Lecture 6

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

What you will learn in Lecture 6

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

6.2 Solutions/Hints of Assignments

6.3 Exercises

6.4 Quiz 1

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

Definition 6.1

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 6.1

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 (準同型) maps $\mathbb{Z}$ onto the **cyclic subgroup** of G generated by g.

Example 6.2
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

$$\begin{aligned} f(\alpha+\beta) &= \cos(\alpha+\beta) + i\sin(\alpha+\beta) \\ &= (\cos\alpha\cos\beta - \sin\alpha\sin\beta) + i(\sin\alpha\cos\beta + \cos\alpha\sin\beta) \\ &= (\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) \\ &= f(\alpha)f(\beta) \end{aligned}$$

Theorem 6.1

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.

*Definition 6.2

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**.

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

*Example 6.3

Let us show that the mathematical structure $\langle \mathbb{R}, + \rangle$ with operation the usual addition is **isomorphic** to the structure $\langle \mathbb{R}^+, \cdot \rangle$ where $\cdot$ is the usual multiplication. (Here $\mathbb{R}^+$ denotes the **set of positive numbers of** $\mathbb{R}$.)

1. We have to somehow convert an operation of addition to multiplication. Recall from $a^{b+c} = (a^b)(a^c)$ that addition of exponents corresponds to multiplication of two quantities.
Thus we try defining $f: \mathbb{R} \to \mathbb{R}^+$ by $f(x) = e^x$ for $x \in \mathbb{R}$.
Note that $e^x > 0$ for all $x \in \mathbb{R}$, so indeed $f(x) \in \mathbb{R}^+$.

2. If $f(x) = f(y)$ then $e^x = e^y$.Taking the natural logarithm, we see that $x = y$, so f is indeed ***one-to-one***.

3. If $r \in \mathbb{R}^+$, then $\ln(r) \in \mathbb{R}$ and $f\big(\ln(r)\big) = e^{\ln(r)} = r$. Thus f is ***onto*** $\mathbb{R}^+$.

4. For $x, y \in \mathbb{R}$, we have $f(x+y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y)$. Thus we see that f is indeed an **isomorphism**.

Solutions/Hints of Assignments

Exercises

1. Determine whether the binary operation $\circ$ on $\mathbb{Z}$ by letting $a \circ b = a - b$ is commutative and whether $\circ$ is associative.

2.Consider Example 3.7, write the permutation α_4 and α_5 of S_3 as product of transpositions.

$$\alpha_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\alpha_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$(1\ 2\ 3) = (1\ 3)(1\ 2)$$

$$(1\ 3\ 2) = (1\ 2)(1\ 3)$$

3. Determine whether the binary operation gives a group structure on the given set.

(1) Let $\circ$ be defined on $\mathbb{R}^+$ by letting $a \circ b = \sqrt{ab}$

(2) Let $\circ$ be defined on $\mathbb{R}^+$ by letting $a \circ b = a/b$

4. Let $(G,\circ)$ be a group and suppose that $a \circ b \circ c = e$ for $a, b, c \in G$. Show that $b \circ c \circ a = e$ is also satisfied.

5.(1)Complete the table to give the group $\mathbb{Z}_6$ with modular addition operation.

(2)Compute the subgroups $\langle 0\rangle, \langle 1\rangle, \langle 2\rangle, \langle 3\rangle, \langle 4\rangle$ and $\langle 5\rangle$ of the group $\mathbb{Z}_6$ given in question (1).

(3)Can we say $\mathbb{Z}_6$ is a cyclic group?

(4)Find the order of the cyclic subgroup $\langle 3\rangle$.

(5)Which elements are generators for the group $\mathbb{Z}_6$ of question (1)?

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1					
2	2					
3	3					
4	4					
5	5					

Quiz 1

Q1. (1)Write the following permutations as cycle notation.

(2)Compute the indicated product $\pi\sigma$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix} \quad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}$$

Q2. (1)Complete the table to give the group $\mathbb{Z}_4$ with modular addition operation.

(2)Compute the subgroups $\langle 0\rangle, \langle 1\rangle, \langle 2\rangle$ and $\langle 3\rangle$ of the group $\mathbb{Z}_4$ given in question (1).

(3)Find the order of the cyclic subgroup $\langle 3\rangle$.

+	0	1	2	3
0	0	1	2	3
1	1			
2	2			
3	3			

Review for Lecture 6

- 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 the internet.

*Theorem

Let $f: A \to B$, $g: B \to C$, and $h: C \to D$. Then

1. The composition of mappings is associative; that is, $(h \circ g) \circ f = h \circ (g \circ f)$;
2. If f and g are both ***one-to-one***, then the mapping $g \circ f$ is ***one-to-one***;
3. If f and g are both ***onto***, then the mapping $g \circ f$ is ***onto***;
4. If f and g are ***bijective***, then so is $g \circ f$.

*Definition

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

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

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

*Theorem

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

*Example

Let $(G,\circ)$ 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 (onto) 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 $\mathbb{Z}_n$.

Appendix (付録)

*Theorem

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