



Lecture 4

Subgroup & Cyclic Group & Lagrange's Theorem

What you will learn in Lecture 4

4.1 Subgroup (部分群)

4.2 Cyclic Group (巡回群)

4.3 Lagrange's Theorem (ラグランジュの定理)

4.1 Subgroup (部分群)

Let us consider the groups $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$, where $+$ is the usual addition of numbers, and note the following:

1. Both these groups have the same binary operation.
2. \mathbb{Z} is a subset of \mathbb{Q} .

The same is true for the groups $(\mathbb{Z}, +)$ and $(\mathbb{R}, +)$; $(\mathbb{Q}, +)$ and $(\mathbb{R}, +)$; $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$.

4.1 Subgroup (部分群)

This leads us to the concept of a **subgroup**. Before formally defining subgroups, let us also note the following:

Let (G, \circ) be a **group** and H be a **nonempty subset** of G . Then H is said to be **closed** under the **binary operation** \circ if $a \circ b \in H$ for all $a, b \in H$.

Suppose H is **closed** under the **binary operation** \circ . Then the restriction of \circ to $H \times H$ is a mapping from $H \times H$ into H . Thus, the binary operation \circ defined on G induces a **binary operation** on H . We denote this induced binary operation on H by \circ also. Thus, (H, \circ) is a **mathematical system**.

It also follows that \circ is **associative** as a binary operation on H , i.e., $a \circ (b \circ c) = (a \circ b) \circ c$ for all $a, b, c \in H$.

If (H, \circ) is a **group**, then we call H a **subgroup** of G .

4.1 Subgroup (部分群)

More formally, we have the following definition.

Definition 4.1

Let (G, \circ) be a group and H be a nonempty subset of G . If (H, \circ) is a group, then (H, \circ) is called a subgroup of (G, \circ) .

For example, consider the rational number group $(\mathbb{Q}, +)$ and its subgroups $(\mathbb{Z}, +)$. Now the identity elements of both these groups is 0.

Next, let $a \in \mathbb{Z}$. Then $a \in \mathbb{Q}$.

Also, the inverse of a in \mathbb{Z} as well as in \mathbb{Q} is $-a$.

In other words, the inverse of a in \mathbb{Z} and the inverse of a in \mathbb{Q} is the same.

4.1 Subgroup (部分群)

In general, we have the following result.

Theorem 4.1

Let (G, \circ) be a group and (H, \circ) be a subgroup of (G, \circ) .

- (i) The identity elements of (H, \circ) and (G, \circ) are the same.
- (ii) If $h \in H$, then the inverse of h in H and the inverse of h in G is the same.

Remark

If (G, \circ) is a group, then $(\{e\}, \circ)$ and (G, \circ) are subgroups of (G, \circ) . These subgroups are called trivial subgroup (自明な部分群).

4.1 Subgroup (部分群)

Example 4.1

Consider the following list of groups.

(i) $(\{0\}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$,

(ii) $(\{1\}, \cdot)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$,

where $+$ is the usual addition operation and \cdot is the usual multiplication operation.

Each group is a subgroup of the group listed to its right.

For example, $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$, and $(\mathbb{R} \setminus \{0\}, \cdot)$ is a subgroup of $(\mathbb{C} \setminus \{0\}, \cdot)$.

4.1 Subgroup (部分群)

Theorem 4.2

Let (G, \circ) be a group and H be a nonempty subset of G . Then (H, \circ) is a subgroup of (G, \circ) if and only if for all $a, b \in H$, $ab^{-1} \in H$.

Proof.

4.1 Subgroup (部分群)

Example 4.2 Find all subgroups of $(\mathbb{Z}, +)$.

Solution: Let $(H, +)$ be a subgroup of $(\mathbb{Z}, +)$. Suppose $H \neq \{0\}$.

Let a be a nonzero element of H . Then $-a \in H$. Since either a or $-a$ is a positive integer, H contains a positive integer. With the help of the principle of well-ordering, we can show that H contains a smallest positive integer. Let a be the smallest positive integer in H . We claim that $H = \{na \mid n \in \mathbb{Z}\}$.

Now $na \in H$ for all $n \in \mathbb{Z}$ and so $\{na \mid n \in \mathbb{Z}\} \subseteq H$. On the other hand, let $b \in H$.

By the division algorithm, there exist c and r in \mathbb{Z} such that $b = ca + r$, where $0 \leq r < a$. Suppose $r \neq 0$. Then $r = b - ca \in H$. Thus, H contains a positive integer smaller than a , a contradiction.

Hence, $r = 0$ and so $b = ca \in \{na \mid n \in \mathbb{Z}\}$.

This implies that $H \subseteq \{na \mid n \in \mathbb{Z}\}$. Thus, $H = \{na \mid n \in \mathbb{Z}\}$ for some $a \in \mathbb{Z}$. Also, for all $n \in \mathbb{Z}$, the set $T = \{nm \mid m \in \mathbb{Z}\} = n\mathbb{Z}$ generate a subgroup of $(\mathbb{Z}, +)$.

Hence, $(n\mathbb{Z}, +)$, $n = 0, 1, 2, \dots$ are the subgroups of $(\mathbb{Z}, +)$.

4.1 Subgroup (部分群)

Definition 4.2

Let H and L be nonempty subsets of G from a group (G, \circ) .
The product of H and L is defined to be the set
 $HL = \{hl \mid h \in H, l \in L\}$.

Example 4.3

Consider the group of symmetries of the square.

Let $H = \{r_{360}, d_1\}$ and $L = \{r_{360}, h\}$. Then H and L are subgroups of G . Now

$$HL = \{r_{360}r_{360}, r_{360}h, d_1r_{360}, d_1h\} = \{r_{360}, h, d_1, r_{90}\}.$$

Now $hd_1 = r_{270} \notin HL$, so HL is **not closed** under the binary operation.

Hence, HL is **not a subgroup** of the symmetries of the square. Also, note that

$$LH = \{r_{360}r_{360}, r_{360}d_1, hr_{360}, hd_1\} = \{r_{360}, d_1, h, r_{270}\},$$

And $\langle H \cup L \rangle = \{r_{360}, r_{90}, r_{180}, r_{270}, h, d_1, d_2\}$.

This example shows that in general the product of subgroups need not be a subgroup.

4.1 Subgroup (部分群)

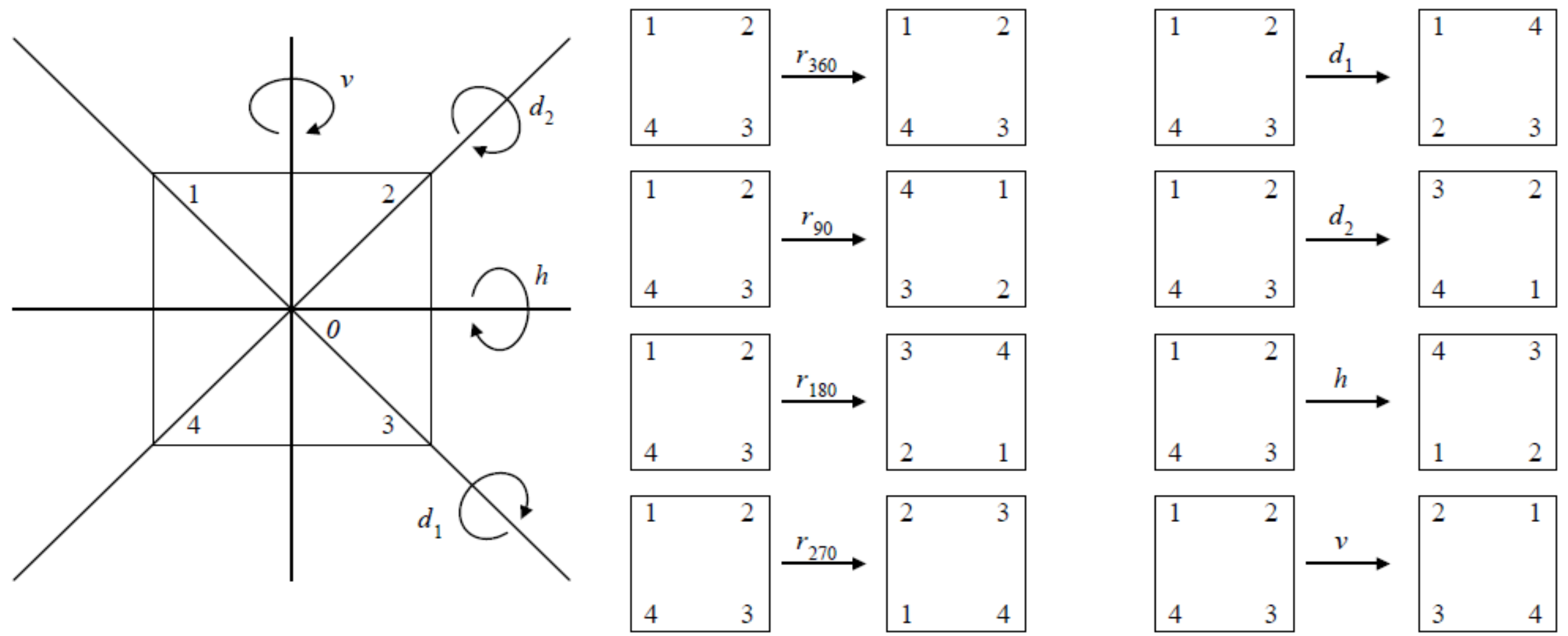
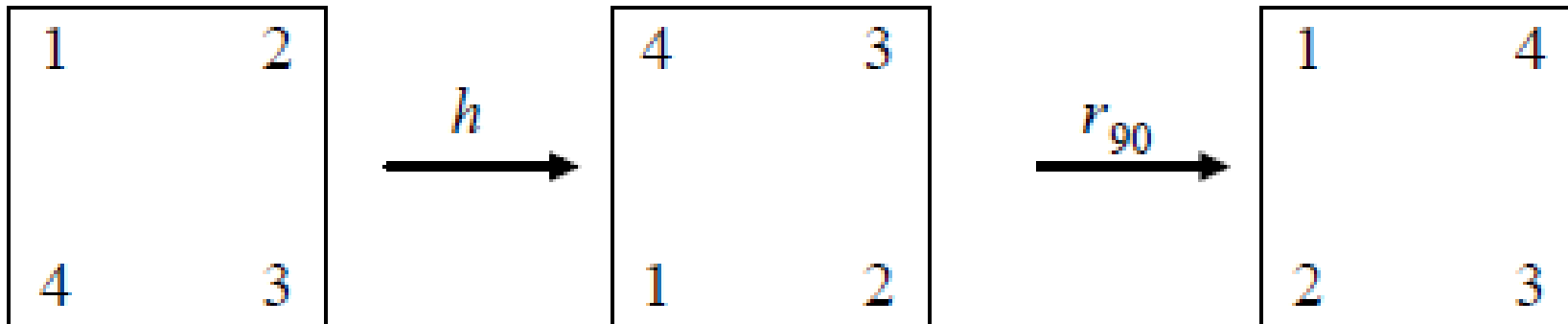


Figure. Rigid motions of a square in symmetry

4.1 Subgroup (部分群)

$$r_{90} \circ h$$



4.1 Subgroup (部分群)

The complete operation table for the operation \circ is as following

\circ	r_{360}	r_{90}	r_{180}	r_{270}	h	v	d_1	d_2
r_{360}	r_{360}	r_{90}	r_{180}	r_{270}	h	v	d_1	d_2
r_{90}	r_{90}	r_{180}	r_{270}	r_{360}	d_1	d_2	v	h
r_{180}	r_{180}	r_{270}	r_{360}	r_{90}	v	h	d_2	d_1
r_{270}	r_{270}	r_{360}	r_{90}	r_{180}	d_2	d_1	h	v
h	h	d_2	v	d_1	r_{360}	r_{180}	r_{270}	r_{90}
v	v	d_1	h	d_2	r_{180}	r_{360}	r_{90}	r_{270}
d_1	d_1	h	d_2	v	r_{90}	r_{270}	r_{360}	r_{180}
d_2	d_2	v	d_1	h	r_{270}	r_{90}	r_{180}	r_{360}

4.1 Subgroup (部分群)

In the following theorem, we give a necessary and sufficient condition for the product of subgroups to be a subgroup.

Theorem 4.3

Let (H, \circ) and (L, \circ) be subgroups of a group (G, \circ) . Then (HL, \circ) is a subgroup of (G, \circ) if and only if $HL = LH$.

Corollary 3.2

If (H, \circ) and (L, \circ) are subgroups of a commutative group (G, \circ) , then (HL, \circ) is a subgroup of (G, \circ) .

4.2 Cyclic Group (巡回群)

4.2 Cyclic Group (巡回群)

In the previous section, we introduced the notion of a subgroup generated by a set. **Groups that are generated by a single element, called cyclic groups**, are of special importance. Cyclic groups are easier to study than any other group.

Definition 4.3

A group (G, \circ) is called a **cyclic group** if there exists $a \in G$ such that
$$G = \langle a \rangle$$
where $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

Let $G = \langle a \rangle$ defines a cyclic group and $b, c \in G$. Then $b = a^n$ and $c = a^m$ for some $n, m \in \mathbb{Z}$. Now

$$bc = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = cb.$$

This shows that G is **commutative**. Hence, every cyclic group is **commutative**. We record this result in the following theorem.

4.2 Cyclic Group (巡回群)

Theorem 4.4

Every cyclic group is commutative.

Example 4.4

- (i) $(\mathbb{Z}, +)$ is a cyclic group because $\mathbb{Z} = \langle 1 \rangle$.
- (ii) $(\{na \mid n \in \mathbb{Z}\}, +)$ is a cyclic group, where a is any fixed element of \mathbb{Z} .

4.2 Cyclic Group (巡回群)

Example 4.5

Consider the set $G = \{e, a, b, c\}$. Define \circ on G by means of the following operation table.

\circ	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

From the multiplication table, it follows that (G, \circ) is a **commutative** group. **However, G is NOT a cyclic group** because

$\langle e \rangle = \{e\}$, $\langle a \rangle = \{e, a\}$, $\langle b \rangle = \{e, b\}$, and $\langle c \rangle = \{e, c\}$

and each of these subgroups is properly contained in G . G is known as the **Klein 4-group** (クラインの四元群).

4.2 Cyclic Group (巡回群)

Theorem 4.5

Let $\langle a \rangle$ be a finite cyclic group of order n .
Then $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$.

Theorem 4.6

Every subgroup of a cyclic group is cyclic.

4.2 Cyclic Group (巡回群)

Corollary 3.2

Let $G = \langle a \rangle$ be a cyclic group of order n , $n > 1$, and H be a proper subgroup of G .

Then $H = a^k$ for some integer k such that k divides n and $k > 1$.
Furthermore, the order $|H|$ divides n .

4.3 Lagrange's Theorem

(ラグランジュの定理)

4.3 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.

4.3 Lagrange's Theorem (ラグランジュの定理)

Definition 4.4

Let H be a subgroup of a group G 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 $a = ea \in Ha$.

4.3 Lagrange's Theorem (ラグランジュの定理)

Example 4.6 Consider the symmetric group S_3 (Example 3.7).

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

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

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

4.3 Lagrange's Theorem (ラグランジュの定理)

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 $a \in S_3$, $aH = Ha$.

4.3 Lagrange's Theorem (ラグランジュの定理)

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

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

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

4.3 Lagrange's Theorem (ラグランジュの定理)

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.

4.3 Lagrange's Theorem (ラグランジュの定理)

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.

4.3 Lagrange's Theorem (ラグランジュの定理)

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 4.7

Let H be a subgroup of a group G 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 4.8

Let H be a subgroup of a group G . 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).

4.3 Lagrange's Theorem (ラグランジュの定理)

Definition 4.5

Let H be a subgroup of a group G . 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 .

4.3 Lagrange's Theorem (ラグランジュの定理)

Theorem 4.9 (Lagrange's Theorem)

Let H be a subgroup of a finite group G . Then the order of H divides the order of G . In particular,

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

4.3 Lagrange's Theorem (ラグランジュの定理)

Theorem 4.10

Let H and L be finite subgroups of a group G . Then

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

Review for Lecture 4

- Subgroup (部分群)
- Trivial Subgroup (自明な部分群)
- Cyclic Group (巡回群)
- Left and Right Cosets (左剰余類と右剰余類)
- Lagrange's Theorem (ラグランジュの定理)

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.