Lecture 5

Lagrange's Theorem & Quotient Group & Homomorphism of Groups

What you will learn in Lecture 5

5.1 Lagrange's Theorem (ラグランジュの定理)

5.2 Normal Subgroup (正規部分群) & Quotient Group (商群)

5.3 Homomorphism (準同型) and Isomorphism (同型) of Groups

5.1 Lagrange's Theorem

(ラグランジュの定理)

5.1 Lagrange's Theorem (ラグランジュの定理)

In the last section, we noted that the order of a subgroup of a finite cyclic group divides the order of the group (Corollary 4.2).

We will learn that this is a special case of a general result, called **Lagrange's theorem**, i.e., **the order of a subgroup of a finite group divides the order of the group**.

History:
Lagrange proved this result in 1770, long before the creation of group theory, while working on the permutations of the roots of a polynomial equation. Lagrange's theorem is a basic theorem of **finite group theory** and is considered by some to be the most important result in finite group theory.

Left and Right Cosets

Definition 5.1

Let $(H,\circ)$ be **a subgroup of a group** $(G,\circ)$ and $a \in G$. The sets $aH = \{ah \mid h \in H\}$ and $Ha = \{ha \mid h \in H\}$ are called the **left and right cosets (左剰余類と右剰余類) of** H **in** G, respectively. The element a is called **a representative** of aH **and** Ha.

If G is **commutative**, then of course we have $aH = Ha$.

Observe that $eH = H = He$ and that $a = ae \in aH$ and $a = ea \in Ha$.

Left and Right Cosets

Example 5.1 Exhibit the left cosets and the right coset of the subgroup $3\mathbb{Z}$ of $\mathbb{Z}$.

Solution:

Due to the notation here is additive, so the left coset of $3\mathbb{Z}$ containing m is $m + 3\mathbb{Z}$. We first take $m = 0$, and obtain

$$3\mathbb{Z} = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}$$

It is one of the left cosets, which contains 0.

Next, we find other left cosets. Now select an element of $\mathbb{Z}$ not in $3\mathbb{Z}$, for example, 1, and find the left coset containing it. We have

$$1 + 3\mathbb{Z} = \{\dots, -8, -5, -2, 1, 4, 7, 10, \dots\}$$

These two left cosets $3\mathbb{Z}$ and $1 + 3\mathbb{Z}$ still do not yet exhaust all elements of $\mathbb{Z}$. For example, 2 is in neither of them. Then we find the left coset containing 2 is

$$2 + 3\mathbb{Z} = \{\dots, -7, -4, -1, 2, 5, 8, 11, \dots\}$$

It is clear that these three left cosets we have found do exhaust $\mathbb{Z}$, so they constitute $\mathbb{Z}$ by three left cosets of $3\mathbb{Z}$.

Left and Right Cosets

Example 5.2 Consider the symmetric group S_3 (Example 3.7).

(1) $$H = \left\{ e, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

is a subgroup of S_3.

We now compute the left and right cosets of H in S_3. The left cosets of H in S_3 are

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} H = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} H = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} H = H$$

and

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} H = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} H = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} H =$$
$$\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

Left and Right Cosets

and the right cosets of H in are

$$H\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=H\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=H\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=H$$

and

$$H\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=H\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=H\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=$$
$$\left\{\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\right\}.$$

Thus, for all $a \in S_3$, $aH = Ha$.

Left and Right Cosets

(2) $$H' = \left\{ e, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$$

is also a subgroup of S_3.

Now we compute the left and right cosets of H' in S_3. The left cosets of H' in S_3

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} H' = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} H' = H',$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} H' = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} H' = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\},$$

and

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} H' = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} H' = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}$$

Left and Right Cosets

and the right cosets of H' in S_3 are

$$H'\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=H'\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=H',$$

$$H'\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=H'\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\left\{\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\right\},$$

and

$$H'\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=H'\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\left\{\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\}.$$

We see that

$$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}H'\neq H'\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}.$$

Thus, the left and right cosets of H' in S_3 are not the same.

Left and Right Cosets

There are some interesting phenomena happening in the above example.

- We see that all left and right cosets of H in S_3 have the same number of elements, namely, 3; that there are the same number of distinct left cosets of H in S_3 as of right cosets, namely, 2; that the set of all left cosets and the set of all right cosets form partitions of S_3; and, finally, that $3 \cdot 2$ equals the order of S_3.
- Similar statements hold for the subgroup H'. We show, in the results to follow, that these phenomena hold in general.

5.1 Lagrange's Theorem (ラグランジュの定理)

Left and Right Cosets

The following theorem tells us **when two left (right) cosets are equal**. It is a result that is used often in the study of groups.

Theorem 5.1

Let $(H,\circ)$ be a **subgroup** of a **group** $(G,\circ)$ and $a, b \in G$. Then
(i) $aH = bH$ if and only if $b^{-1}a \in H$.
(ii) $Ha = Hb$ if and only if $ab^{-1} \in H$.

Theorem 5.2

Let $(H,\circ)$ be a **subgroup** of a **group** $(G,\circ)$. Then for all $a, b \in G$, either $aH = bH$ or $aH \cap bH = \emptyset$ (i.e., two left cosets are either equal or they are disjoint). Similar result also satisfied for two right cosets.

5.1 Lagrange's Theorem (ラグランジュの定理)

Number of Distinct Cosets

Definition 5.2

Let $(H,\circ)$ be a subgroup of a group $(G,\circ)$. Then the number of distinct (相異なる) left (or right) cosets, written as $[G:H]$, of H in G is called the index of H in G.

Theorem 5.3 (Lagrange's Theorem)

Let $(H,\circ)$ be a **subgroup** of a **finite group** $(G,\circ)$. Then **the order of** $(H,\circ)$ **divides the order of** $(G,\circ)$. In particular,

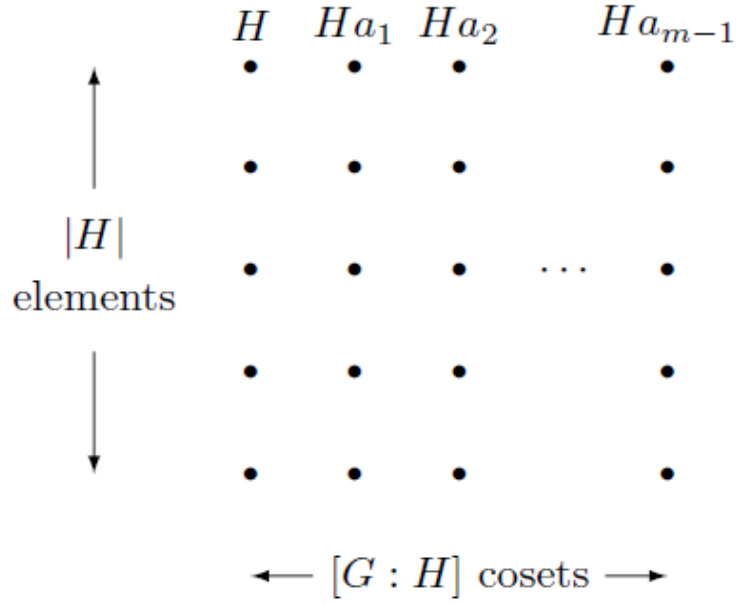
$$|G| = [G : H]|H|.$$

Proof:

Suppose that $[G : H] = m$. Every element of G is in a coset of H, and Theorem 4.8 tells us we can decompose G into a union of m pairwise disjoint cosets:

$$G = H \cup Ha_1 \cup Ha_2 \cup \cdots \cup Ha_{m-1}$$

But each of these cosets has $|H|$ elements. Thus, there must be $[G : H]|H|$ elements in G altogether.



Lagrange's Theorem

Theorem 5.4

Every group of prime order is cyclic.

Proof:

Let group $(G,\circ)$ be of prime order p, and let a be an element of G different from the identity element e.

Then the cyclic subgroup $(\langle a\rangle,\circ)$ of $(G,\circ)$ generated by a has at least two elements, a and e.

But by Lagrange's Theorem, the order $m \geq 2$ of $\langle a\rangle$ must divide the prime p.

Thus we must have $m = p$ and $\langle a\rangle = G$, so $(G,\circ)$ is cyclic.

5.2 Normal Subgroup (正規部分群) &

Quotient Group (商群)

Normal Subgroup

Definition 5.3

Let $(G,\circ)$ be a group. A subgroup $(H,\circ)$ of $(G,\circ)$ is said to be a **normal subgroup (正規部分群) (or invariant subgroup)** of G if $aH = Ha$ for all $a \in G$.

Example 5.3 Let $(G,\circ)$ be an **abelian group**. Every subgroup $(H,\circ)$ of $(G,\circ)$ is a normal subgroup.
Since $gh = hg$ for all $g \in G$ and $h \in H$, it will always be the case that $gH = Hg$.

Example 5.4 Let $(H,\circ)$ be the subgroup of S_3 consisting of elements (1) and $(1\ 2)$. Since

$(1\ 2\ 3)H = \{(1\ 2\ 3),(1\ 3)\}$ and $H(1\ 2\ 3) = \{(1\ 2\ 3),(2\ 3)\}$;

$(H,\circ)$ cannot be a normal subgroup of S_3.

However, the subgroup $(N,\circ)$, consisting of the permutations $(1), (123)$, and (132), is normal since the cosets of N are

$$N = \{(1),(1\ 2\ 3),(1\ 3\ 2)\}$$

$$(1\ 2)N = N(1\ 2) = \{(1\ 2),(1\ 3),(2\ 3)\}$$

Example 5.5

Recall Example 5.2. $(H,\circ)$ is a normal subgroup of S_3. Consider $h = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in H$. Then

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ h = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

and

$$h \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Hence,

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ h \neq h \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

even though

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} H = H \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Normal Subgroup

Theorem 5.5

Let $(H,\circ)$ be a subgroup of a group $(G,\circ)$. Then $(H,\circ)$ is a **normal subgroup** of $(G,\circ)$ **if and only if** for all $a \in G$, $aHa^{-1} \subseteq H$.

Proof:

Theorem 5.6

Let $(H,\circ)$ and $(L,\circ)$ be **normal subgroups of a group** $(G,\circ)$. Then

(i) $H \cap L$ **generates a normal subgroup of** $(G,\circ)$,

(ii) $HL = LH$ **generates a normal subgroup of** $(G,\circ)$,

(iii) $\langle H \cup L \rangle = HL$.

Quotient Subgroup

Definition 5.4

Let $(G,\circ)$ be a group and $(H,\circ)$ be a **normal subgroup** of $(G,\circ)$. The **group** $(G/H,\circ)$ is called the **quotient group (商群)** (or **factor group**) of G by H.

Theorem 5.7

Let $(H,\circ)$ be a **normal subgroup** of a group $(G,\circ)$. Denote the set of all left cosets $\{aH \mid a \in G\}$ by G/H and define $\circ$ on G/H by for all $aH, bH \in G/H$,

$$(aH) \circ (bH) = abH$$

Then $(G/H,\circ)$ is a **quotient group (商群)**.

Quotient Subgroup

Example 5.6

the normal subgroup of S_3 in Example 3.7,
$H = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$.
The cosets of H in S_3 are H and $(1\ 2)H$ from Example 5.2.
The quotient group S_3/H has the following operation table by $aH, bH \in S_3/H$ in Theorem 5.7. (Here $aH = H$, $bH = (1\ 2)H$)

	H	$(1\ 2)H$
H	H	$(1\ 2)H$
$(1\ 2)H$	$(1\ 2)H$	H

Quotient Subgroup

Example 5.7

Consider the normal subgroup $3\mathbb{Z}$ of $\mathbb{Z}$ (Example 5.1). The cosets of $3\mathbb{Z}$ in $\mathbb{Z}$ are

$$0 + 3\mathbb{Z} = \{\dots, -3, 0, 3, 6, \dots\}$$
$$1 + 3\mathbb{Z} = \{\dots, -2, 1, 4, 7, \dots\}$$
$$2 + 3\mathbb{Z} = \{\dots, -1, 2, 5, 8, \dots\}$$

The group $\mathbb{Z}/3\mathbb{Z}$ is given by the operation table below.

$+$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$0+3\mathbb{Z}$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$1+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$	$0+3\mathbb{Z}$
$2+3\mathbb{Z}$	$2+3\mathbb{Z}$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$

Quotient Subgroup

In general, the subgroup $(n\mathbb{Z},\circ)$ of $(\mathbb{Z},\circ)$ is **normal**. The cosets of $\mathbb{Z}/n\mathbb{Z}$ are

$$n\mathbb{Z}$$
$$1+n\mathbb{Z}$$
$$2+n\mathbb{Z}$$
$$\vdots$$
$$(n-1)+n\mathbb{Z}.$$

The sum of the cosets $k+\mathbb{Z}$ and $l+\mathbb{Z}$ **is** $k+l+\mathbb{Z}$.
Notice that we have written our cosets additively, because the group operation is integer addition.

Quotient Subgroup

Example 5.8 Consider $\mathbb{Z}_8$ (see Example 2.7) and let $H = \{[0], [4]\}$. Then $(H, \circ)$ is a normal subgroup of $(\mathbb{Z}_8, \circ)$. Now $|H| = 2$ and $|\mathbb{Z}_8| = 8$. Thus, $|\mathbb{Z}_8/H| = \frac{|Z8|}{|H|} = 4$. Hence, $\mathbb{Z}_8/H$ has four elements. We know

$$[0] + H = H = [4] + H,$$

$$[1] + H = \{[1], [5]\} = [5] + H,$$

$$[2] + H = \{[2], [6]\} = [6] + H,$$

and

$$[3] + H = \{[3], [7]\} = [7] + H.$$

Hence, $\mathbb{Z}_8/H = \{[0] + H, [1] + H, [2] + H, [3] + H\}$.

5.3 Homomorphism (準同型) and Isomorphism (同型) of Groups

Homomorphism

Definition 5.5

A **homomorphism (準同型)** between groups $(G_1,\circ)$ and $(G_2,*)$ is a function (or map) $f : G_1 \to G_2$ such that

$$f(a \circ b) = f(a) * f(b).$$

for all $a, b \in G_1$.

(Here $\circ$ and $*$ are two binary operations.)

Example 5.9

Let $(\mathbb{Z}, +)$ and $(G, \cdot)$ be groups and $g \in G$.

Define a function $f: \mathbb{Z} \to G$ by $f(n) = g^n$. Then f is a group homomorphism, since

$f(m+n) = g^{m+n} = g^m g^n = f(m)f(n)$:

This homomorphism maps $\mathbb{Z}$ onto the **cyclic subgroup** of G generated by g.

Example 5.10

We define a circle group $(T,\circ)$ consists of all **complex numbers** $z \in \mathbb{C}$ such that $|z| = 1$. We can define a homomorphism f from the additive group of real numbers $\mathbb{R}$ to T by

$f: \theta \mapsto \cos\theta + i\sin\theta.$

Indeed, for $\alpha, \beta \in \mathbb{R}$, we have

$$f(\alpha+\beta) = \cos(\alpha+\beta) + i\sin(\alpha+\beta)$$

$$= (\cos\alpha\cos\beta - \sin\alpha\sin\beta) + i(\sin\alpha\cos\beta + \cos\alpha\sin\beta)$$

$$= (\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta)$$

$$= f(\alpha)f(\beta):$$

Theorem 5.11

Let f be a **homomorphism** of a group $(G_1,\circ)$ into a group $(G_2,*)$.

Then

(i) $f(e_1) = e_2$.

(ii) $f(a^{-1}) = [f(a)]^{-1}$ for all $a \in G_1$.

(iii) If H_1 is a subgroup of G_1, then $f(H_1) = \{f(h) \mid h \in H_1\}$ is a subgroup of G_2.

(iv) If G_1 is commutative, then $f(G_1)$ is commutative.

Kernel

*Definition 5.6

Let f be a homomorphism of a group $(G_1,\circ)$ into a group $(G_2,*)$.

The **kernel** of f, written $Ker\ f$, is defined to be the set

$$Ker\ f = \{a \in G_1 \mid f(a) = e_2\}.$$

*Theorem 5.12

Let f be a homomorphism of a group $(G_1,\circ)$ into a group $(G_2,*)$.

Then $(Ker\ f,\circ)$ is a **normal subgroup** of $(G_1,\circ)$.

Notice: * mark is optional material. It will not be included in both middle and final examinations.

Isomorphism

*Definition 5.7

A **homomorphism** f **of a group** $(G_1,\circ)$ **into a group** $(G_2,*)$ is called an **isomorphism (同型)** of G_1 onto G_2 if f is **one-to-one** and **onto** G_2. In this case, we write $G_1 \simeq G_2$ and say that G_1 and G_2 are **isomorphic**.

Isomorphism

***Example 5.11** Let G be a cyclic group with generator g.

Define a map $f: \mathbb{Z} \to G$ by $n \mapsto g^n$. This map is a **surjective homomorphism** since $f(m+n) = g^{m+n} = g^m g^n = f(m)f(n)$:

Clearly f is **onto**. If $|g| = m$, then $g^m = e$.

Hence, $ker\ f = m\mathbb{Z}$ and $\mathbb{Z}/ker\ f = \mathbb{Z}/m\mathbb{Z} \simeq G$.

On the other hand, if the order of g is **infinite**, then $ker\ f = 0$ and f is an **isomorphism** of G and $\mathbb{Z}$.

Hence, **two cyclic groups** are **isomorphic** exactly when they have the **same order**.

Up to **isomorphism**, the only **cyclic groups** are $\mathbb{Z}$ and $\mathbb{Z}_n$.

Isomorphism

*Theorem 5.13

Every **finite cyclic group** of **order** n is **isomorphic** to $(\mathbb{Z}_n, +_n)$ and every **infinite cyclic group** is **isomorphic** to $(\mathbb{Z}, +)$.

Review for Lecture 5

- Lagrange's Theorem (ラグランジュの定理)
- Normal Subgroup (正規部分群)
- Quotient Group (商群)
- Homomorphism (準同型) of Groups
- Isomorphism (同型) of Groups

Assignment

Please Check https://github.com/uoaworks/Applied-Algebra

References

[1] Thomas W. Judson etc. Abstract Algebra Theory and Applications, 2018

[2] D. S. Malik, John N. Mordeson, M.K. Sen, Introduction to Abstract Algebra, 2007

[3] **(おすすめ)** 松本 眞, 代数系への入門, http://www.math.sci.hiroshima-u.ac.jp/~m-mat/TEACH/daisu-nyumon2014.pdf

[4] Wikipedia

[5] Materials from internet.

Appendix (付録)

Lagrange's Theorem

*Theorem

Let $(H,\circ)$ and $(L,\circ)$ be finite subgroups of a group $(G,\circ)$. Then the order

$$|HL| = \frac{|H||L|}{|H \cap L|}$$