Lectures schedule

28th Jan

29th Jan [Extra Lecture] Missing class } Homomorphism & Isomorphism with Problem session

1st feb

3rd feb

4th feb

8th feb [Make-up lecture] Problem session

10th feb [Exam] ~ 30 marks

Thursday 12pm (approx.) 50 mins.

2 Short Quizzes : 30th January ~ 5 marks

May be 6th ~~5th~~ february ~ 5 marks

Lecture 9 (MA2070)

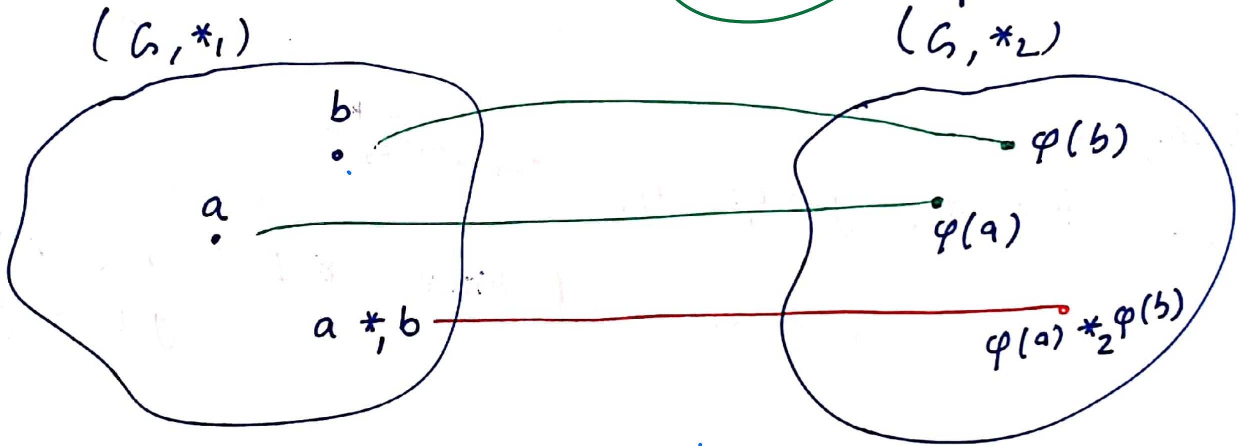
January 28, 2022

Group Isomorphism.

Let $(G, *_1)$ and $(G', *_2)$ be groups.

An isomorphism $\varphi : G \longrightarrow G'$ is a bijective map that preserves the group operation, i.e.,

$$\varphi(a *_1 b) = \varphi(a) *_2 \varphi(b) \quad \forall a, b \in G.$$



$(G, *_1)$	$(G', *_2)$	$\varphi(a *_1 b) = \varphi(a) *_2 \varphi(b)$
$\cdot$	$\cdot$	$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$
$\cdot$	$+$	$\varphi(a \cdot b) = \varphi(a) + \varphi(b)$
$+$	$\cdot$	$\varphi(a + b) = \varphi(a) \cdot \varphi(b)$
$+$	$+$	$\varphi(a + b) = \varphi(a) + \varphi(b)$

Definition. Two groups G and G' are called isomorphic if there exists an isomorphism

$$\varphi : G \to G'.$$

Notation. $G \approx G'$ $\quad$ G is isomorphic to G' [Artin]

$G \cong G'$ $\quad$ "

Example.

(1). For any group G, ~~$G \approx G$~~

$G \approx G$ $\quad$ [Since $\mathrm{Id} : G \to G$, $g \mapsto g$]

(2) $G = (\mathbb{Z}, +)$ and $G' = (G, \cdot)$ Cyclic group $= \langle a \rangle$

$\{\ldots, a^{-2}, a^{-1}, 1, a, a^2, \ldots\}$

an infinite cyclic group.

$$\varphi : \mathbb{Z} \longrightarrow G$$
$$n \longmapsto a^n$$

Is this φ an isomorphism? Yes.

Note. An infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$.

To check that $\varphi : G \to G'$ is an isomorphism,

we need to show

(i) φ is a function

(ii) φ is one-one

(iii) φ is onto

(iv) $\varphi(ab) = \varphi(a)\varphi(b) \ \forall a, b \in G$

Now;

$$\varphi : \underset{(\mathbb{Z},+)}{\mathbb{Z}} \longrightarrow \underset{(\mathbb{C},\cdot)}{\mathbb{C}}$$

$$n \longmapsto a^n$$

$$\varphi(n) = \varphi(m) \Rightarrow n = m.$$

one - one : ~~$\varphi(a) = \varphi(b) \Rightarrow a = b$~~

onto : For every element a^n; $\exists$ some element $x \in \mathbb{Z}$ s.t. $\varphi(x) = a^n$, $x = n$

$$\varphi(n) = \varphi(m)$$

$$a^n = a^m \Rightarrow a^{n-m} = 1$$

$$\Rightarrow n - m = 0$$

$$\Rightarrow n = m$$

$\varphi(ab) = \varphi(a)\varphi(b)$

$$\varphi(m+n) = \varphi(m)\varphi(n)$$

$$a^{m+n} = a^m \cdot a^n = \varphi(m)\cdot\varphi(n)$$

Example (3).

$$G = \{1, x, x^2, \dots, x^{n-1}\} = \langle x \rangle$$

$$G' = \{1, y, y^2, \dots, y^{n-1}\} = \langle y \rangle$$

$\mathrm{ord}(x) = n$

$\mathrm{ord}(y) = n$

$$\varphi : (G, \cdot) \longrightarrow (G', \cdot)$$

$$x \longrightarrow y$$

Note that $x^i \longrightarrow y^i$ for all i

Prove that φ is an isomorphism.

Note. Two cyclic groups of the same order are isomorphic.

Example (4). $(\mathbb{R}, +)$ and $(\mathbb{R}_{>0}, \cdot)$

$\uparrow$ +ve real numbers

Define $\varphi : \mathbb{R} \longrightarrow \mathbb{R}_{>0}$

$$x \longmapsto e^x$$

Note that $\varphi : \mathbb{R} \longrightarrow \mathbb{R}_{>0}$ defined by

$$\varphi(x) \doteq e^{x} \quad \text{is well-defined.}$$

→ one-one ⟶ $\varphi(x) = \varphi(y)$

$\Rightarrow e^{x} = e^{y}$

$\Rightarrow \log_e e^{x} = \log_e e^{y}$

$\Rightarrow x = y$

→ onto

↓

For any real number $y \in \mathbb{R}_{>0}$

$\exists\ x$ s.t. $\varphi(x) = y$

?

$\Downarrow$

$e^{x} = y$

$\Rightarrow x = \log_e y \qquad \left[\because \begin{array}{l} y \neq 0 \\ y > 0 \end{array}\right]$

→ $\varphi(x+y)$

$= e^{x+y}$

$= e^{x} \cdot e^{y}$

$= \varphi(x)\,\varphi(y) \qquad \forall\ x, y \in (\mathbb{R}, +)$

φ is well-defined

φ is 1-1

φ is onto

$\varphi(ab) = \varphi(a)\,\varphi(b)$

Example (5). $G = (\mathbb{R}, +)$

$$G' = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \;\middle|\; x \in \mathbb{R} \right\}$$

Is this even a group?

Are $G = (\mathbb{R}, +)$ and $(G', \cdot)$ isomorphic?

Define

$$\varphi : G \longrightarrow G'$$
$$x \longmapsto \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$$

Check that φ is one-one onto.

$$\varphi(x+y) = \begin{bmatrix} 1 & x+y \\ 0 & 1 \end{bmatrix}$$
$$= \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix}$$
$$= \varphi(x)\, \varphi(y)$$

Example (6). $\varphi : (\mathbb{R}, +) \longrightarrow (\mathbb{R}, +)$

$$x \longmapsto x^n$$

φ is isomorphism if $n = 1$.

If $n > 1$; $\varphi(x+y) = (x+y)^n \neq x^n + y^n$

φ is not an isomorphism.

Example (7). $(\mathbb{Q}, +) \overset{?}{\cong} (\mathbb{Q}-\{0\}, \cdot)$

$(\mathbb{R}, +) \overset{?}{\cong} (\mathbb{Q}, +)$

Justify your answer! $(\mathbb{R}-\{0\}, \cdot) \overset{?}{\cong} (\mathbb{C}-\{0\}, \cdot)$

$(\mathbb{Z}, +) \overset{?}{\cong} (\mathbb{Q}, +)$

Properties of Isomorphisms.

$\varphi : G \longrightarrow G'$ is an isomorphism.

(1)

$$\varphi \quad \boxed{\varphi(1_G) = 1_{G'}}$$

[call 1_G as e and $1_{G'}$ as e']

$$e = e \cdot e$$

$$\varphi(e) = \varphi(e \cdot e) = \varphi(e)\,\varphi(e)$$

So, $\varphi(e) = \varphi(e)\,\varphi(e)$ — (I)

Now; $\varphi(e) \in G'$ and e' is in G'

$\varphi(e) = e'\,\varphi(e)$ — (II)

From (I) and (II),

$$\varphi(e)\,\varphi(e) = e'\,\varphi(e)$$

$\Rightarrow \varphi(e) = e'$ [using concellation law]

(2). $\boxed{\text{For all } a \in G, \text{ \& } \varphi : G \to G' \text{ isomorphism} \quad \varphi(a^n) = \varphi(a)^n \quad \forall n \in \mathbb{Z}.}$

Induction:

True for $n = 1$, $\varphi(a) = \varphi(a)$

$n = 2$; $\varphi(a^2) = \varphi(a \cdot a)$

$= \varphi(a)\,\varphi(a)$

$= \varphi(a)^2$

Assume that

$$\varphi(a^k) = \varphi(a)^k \quad \text{for all integers } k \leq n$$

$$\varphi(a^{k+1}) = \varphi(a^k \cdot a)$$

$$= \varphi(a^k)\,\varphi(a)$$

$$= (\varphi(a))^k \cdot \varphi(a)$$

$$= (\varphi(a))^{k+1}$$

True for all positive integers

Now we want to extend to all integers.

If n is negative; $-n$ is positive

$$e = \varphi(e) = \varphi(a^n \cdot a^{-n})$$

$$= \varphi(a^n)\,\varphi(a^{-n})$$

$$= \varphi(a^n) \cdot (\varphi(a))^{-n}$$

$$e = \varphi(e) = \varphi(a^n \cdot a^{-n})$$

$$= \varphi(a^n) \cdot \varphi(a^{-n})$$

$$= \varphi(a^n) \cdot (\varphi(a))^{-n} \quad [\because -n \text{ is positive}]$$

$$\Rightarrow \quad \varphi(a)^n = \varphi(a^n) \quad \text{for all } n \text{ negative integers.}$$

When $n = 0$;

$$\varphi(\underset{\overset{\parallel}{e}}{a^0}) = \varphi(e)$$

$$= e'.$$

Thus; $\varphi(x^n) = \varphi(x)^n \quad \forall\, n \in \mathbb{Z}.$

(3) For any element a and b in G, $\varphi : G \to G'$ isomorphism

~~a~~ $a * b = b * a$

$$\boxed{ab = ba \iff \varphi(a)\varphi(b) = \varphi(b)\varphi(a)}$$

(4) $\boxed{G = \langle a \rangle \iff G' = \langle \varphi(a) \rangle}$ $\varphi : G \to G'$ isomorphism

Proof.

$$\varphi : G \longrightarrow G'$$
$$a \longmapsto \varphi(a)$$

$\langle \varphi(a) \rangle \subseteq G'$ [since $\varphi(a) \in G'$]

Now, given that $G = \langle a \rangle$

$$\begin{array}{c}\langle a\rangle \\ \shortparallel \\ \varphi : G \longrightarrow G' \\ \quad\quad\quad \Downarrow \\ \quad\quad\quad b\end{array} \qquad\qquad \langle \varphi(a)\rangle \subseteq G'$$

$$\underset{(\supseteq)}{=} \quad \uparrow b$$

$\exists$ a^K for some K such that

$$\varphi(a^K) = b$$

$$\Rightarrow (\varphi(a))^K = b$$

$\Rightarrow b \in \langle \varphi(a)\rangle$ True for any $b \in G'$

$\boxed{\text{Hence } \langle \varphi(a)\rangle = G'}$.

Other way, Assume that $G' = \langle \varphi(a)\rangle$

we want to show $\langle a\rangle = G$.

Since $a \in G$, $\langle a\rangle \subseteq G$.

$\supseteq$ $\uparrow b$ (any such b)

$$G \longrightarrow G' = \langle \varphi(a)\rangle$$
$$b \longmapsto \varphi(b)$$

$$\Rightarrow \varphi(b) \in \langle \varphi(a)\rangle$$

$\Rightarrow \varphi(b) = (\varphi(a))^K$ for some $K \in \mathbb{Z}$

$= \varphi(a^K)$ for some K

Since φ is one-one

$\Rightarrow b = a^K$ for some K

$\Rightarrow b \in \langle a\rangle$. $\boxed{\text{Thus } \langle a\rangle = G}$

(5). $\varphi : G \longrightarrow G'$ isomorphism.

Then $o(a) = o(\varphi(a)) \quad \forall\, a \in G$.

(6). $\varphi : G \longrightarrow G'$ isomorphism

For fixed integer K and fixed element $b \in G$,

$x^K = b$ has same number of solutions in G as $x^K = \varphi(b)$ in G'.

Applications: (i) $(\mathbb{R}-\{0\}, \cdot) \not\cong (\mathbb{C}-\{0\}, \cdot)$

$x^4 = 1$ $\quad b^4 \qquad \varphi(b) \quad$ $x^4 = 1$

(7). $\varphi : G \longrightarrow G'$ isomorphism. If G is finite, then G and G' have exactly the same number of elements of every order.

Proof. Exercise.

(5), (6), (7)