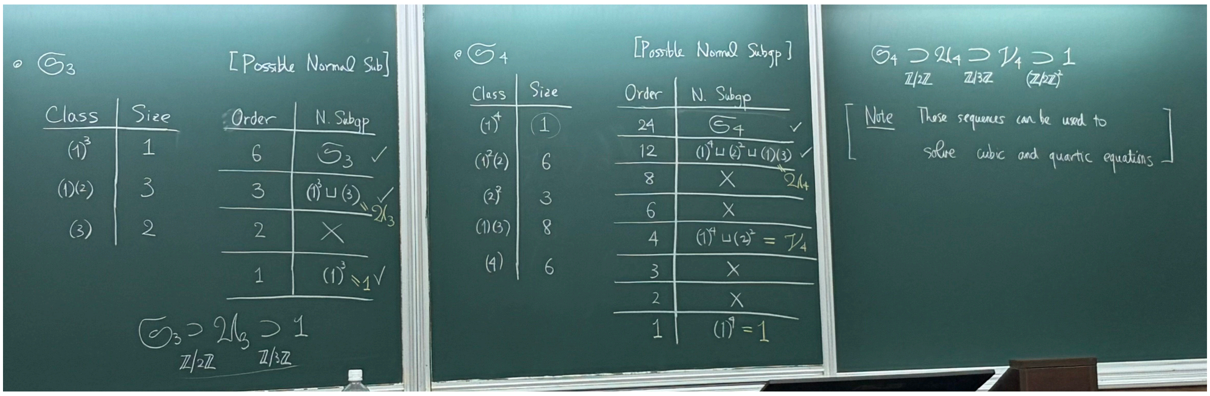
$$\{\text{Conjugacy classes of } S_n\} = \{\text{cycle types } (1)^{v_1}(2)^{v_2}\ldots \text{ with } 1\cdot v_1 + 2\cdot v_2 + \cdots = n\}.$$

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

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



- $\mathfrak{S}_3$

[Possible Normal Sub]

Class	Size
$(1)^3$	1
$(1)(2)$	3
(3)	2

Order	N. Subgp
6	$\mathfrak{S}_3$ ✓
3	$(1)^3 \sqcup (3) = \mathfrak{A}_3$ ✓
2	×
1	$(1)^3 = 1$ ✓

$$\underset{\mathbb{Z}/2\mathbb{Z}}{\mathfrak{S}_3 \supset \mathfrak{A}_3} \underset{\mathbb{Z}/3\mathbb{Z}}{\supset 1}$$

- $\mathfrak{S}_4$

[Possible Normal Subgp]

Class	Size
$(1)^4$	1
$(1)^2(2)$	6
$(2)^2$	3
$(1)(3)$	8
(4)	6

Order	N. Subgp
24	$\mathfrak{S}_4$ ✓
12	$(1)^4 \sqcup (2)^2 \sqcup (1)(3)$ ✓ $= \mathfrak{A}_4$
8	×
6	×
4	$(1)^4 \sqcup (2)^2 = \mathcal{V}_4$
3	×
2	×
1	$(1)^4 = 1$

$$\mathfrak{S}_4 \underset{\mathbb{Z}/2\mathbb{Z}}{\supset} \mathfrak{A}_4 \underset{\mathbb{Z}/3\mathbb{Z}}{\supset} \mathcal{V}_4 \underset{(\mathbb{Z}/2\mathbb{Z})^2}{\supset} 1$$

[Note These sequences can be used to solve cubic and quartic equations]

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:

$$(a_1a_2)(a_2a_3)\dots(a_{n-1}a_n)I_n = \tau.$$

Note that we first operate (a_1a_2), then (a_2a_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. ■

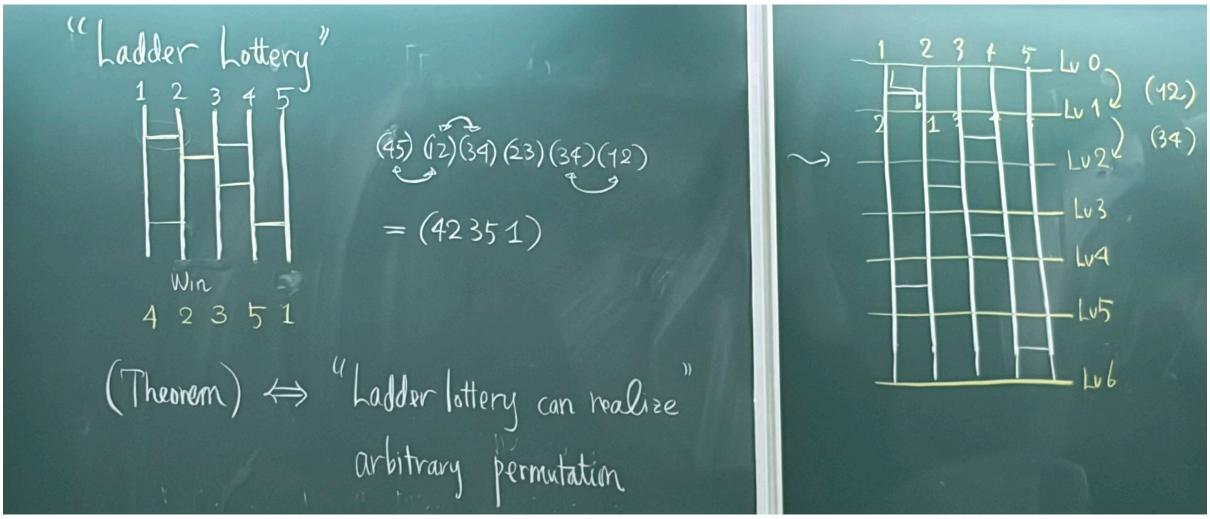


Figure 1.7: Ladder Lottery can realize arbitrary permutations

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

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

then

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

Proof. If we can show it is true for σ is a general permutation and τ is $(i, i+1)$ for all $1 \le i \le n$, then for $\tau = \tau_1\tau_2\dots\tau_l$, we have

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

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 $\operatorname{inv}(\sigma\tau) = \operatorname{inv}(\sigma) - 1$ and $\operatorname{inv}(\tau) = 1$, so

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

- Case 2: $\sigma(i) < \sigma(i+1)$, then $\operatorname{inv}(\sigma\tau) = \operatorname{inv}(\sigma) + 1$ and $\operatorname{inv}(\tau) = 1$, 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 $n \geq 2$, 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 $1 \leq i \leq n$ s.t. $i + k \leq n$ and $k > 0$, then since $t(i) = i + k$, so $t(i) > t(i + j) = i + j$ for all $1 \leq j \leq k$. Hence, we know there are k inverse pairs, also since for all $i + 1 \leq j \leq i + k - 1$, 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 $c_1c_2 \ldots c_n$ and $c'_1c'_2 \ldots c'_m$, 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 $\mathrm{inv}(t)$ is odd for all transpositions t, and $n + m$ is odd, so we know $\sum_{i=1}^{n} \mathrm{inv}(c_i) + \sum_{i=1}^{m} \mathrm{inv}(c'_{m+1-i})$ 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

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

since $\mathrm{sgn}((a_1a_2\ldots a_n)) = (-1)^{n-1}$ (It is the product of $n - 1$ transpositions).

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

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

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

■

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 $V_4 = \{e, (12)(34), (13)(24), (14)(23)\} \triangleleft A_4 = V_4 = A_4 \cup \{\text{permutations of a cycle of size 4}\}$ 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 $l \leq m$, 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 ($p < q$) 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 $n_q \equiv 1 \mod q$. Also, since we can define a group actions of G on $\mathrm{Syl}_q(G) = \{\text{Sylow } q\text{-subgroup}\}$ by

$$\varphi : (G, \mathrm{Syl}_q(G)) \to \mathrm{Syl}_q(G), \quad g \cdot P = gPg^{-1},$$

and this action is well-defined by (3) of Sylow's theorem. Thus, we know $\mathrm{Syl}_q(G) = \mathrm{Orb}(Q)$ for some $Q \in \mathrm{Syl}_q(G)$ since (1) of Sylow's theorem gyarantee the existence. Thus, by orbit-stabalizer theorem we know

$$\mathrm{Orb}(Q) \cdot \mathrm{Stab}(Q) = |G| \Rightarrow \mathrm{Syl}_q(G) = \mathrm{Orb}(Q) \mid |G| = pq,$$

and since $n_q \equiv 1 \mod q$, so we have $n_q \mid p$, so $n_q = 1, p$. If $n_q = p$, then $p \equiv 1 \mod q$, which means $q \mid p - 1$, but

$$p - 1 < q - 1 < q,$$

so this is impossible. Now we know $n_q = 1$. Thus, we know Sylow q-subgroup is a unique Q, and it is normal by plugging P_1, P_2 both to be Q in (3) of Sylow's theorem. Similarly we can show $n_p = 1$ and thus Sylow p-subgroup is a normal P. Hence, $|P| = p$ and $|Q| = q$, and since $P \cap Q$ is a subgroup of P and Q, so $|P \cap Q| \mid p$ and $|P \cap Q| \mid q$, so we have $P \cap Q = \{1\}$, which means

$$P \times Q \simeq PQ = G$$

since

$$|PQ| = \frac{|P|\,|Q|}{|P \cap Q|} = |P||Q|.$$

This proves $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ and since p, q are distinct prime (implies P, Q are cyclic), 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 $N \lhd G$ and $H < G$ and $N \cap H = \{1\}$, and there exists $\varphi : H \to \mathrm{Aut}(N)$ 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

$$g = nh(n \in N, h \in H) \quad g' = n'h' \left(n' \in N, h' \in H\right),$$

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 7 Nov. 13:20

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

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 $n_p := \left|\mathrm{Syl}_p(G)\right|$, 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, $|H| = p^r$.

■

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.

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

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

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

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

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 $|G|$. ■

Lecture 15

1.11 Semidirect Product

12 Nov. 13:20

Suppose N, N' are groups, then

$$N \times N' = \{(n, n') \mid n \in N, n' \in N'\}$$

has a componentwise multiplication

$$(n_1, n_1') \cdot (n_2, n_2') = (n_1 n_2, n_1' n_2'),$$

and we call it the outer product.

Besides, starting from the product group G, suppose $N \triangleleft G$ and $N' \triangleleft G$ s.t. $NN' = G$ and $N \cap N' = \{1\}$, then $g = nn'$ is unique. Since if $n_1 n_1' = n_2 n_2'$, then $n_2^{-1} n_1 = n_2' n_1'^{-1} \in N \cap N' = \{1\}$.

Thus,

$$N \times N' \simeq NN', \quad (n, n') \mapsto nn'.$$

Now let's generalize this. Let G be a group and suppose $N \triangleleft G$ and $H < G$ s.t. $NH = G$ and $N \cap H = \{1\}$, then we can similarly deduce that $g = nh$ is unique. Besides, for $nh, n'h' \in NH = G$, we know

$$(nh) \cdot (n'h') = nhn'h^{-1}hh' = n\left(hn'h^{-1}\right)hh' \in NH$$

since $n, hn'h^{-1} \in N$ and $hh' \in H$. So in terms of the multiplication on the set $N \times H$, the multiplication in G

$$\Leftrightarrow (n, h) \cdot (n', h') = (n\varphi_h(n'), hh')$$

with $\varphi_h(n) := hnh^{-1}$ for $h \in H$ and $n \in N$.

Note 1.11.1. The inner viewpoint requires the multiplication of G in φ_h.

Question. How can we reconstruct such groups?

Observe that $\varphi_h : N \to N$ is a group automorphism, so there is a group action of H on N:

$$(h, n) \mapsto \varphi_h(n).$$

Now we can equivalently define

$$\varphi : H \to \mathrm{Aut}(N), \quad h \mapsto \varphi_h.$$

In fact,

$$\varphi_g \circ \varphi_h(n) := \varphi_g(\varphi_h(n)) = ghnh^{-1}g^{-1} = \varphi_{gh}(n).$$

This shows

$$\varphi : H \to \mathrm{Aut}(N)$$

is a group homomorphism.

Question. What if we start with a general group action of H on N:

$$H \to \mathrm{Aut}(N), \quad h \mapsto \varphi_h,$$

and define a multiplication on the set $N \times H$ as

$$(*) \quad (n,h)\cdot(n',h') \coloneqq (n\varphi_h(n'), hh')?$$

Theorem 1.11.1. The binary operation $(*)$ satisfies all group laws, so it defines a group structure on $N \times H$ (the product set).

Notation. The resulting group is defined as

$$N \rtimes_\varphi H,$$

where φ may be ommited if it is clear.

Here,

$$\begin{cases} N \times \{1\} \triangleleft N \rtimes_\varphi H \\ \{1\} \times H < N \rtimes_\varphi H \end{cases}$$

using these subgroups.

(Check the group axioms).

- Associativity:

$$\begin{aligned}
&(n_1,h_1)\cdot((n_2,h_2)\cdot(n_3,h_3)) \\
&= (n_1,h_1)\cdot(n_2\varphi_{h_2}(n_3), h_2h_3) \\
&= (n_1\varphi_{h_1}(n_2\varphi_{h_2}(n_3)), h_1h_2h_3) \\
&= (n_1\varphi_{h_1}(n_2)\varphi_{h_1}(\varphi_{h_2}(n_3)), h_1h_2h_3) \\
&= (n_1\varphi_{h_1}(n_2)\varphi_{h_1h_2}(n_3), h_1h_2h_3).
\end{aligned}$$

  Also, we know

$$((n_1,h_1)\cdot(n_2,h_2))\cdot(n_3,h_3) = (n_1\varphi_{h_1}(n_2)\varphi_{h_1h_2}(n_3), h_1h_2h_3),$$

  so the associativity holds.

- Inverse:

$$(n,h)^{-1} = \left(\varphi_{h^{-1}}\left(n^{-1}\right), h^{-1}\right).$$

■

Example 1.11.1.

- If $\varphi : H \to \mathrm{Aut}(N)$ is trivial i.e. $\varphi(H) = \{1\}$, then

$$N \rtimes_\varphi H = N \times H.$$

- Suppose $N = \mathbb{Z}/m\mathbb{Z} = C_m$, which is cyclic, then since $\mathbb{Z}/m\mathbb{Z} = \langle 1 \rangle$, so $\varphi \in \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})$ is determined by $\varphi(1)$ since $\varphi(1^n) = (\varphi(1))^n$, so we need $\varphi(1)$ coprime to m. That is, $\varphi(1) \in (\mathbb{Z}/m\mathbb{Z})^\times$.

Chapter 2

Ring theory

Lecture 16

Definition 2.0.1 (Ring)**.** A set A is called a ring if it has two binary operations $+$ and $\cdot$ satisfying the following conditions: 14 Nov. 13:30

- $(A, +)$ is an abelian group.
- $(A, \cdot)$ is a monoid. (Only has associativity and identity).
- $+$ and $\cdot$ are coherent in the following way:

$$\begin{cases}(a+b)\cdot c = a\cdot c + b\cdot c\\ a\cdot(b+c) = a\cdot b + a\cdot c.\end{cases}$$

Example 2.0.1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are rings.

Note 2.0.1. If $\cdot$ is commutative, then A is called a commutative ring.

Example 2.0.2. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all commutative rings, while

$$M_n(\mathbb{Z}) = \{n\times n \text{ matrices with integers entries}\}$$

is non-commutative if $n \geq 2$.

Given a ring A, we know $(A, +)$ is an abelian group, and

$$A^\times = \{a \in A \mid \exists b \text{ s.t. } ab = ba = 1_A\}$$

forms a group called multiplication group of A sisnce for $a, a' \in A^\times$ we know $aa' \in A^\times$.

Example 2.0.3. Let G be a finite group, A commutative ring. The group ring is the ring denoted by $A[G]$, defined as:

- underlying set:

$$\left\{\sum_{g\in G} a_g \cdot g \mid a_g \in A\right\}.$$

- Addition $+$: If

$$\begin{cases}a = \sum a_g\cdot g\\ b = \sum b_g \cdot g,\end{cases}$$

then $a+b=\sum(a_g+b_g)\cdot g$.

- Multiplication:

$$ab=\sum_{g,h\in G}a_gb_h(g\cdot h)=\sum_{\sigma\in G}\left(\sum_{gh=\sigma}a_gb_h\right)\sigma.$$

For example, $G=\mathbb{Z}/3\mathbb{Z}=\left\{\overline{0},\overline{1},\overline{2}\right\}$, then the group ring is

$$\left\{a_0\cdot\overline{0}+a_1\cdot\overline{1}+a_2\cdot\overline{2}\mid a_0,a_1,a_2\in A\right\},$$

where for $a=a_0\overline{0}+a_1\overline{1}+a_2\overline{2}$ and $b=b_0\overline{0}+b_1\overline{1}+b_2\overline{2}$ we know

- $a+b=(a_0+b_0)\overline{0}+(a_1+b_1)\overline{1}+(a_2+b_2)\overline{2}$.
- $$a\cdot b=(a_0b_0)(\overline{00})+\cdots+a_2b_2(\overline{22}).$$

Note 2.0.2. In representation theorey of G, group ring is very important (Group cohomology).

Example 2.0.4. Let D be a square-free integer, then

$$\mathbb{Z}[\sqrt{D}]=\left\{a+b\sqrt{D}\mid a,b\in\mathbb{Z}\right\}.$$

For $\alpha=a+b\sqrt{D}$ and $\beta=c+d\sqrt{D}$, then $\alpha+\beta=(a+c)+(b+d)\sqrt{D}$ and

$$\alpha\beta=(a+b\sqrt{D})(c+d\sqrt{D})=(ac+bdD)+(ad+bc)\sqrt{D},$$

so $\mathbb{Z}[\sqrt{D}]$ forms a ring. On the other hand,

$$\left\{a+b\sqrt{2}+c\sqrt{3}\mid a,b,c\in\mathbb{Z}\right\}$$

doesn't form a ring, while

$$\left\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\mid a,b,c,d\in\mathbb{Z}\right\}$$

forms a ring.

Example 2.0.5 (Quaterums).

$$\mathbb{H}=\{a+bi+cj+dk\mid a,b,c,d\in\mathbb{R}\}$$

where i,j,k are imaginary units

$$i^2=j^2=k^2=-1,\quad ij=k,jk=i,ki=j,\quad ji=-k,kj=-i,ik=-j.$$

Hence, H is a non-commutable ring.

Hence, we know

$$\underbrace{\mathbb{R}\subseteq\mathbb{C}\subseteq\mathbb{H}}_{\text{rings in our def}}\subseteq\underbrace{\mathbb{O}}_{\text{NOT associative}},$$

Note that

$$\begin{aligned}&\left\{x\in\mathbb{R}\mid x^2=-1\right\}=\varnothing\\&\left\{x\in\mathbb{C}\mid x^2=-1\right\}=\{\pm i\}\\&\left\{x\in\mathbb{H}\mid x^2=-1\right\}=\left\{ai+bj+ck\mid a^2+b^2+c^2=1\right\}\simeq S^2\text{ (2 dimensional ball)}\\&\left\{x\in\mathbb{O}\mid x^2=-1\right\}=\left\{a_1i_1+a_2i_2+\cdots+a_7i_7\mid a_1^2+\cdots+a_7^2=1\right\}\simeq S^6\text{ (6 dimensional sphere).}\end{aligned}$$

Example 2.0.6.

$$C^\infty(\mathbb{R}) = \{\text{real functions differentiable infinitely times}\}.$$

Given a set X (with some geometry),

$$C(X) = \{\text{functions with conditions}\} \subseteq \mathrm{Map}(X, A),$$

where A is a ring, so $f \cdot g \in C(X)$ gives $fg \in C(X)$ by $(f \cdot g)(x) = f(x) \cdot g(x)$.

In general, given a space, considering certain class of functions on that space is a very important idea of investigating the space, and in this way. One may study the ring (or modules) of functions.

Note 2.0.3. If $0_A = 1_A$, $A = \{0_A\}$, and in many statements, we need to exclude this case.

Next, we consider the maps between rings.

Definition 2.0.2 (Ring homomorphism/isomorphism)**.** Let A, B be rings, and

$$f : A \to B$$

is called a ring homomorphism if it respects the ring statements, i.e.

- $f(x + y) = f(x) + f(y)$ for all $x, y \in A$.
- $f(xy) = f(x)f(y)$ for all $x, y \in A$.
- $f(1_A) = 1_B$.
- $f(0_A) = 0_B$.

If $f : A \to B$ has an inverse, then f is said to be an isomorphism, denoted as $A \simeq B$.

Proposition 2.0.1. If $f : A \to B$ and $g : B \to C$ are ring homomorphisms, then $g \circ f : A \to C$ is a ring homomorphism.

Note 2.0.4. Thus, we may define

$$\mathrm{Aut}^{\mathrm{alg}}(A) = \{\text{All ring automorphisms of } A\} \ (= \text{isomorphism from } A \text{ to itself}),$$

and this forms a group.

Lecture 17

If A is a ring and $0_A = 1_A$, then for $x \in A$, 19 Nov. 13:20

$$x = x \cdot 1_A = x \cdot 0_A = 0_A,$$

so $A = \{0\}$, which is called a singleton or zero ring.

Division

We define $z = \frac{x}{y}$ if $x = y \cdot z$ for some z existing uniquely. Thus, division by 0 is not defined. Thus, division isn't defined for every element of a ring.

Definition 2.0.3. A ring A is called a division ring if $x \in A \setminus \{0\}$ has an inverse.

Remark 2.0.1. Zero ring is excluded usually.

Remark 2.0.2. A division ring A is called a field if A is commutative.

There are so many rings other than the one we usually deal with.

Definition 2.0.4 (Zero divisors). If $a, b \in A \setminus \{0\}$ satisfies $ab = 0$, then a, b are zero divisors.

Example 2.0.7. In $\mathbb{R} \times \mathbb{R}$, if we define

$$\begin{cases} (a,b) + (c,d) = (a+c, b+d) \\ (a,b) \cdot (c,d) = (ac, bd), \end{cases}$$

then $\mathbb{R} \times \mathbb{R}$ has zero divisors:

$$(1,0) \cdot (0,3) = (0,0).$$

Definition 2.0.5. The ring without zero-divisors are called integral domains.

Definition 2.0.6 (Subrings). For a ring R, if a subset $S \subseteq R$ forms a ring with the same ring structure as R, then S is called a subring.

Example 2.0.8. If $R = \mathbb{Z}$, then is there any subring of $\mathbb{Z}$?

Proof. First, subgroups of $\mathbb{Z}$ are of the forms $n \cdot \mathbb{Z}$, but $1 \notin n\mathbb{Z}$ if $n \neq 1$, so $\mathbb{Z}$ doesn't have any nontrivial subring. ⊛

Example 2.0.9. If $R = \mathbb{Q}$, then is there any subring?

Proof. Consider

$$\mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{n}{2^\ell} \mid \ell \geq 0, n \in \mathbb{Z}\right\}$$

and

$$\mathbb{Z}_{(2)} = \left\{\frac{n}{m} \mid n \in \mathbb{Z}, m \text{ is odd}\right\},$$

they are both subrings of R. ⊛

Suppose R, S are rings, then if

$$\begin{aligned} &\phi : R \to S \\ &\phi(x+y) = \phi(x) + \phi(y) \\ &\phi(x \cdot y) = \phi(x) \cdot \phi(y) \\ &\phi(1_R) = 1_S \\ &\phi(0_R) = 0_S, \end{aligned}$$

then ϕ is a ring homomorphism and $\ker \phi$ forms an ideal of R (in group homomorphism it is a normal subgroup).

Lecture 18

Definition 2.0.7. We say a ring A is an integral domain if A is not the trivial ring and for all $a, b \neq 0$ we have $ab \neq 0$, i.e. there is no zero divisors. 26 Nov. 13:20

Definition 2.0.8. We say a ring A is a field if A is not the trivial ring and for all $a \in A \setminus \{0\}$, $\exists b \in A$ s.t. $ab = ba = 1_A$, i.e.

$$A^\times = A \setminus \{0\}.$$

Remark 2.0.3. In fact, we can generalize integral domains to field of fractions. Thr prototype is

$$\mathbb{Z} \to \mathbb{Q} = \left\{ \frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{Z} \setminus \{0\} \right\}.$$

Here the meaning of $\frac{p}{q}$ is

$$(p, q) \sim (p', q') \Leftrightarrow \exists r, r' \text{ s.t. } r \cdot p = r' \cdot p' \text{ and } r \cdot q = r' \cdot q'.$$

And we can define

- $$\frac{p}{q} + \frac{p'}{q'} = \frac{pq' + p'q}{qq'}, \text{ i.e. } (p, q) + (p', q') = (pq' + p'q, qq').$$
- $$\frac{p}{q} \cdot \frac{p'}{q'} = \frac{pp'}{qq'}, \text{ i.e. } (p, q) \cdot (p', q') = (pp', qq').$$

Also, there is an injective homomorphism:

$$\mathbb{Z} \to \mathbb{Q}, \quad m \mapsto \frac{m}{1}.$$

The same construction is possible for

$$\mathbb{C}[t] \to \mathbb{C}(t) = \left\{ \frac{p(t)}{q(t)} \mid p(t) \in \mathbb{C}[t], q(t) \in \mathbb{C}[t] \setminus \{0\} \right\}.$$

In general, given an integral domain A,

$$A \sim Q(A) = \{(p, q) \in A \times A \setminus \{0\}\} / \sim$$

where $(p, q) \sim (p', q') \Leftrightarrow pq' = p'q$.

Proposition 2.0.2. $\varphi : A \to Q(A)$ where $\varphi(a) = (a, 1)$ is an injective ring.

Proof. Check that $\ker \varphi = \{0\}$ and

$$\begin{aligned} \varphi(a + b) &= \varphi(a) + \varphi(b) \\ \varphi(ab) &= \varphi(a)\varphi(b) \\ \varphi(1_A) &= 1_{Q(A)}. \end{aligned}$$

■

Corollary 2.0.1. $Q(A)$ is a field.

Proof. Note that

$$(p, q)^{-1} = (q, p).$$

■

Modules are the generalization of vector spaces

Definition 2.0.9. A vector space V/k (or V over k) where k is a field means

(1) $(V, +)$ is an abelian group (vector can be added)

(2) $\forall r \in k$, $\forall v \in V$, $rv \in V$.

(3) $r(v + v') = rv + rv'$ and $(r + r')v = rv + r'v$ for $r, r' \in k$ and $v, v' \in V$.

Definition 2.0.10. Modules M/R has same definition as vector spaces if replacing k (a field) with R (a ring), and V (vector spaces) by M (modules). In this case, M is called an R-module.

Comparision between vector spaces and modules

If V is a vector space over $\mathbb{R}$ (of finite dimension), then $V \simeq \mathbb{R}^n$ with some n. However, there are huge varieties of $\mathbb{Z}$-modules. For example, $M = \mathbb{Z}^n$ is a $\mathbb{Z}$-module, and $M = \mathbb{Z}/5\mathbb{Z}$ is also a $\mathbb{Z}$-module. In fact, any module under any ring is a $\mathbb{Z}$-module. Hence, for an R-module, M, we can always view M as a $\mathbb{Z}$-module.

Remark 2.0.4. We can view every module (in fact abelian group) as a $\mathbb{Z}$ module since for all $m \in \mathbb{Z}$ and $x \in M$, we can define

$$m \cdot x = x + x + \cdots + x \in M,$$

and thus we know all rules in the definition of modules hold.

Definition 2.0.11. We call M' a sub R-module if M is a R-module and $M' \subseteq M$ forms an R-module. (Note that for all $r \in R$ and $m \in M'$ we have $rm \in M'$)

Definition 2.0.12. An ideal I of a ring R is a sub R-module of R, i.e.

- I is a subgroup of $(R, +)$.
- For $r \in R$, $x \in I$, $r \cdot x \in I$.
- Distributive.

Example 2.0.10. If $R = \mathbb{Z}$, then all ideals are of the form $m \cdot \mathbb{Z}$.

Lecture 19

28 Nov. 13:20

Remark 2.0.5. $I \subseteq R$ is called an ideal if I is a submodule of R (viewed as an R-submodule)

Remark 2.0.6. $\{0\}, R$ are R-modules "trivial", so I is called a non-trivial ideal of R if $\{0\} \subsetneq I \subsetneq R$.

Remark 2.0.7. R is a field iff R has no non-trivial ideals.

Remark 2.0.8. If $I \subseteq R$ is a non-trivial ideal, then $a \in I$ is not invertible.

Example 2.0.11 (Examples of ideals)**.**

- $R = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \ldots$ (fields), then only ideals are $\{0\}$ and R itself.
- $R = \mathbb{Z}$, then since $m\mathbb{Z}$ are the only subgroups of $\mathbb{Z}$, and they are all ideals.
- For a finite subset S of R,

  $$I(S) := \{r_1 s_1 + r_2 s_2 + \cdots + r_m s_m \mid r_1, \ldots, r_m \in R\}$$

  and $S = \{s_1, s_2, \ldots, s_m\}$ form an ideal of R called the ideal generated by S.

  Remark 2.0.9. $I(S)$ is the minimal ideal of R containing S.

  Also, $I(S)$ is more commonly denoted by $(s_1, s_2, \ldots, s_m)$.

Question. Is the case of $\mathbb{Z}$, does $I(S)$ give you anthing now?

Answer. Consider

$$(3,5) = \{3m + 5n \mid m, n \in \mathbb{Z}\},$$

then since $1 \in (3,5)$, so $(1) = \mathbb{Z}$. ⊛

Remark 2.0.10. If k is a field, then $k[t]$ (the polynomial ring over k) has ideals of the form $(p(t))$, which can be shown by Euclidean algorithm.

Question. If $R = k[x,y]$, then is (x,y) generated by one element?

Answer. It is not possible. Since

$$(x,y) = \{p(x,y)x + q(x,y)y \mid p, q \in k[x,y]\} = \left\{ \sum_{(i,j)\neq(0,0)} a_{ij}x^i y^j \mid \{a_{ij}\} \subseteq k \right\}.$$

We show that there is no $r(x,y) \in k[x,y]$ s.t. $(x,y) = (r(x,y))$. Since

$$r(x,y) \mid x \text{ and } r(x,y) \mid y,$$

so

$$r(x,y) \mid \gcd(x,y) = 1.$$

Hence, $(x,y) = (r(x,y)) = (1) = k[x,y]$, which is a contradiction. ⊛

Numbers to Ideals

Note that $d \mid n$ for $n, d \in \mathbb{Z}$ if and only if $n = dm$ for some $m \in \mathbb{Z}$ if and only if $n \in (d)$ if and only if $(n) \subseteq (d)$. Also, p is prime means

$$p \mid ab \Rightarrow p \mid a \text{ or } p \mid b.$$

This is the number perspective. In the ideal perspective,

$$ab \in (p) \Rightarrow a \in (p) \text{ or } b \in (p).$$

Definition 2.0.13. An ideal $\mathcal{P}$ of R is called a prime ideal if

$$ab \in \mathcal{P} \Rightarrow a \in \mathcal{P} \text{ or } b \in \mathcal{P}.$$

Definition 2.0.14. $m \subsetneq R$ is called a maximal ideal if there is no ideals between m and R, i.e.

$$m \subseteq I \subseteq R \Rightarrow I = m \text{ or } I = R.$$

Example 2.0.12. $(x-a, y-b)$ are maximal ideals of $k[x,y]$ for $a, b \in k$.

Example 2.0.13. p with p prime are maximal ideals of $\mathbb{Z}$.

Theorem 2.0.1. Let $\phi : A \to B$ be a ring homomorphism:

- $\operatorname{Im}\phi$ is a subring of B.

- $\ker \phi = \phi^{-1}(\{0\})$ is an ideal of A.
- For any ideal $J \subseteq B$, $\phi^{-1}(J)$ is an ideal of A.

Proof. Let's show the third one. If $a \in A$ and $x \in \phi^{-1}(J)$, then $a \cdot x \in \phi^{-1}(J)$. ■

Example 2.0.14. $\phi : \mathbb{Z} \to 3\mathbb{Z}$ defined by modulo 3 where $\ker \phi = 4\mathbb{Z}$ is not a subring but an ideal.

Recall that $H \triangleleft G$ gives G/H a group, and

$$\phi : G \to G/H$$

has $\ker \phi = H$. If $I \subseteq R$ is an ideal, then R/I forms a ring by

$$(x + I) \cdot (y + I) = (xy + I).$$

And $\phi : R \to R/I$ has the ker of I.

Lecture 20

Recall that we have $R/\ker \phi \simeq \operatorname{Im} \phi$ if R is a group. Now let R be a ring, and $I \subseteq R$ be an ideal, then 3 Dec. 13:20

$$\phi : R \to R/I, \quad r \mapsto r + I = \{r + a \mid a \in I\}.$$

is a group homomorphism (since we assume R is a ring and thus abelian in addition and thus I is normal in R and thus R/I is a group). Thus, we have

$$(x + I) \cdot (y + I) = xy + xI + yI + I^2 = xy + I.$$

Hence,

$$R/\ker \phi \simeq \operatorname{Im} \phi$$

is naturally viewed as a ring isomorphism.

Proposition 2.0.3. P is a prime ideal of R iff R/P is an integral domain.

Proof. Since $x, y \notin P$ implies $xy \notin P$, so if $x \neq \overline{0}$ and $y \neq \overline{0}$, then $xy \neq \overline{0}$. Note that $a = \overline{0}$ iff $a \in P$. ■

Proposition 2.0.4. m is a maximal ideal of R iff R/m is a field.

Proof. Need to show $x \neq \overline{0} \in R/m$ is invertible. Suppose $x' \in R$ s.t. $\overline{x'} = x$. By assumption, $x' \notin m$. Consider

$$(x') + m = \{a \cdot x' + p : a \in R, p \in m\},$$

then $m \subsetneq m + (x') \subseteq R$ since $x' \in (x') + m$ but $x' \notin m$. Hence, $m + (x') = R$. Thus, there exists $\alpha \in m$ and $r \in R$ s.t.

$$1 = \alpha + rx',$$

and by taking modulo m, we know

$$\overline{1} = \overline{r} \cdot x,$$

which shows x is invertible. ■

Example 2.0.15. If $R = K$ is a field, then $a \in K \setminus \{0\}$ generates K, so the only ideals of K are K and $\{0\}$.

Example 2.0.16. If $R = \mathbb{Z}$, then $n\mathbb{Z}$ are the only ideals and $p\mathbb{Z}$ for prime p are the only prime ideals. Also, $p\mathbb{Z}$ for prime p are the only maximal ideals. Hence, $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/0\mathbb{Z}$ are integral domains and $\mathbb{Z}/p\mathbb{Z}$ is a fields.

Example 2.0.17. If $R = \mathbb{Q}[t]$, and every ideal is principle, i.e. of the form $(p(t))$ by Euclidean algorithm. As for the prime ideal, if $I = (p(t))$ and $p(t)$ is irreducible, then I is prime. Also, (0) is prime.

Lecture 21

5 Dec. 13:20

Theorem 2.0.2 (First isomorphism theorem). Let $\phi : R \to R'$ be ring homomorphism, then there exists unique ring isomorphism

$$\psi : R/\ker\phi \to \operatorname{Im}\phi$$

s.t. $\phi = \psi \circ \pi$ where $\pi : R \to R/\ker\phi$ by $r \mapsto r + \ker\phi$, which is a group homomorphism. Such a ψ exists as a group homomorphism $(R/\ker\phi, +) \to (R', +)$. As for the multiplication, we can view

$$\psi(xy) = \psi\left(\pi(x')\pi(y')\right)$$

for some x', y' since π is surjective and then use the fact that ϕ is a ring homomorphism, so

$$\psi(xy) = \psi\left(\pi(x')\pi(y')\right) = \psi\left(\pi(x'y')\right) = \psi\pi(x'y') = \phi(x'y') = \phi(x')\phi(y') = \psi(x)\psi(y).$$

Example 2.0.18. $R = K[t]$ where K is a field, then R is a PID, i.e. all ideals are of the form $(p(t))$ for some $p(t) \in K[t]$. Hence, prime ideals are $(p(t))$ with $p(t)$ irreducible or 0. Thus, $(p(t))$ is maximal iff $p(t)$ is irreducible, and $(p(t))$ maximal means $K[t]/(p(t))$ is a field.

Example 2.0.19. For $K = \mathbb{C}$, we know K is algebraically closed, so the only irreducible polynomial are $a(t-b)$ for $a \neq 0$ and $b \in \mathbb{C}$, so

$$\mathbb{C}[t]/(a(t-b)) = \mathbb{C}[t]/(t-b) \to \mathbb{C},$$

where $\mathbb{C}[t]/(t-b) = C + ((t-b))$. Now consider

$$\phi : \mathbb{C}[t] \to \mathbb{C}, \quad f(t) \mapsto f(b),$$

then this is a surjective ring homomorphism, which is trivial. Thus. by first isomorphism theorem,

$$\mathbb{C}[t]/\ker\phi \simeq \mathbb{C},$$

where $\ker\phi = \{f(t) \mid f(b) = 0\} = \{f(t) \mid (t-b) \mid f(t)\}$, so

$$\mathbb{C}[t]/(t-b) \simeq \mathbb{C}.$$

Example 2.0.20. For $K = \mathbb{R}$, then the irreducible polynomials are

$$f_1(t) = a(t-b) \text{ for } a \neq 0, b \in \mathbb{R}, f_2(t) = a(t^2 - bt + c) \text{ for } a \neq 0, b^2 - 4ac < 0.$$

Hence,

$$\mathbb{R}[t]/(f_1(t)) \simeq \mathbb{R}, \quad \mathbb{R}[t]/(f_2(t)) \simeq \mathbb{R}[u]/(u^2+1).$$

Note that $\mathbb{C} = \mathbb{R}[\sqrt{-1}]$, so

$$\phi : \mathbb{R}[u] \to \mathbb{R}[\sqrt{-1}], \quad u \mapsto \sqrt{-1}$$

is a surjective ring homomorphism, and thus

$$\mathbb{R}[u]/\ker(\phi) \simeq \mathbb{R}[\sqrt{-1}] = \mathbb{C},$$

and $\ker\phi = (u^2+1)$. Hence, $\mathbb{R}[u]/(u^2+1) \simeq \mathbb{C}$.

Theorem 2.0.3 (Second isomorphism theorem)**.** Suppose B is a ring and $A \subseteq B$ is a subring and $I \subseteq B$ is an ideal of B, and $\pi : B \to B/I$ is the natural ring homomorphism, then $I \cap A$ is an ideal of A and

$$A/(I \cap A) \simeq \pi(A).$$

Proof. Let $x \in I \cap A$ and $a \in A$, then

$$\begin{cases} ax \in I \text{ since } I \subseteq B \text{ is an ideal} \\ ax \in A \text{ since } a, x \in A, \end{cases}$$

so $ax \in I \cap A$ and thus $I \cap A \subseteq A$ is an ideal. Now consider $\pi|_A$, so we know

$$A/\ker \pi|_A \simeq \pi(A).$$

Note that $\ker \pi|_A = I \cap A$. ■

Example 2.0.21. Consider $B = \mathbb{Z}[\sqrt{-1}]$ and $A = \mathbb{Z}$ and $I = (2 + \sqrt{-1})\mathbb{Z}[\sqrt{-1}]$, then by Second isomorphism theorem we know

$$\pi(\mathbb{Z}) \simeq \mathbb{Z}/(2 + \sqrt{-1})\mathbb{Z}[\sqrt{-1}] \cap \mathbb{Z},$$

then for all $p \in (2 + \sqrt{-1})\mathbb{Z}[\sqrt{-1}]$ we know

$$p = (a + b\sqrt{-1})(2 + \sqrt{-1}) = (2a - b) + (a + 2b)\sqrt{-1}.$$

Thus, if $p \in \mathbb{Z}$, we need $a + 2b = 0$, i.e. $p = -5b \in 5\mathbb{Z}$, so

$$(2 + \sqrt{-1})\mathbb{Z}[\sqrt{-1}] \cap \mathbb{Z} = 5\mathbb{Z},$$

i.e. $\pi(\mathbb{Z}) \simeq \mathbb{Z}/5\mathbb{Z}$.

Theorem 2.0.4. Let A be a ring and $I \subseteq A$ be an ideal and $\pi : A \to A/I$ is the natural homomorphism, and

$$X = \{\text{ideals of } A/I\}, \quad Y = \{\text{ideals of } A \text{ containing } I\}.$$

Then there is a bijection between X and Y.

Proof. Consider

$$\phi : X \to Y, \quad J \mapsto \pi^{-1}(J) = \{a \in A \mid \pi(a) \in J\},$$

and

$$\psi : Y \to X, \quad J \mapsto \pi(J),$$

then this gives a bijection. We first show the well-definedness of ϕ.

- $\pi^{-1}(J)$ is an ideal containing I since

  $$\pi\left(A\pi^{-1}(J)\right) = \pi(A) \cdot \pi^{-1}(J) \subseteq J$$

  since $\pi(A) = A/I$ and $\pi(\pi^{-1}(J)) = J$. Hence, we know

  $$A\pi^{-1}(J) \subseteq \pi^{-1}(J).$$

  Now since

  $$I = \pi^{-1}\left(0_{A/I}\right) \subseteq \pi^{-1}(J),$$

  so we're done.

- well-definedness of ψ: For $J \subseteq A$ s.t. $I \subseteq J$, we want to show $\pi(J) \subseteq A/I$ is an ideal. For $a+I \in A/I$ and $x+I \in \pi(J)$,

$$(a+I)(x+I) = ax + xI + aI + I^2 \subseteq ax + I \subseteq J + I = J.$$

■

Theorem 2.0.5 (3rd Isomorphism theorem)**.** A is a ring and $I \subseteq J \subseteq A$ are ideals, then

(1) $\phi : A/I \to A/J$ defined by $x+I \mapsto x+J$ is a well-defined surjective ring homomorphism with $\ker\phi = J/I \subseteq A/I$.

(2) $(A/I)/(J/I) \simeq A/J$.

Lecture 22

12 Dec. 13:20

Example 2.0.22. Now suppose $A = \mathbb{Z}[x]$ and $J = \left(x^2+1, 2+x\right)$ and $I = \left(x^2+1\right)$, then since

$$A/I \simeq \mathbb{Z}[\sqrt{-1}],$$

so

$$J/I \simeq \left(2+\sqrt{-1}\right)\mathbb{Z}[\sqrt{-1}].$$

Remark 2.0.11. $A/I \simeq \mathbb{Z}[\sqrt{-1}]$ since every equivalence class in A/I is $[ax+b]$ for some $a, b \in \mathbb{Z}$, and $ax+b \mapsto ai+b$ is a bijection, and $\mathbb{Z}[\sqrt{-1}] = \{a+bi : a, b \in \mathbb{Z}\}$.

Example 2.0.23. If $A = \mathbb{Z}[x]$ and $J = \left(x^2+1, 2+x\right)$ and $I' = (2+x)$, then

$$(A/I')/(J/I') \simeq A/J.$$

Also,

$$A/I' \simeq \mathbb{Z},$$

and

$$J = \left\{\left(x^2+1\right)f(x) + (2+x)g(x)\right\},$$

so

$$J/I' = \left\{\left((-2)^2+i\right)f(-2) + 0\cdot g(-2)\right\} = 5\mathbb{Z}.$$

Thus,

$$J/I' \simeq 5\mathbb{Z}.$$

Hence,

$$\mathbb{Z}[x]/\left(x^2+1, 2+x\right) \simeq \mathbb{Z}/5\mathbb{Z}.$$

Example 2.0.24. Suppose $A = \mathbb{Z}[\sqrt{-1}] = \{a+bi \mid a, b \in \mathbb{Z}\}$ and $m = (2+\sqrt{-1}) = (2+\sqrt{-1})\mathbb{Z}[\sqrt{-1}]$, then

$$A/m \simeq F_5 = \mathbb{Z}/5\mathbb{Z}$$

since

$$\mathbb{Z}[\sqrt{-1}]/(2+\sqrt{-1}) \simeq \mathbb{Z}[x]/\left(x^2+1, 2+x\right) \simeq \mathbb{Z}/(5) = \mathbb{Z}/5\mathbb{Z}.$$

Example 2.0.25. How about $\mathbb{Z}[i]/(3)$? Suppose $A = \mathbb{Z}[x]$ and $J = \left(x^2+1, 3\right)$ and $I = \left(x^2+1\right)$ and

$I' = (3)$, then

$$(A/I)/(J/I) \simeq A/J.$$

Note that

$$(A/I)/(J/I) \simeq \mathbb{Z}[i]/(3).$$

Also,

$$(A/I')/(J/I') \simeq A/J,$$

and

$$A/I' \simeq \mathbb{F}_3[x] \quad J/I' \simeq \left(x^2+1\right)\mathbb{F}_3[x].$$

Thus,

$$\mathbb{Z}[i]/(3) \simeq \mathbb{F}_3[x]/\left(x^2+1\right).$$

Note that $\left(x^2+1\right)$ is prime if and only if x^2+1 is irreducible. If x^2+1 is reducible, then

$$x^2+1 = (x-a)(x-b) \text{ with } a, b \in \mathbb{F}_3.$$

However,

$$0^2+1 = 1 \neq 0, \quad 1^1+1 = 2 \neq 0, 2^2+1 = 2 \neq 0,$$

so neither $0, 1, 2$ is the root of $(x-a)(x-b)$, i.e. x^2+1 is irreducible. Since $\left(x^2+1\right)$ is maximal iff x^2+1 is prime iff x^2+1 is irreducible, so we know $\left(x^2+1\right)$ is maximal.

Note that we extend 3 to any prime $p \in \mathbb{Z}$. We have seen $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ for prime p. Note that we have

$$\mathbb{F}_p[x]/\left(x^2+1\right) \simeq \mathbb{Z}[i]/(p),$$

and

$$\begin{aligned} \text{The primality of } p \text{ in } \mathbb{Z}[i] &\Leftrightarrow \text{Irreducibility of } x^2+1 \text{ in } \mathbb{F}_p[x] \\ &\Leftrightarrow x^2 \equiv -1 \mod p \text{ has no solutions in } \mathbb{F}_p \\ &\Rightarrow p \equiv 3 \mod 4. \end{aligned}$$

Remark 2.0.12. p is prime in $\mathbb{Z}[i]$ if $p \equiv 3 \mod 4$ and p is not prime if $p \equiv 1, 2 \mod 4$.

Remark 2.0.13. We define

$$\left(\frac{D}{p}\right) = \begin{cases} 1, & \text{if } x^2 \equiv D \mod p \text{ for some } x \in \mathbb{F}_p; \\ -1, & \text{otherwise.} \end{cases}$$

We have

$$\left(\frac{D_1}{p}\right)\left(\frac{D_2}{p}\right) = \left(\frac{D_1 D_2}{p}\right).$$

Proposition 2.0.5. If K is a field with $|K| < \infty$, then $|K| = p^m$ with p prime and $m \geq 1$.

Proof. If $n := \underbrace{1+1+\cdots+1}_{n}$ are all different, then $|K| = \infty$. Thus, suppose $n = m$ with $n > m$, then $(n-m)_K = 0_K$. Let ℓ be the smallest positive integer s.t. $\ell_k = 0_k$. If ℓ is a composite number, say $\ell = \ell_1 \times \ell_2$ for $\ell_1, \ell_2 > 1$, then K has non-zero zero divisors since $\ell_1, \ell_2 \neq 0$ and $\ell_1\ell_2 = 0$. Thus, ℓ must be a prime number since all fields are integral domains, say $\ell = p$, where p is prime. Now since $\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\} \subseteq K$ and form a subfield, so K is an $\mathbb{F}_p$ vector space. Let $v_1, v_2, \ldots, v_m$ ve the basis of K, then

$$K = \left\{\sum_{i=1}^{m} a_i v_i \mid a_i \in \mathbb{F}_p\right\},$$

so $|K| = p^m$. ∎

Theorem 2.0.6. Let K be a field of $q = p^m$ elements, then $K^\times$ is cyclic.

Before proof, we need the following:

Theorem 2.0.7. Let G be a finite abelian group, then

$$G \simeq \prod_{i=1}^{r} \mathbb{Z}/m_i\mathbb{Z}$$

where $m_1 \mid m_2 \mid \cdots \mid m_r$.

Theorem 2.0.8. Let K be a field of $q = p^m$ elements, then $K^\times$ is cyclic.

Proof. There are two useful facts:

(1) $|S_d| = \left|\left\{x \in K \mid x^d = 1\right\}\right| \leq d$ for $d \geq 1$.

(2) G: abelian group of $|G| = n$ and $\# \left\{x \in G \mid x^d = 1\right\} \leq d$ for $d \mid n$ implies G cyclic.

We prove the first one. Note that $a \in S_d$ iff $(x-a) \mid x^d - 1$, so $|S_d| \leq d$. Now we prove the second one. Suppose

$$G \simeq \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_\ell\mathbb{Z}$$

and $\ell \geq 2$, i.e. not cyclic, then consider the element of

$$\{x^{m_1} = 1\},$$

then

$$|\{x \in G \mid x^{m_1} = 1\}| = m_1^\ell \leq m_1,$$

so $\ell = 1$, which shows G cyclic. Thus, $\ell = 1$, and thus $K^\times$ is cyclic and of order $q-1$. Thus,

$$K^\times = \left\{x \in K \mid x^{q-1} = 1\right\}.$$

This shows

$$K^\times = \left\{x \in K \mid x^{q-1} = 1\right\},$$

so

$$K = \{x \in K \mid x^q = x\}.$$

■

Appendix

Appendix A

Extra Proof

Theorem A.0.1. If $H, K < G$, then

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

Theorem A.0.2. If $A, B \lhd G$, then $AB \lhd G$.

Proof.

- $AB < G$:

$$a_1 b_1 a_2 b_2 = a_1 \left(b_1 a_2 b_1^{-1}\right) b_1 b_2 \in AB, \quad (ab)^{-1} = b^{-1} a^{-1} = \left(b^{-1} a^{-1} b\right) b^{-1} \in AB.$$

- $AB \lhd G$:

$$gABg^{-1} = \left(gAg^{-1}\right)\left(gBg^{-1}\right) = AB.$$

■

Theorem A.0.3. If $A, B \lhd G$ and $A \cap B = \{e\}$, then $AB \simeq A \times B$.

Proof. Define $\varphi : A \times B \to AB$ by $\varphi(a, b) = ab$, and this is the isomorphism. ■