Abstract Algebra Class Notes

3/25/2014

New HW will be announced on Thursday, March 27
Exam # 1 will be returned on Thursday, March 27
Math Colloquium: Wed, March 26 in SEC 105 from 3-4pm

Chapter 3 Section 5 – Isomorphisms

<u>Defn:</u> Let G be a group with respect to $\circledast$ and Let G' be a group with respect to $\boxed{*}$

Note! : The use of $\circledast$ and $\boxed{*}$ may be used to indicate different group operations.

A mapping $\phi: G \to G'$ is an <u>isomorphism</u> if

1) ϕ is bijective (aka it is both one-to-one <u>and</u> onto)
2) $\phi(x \circledast y) = \phi(x) \boxed{*} \phi(y)$ for all $x, y \in G$

If $\exists\, \phi: G \to G'$ is an isomorphism, then we say G and G' are <u>isomorphic</u>.

Note! : An isomorphism, $\phi: G \to G$, is called an <u>automorphism</u>.

Thm 3.26 – Images of Identities and Inverses

Let $\phi: G \to G'$ be an isomorphism, then

1) $\phi(e) = e'$, where $e' \in G'$

2) $\phi(x)^{-1} = \phi(x^{-1})$ for all $x \in G$

Proof:

Property 1 $\Rightarrow$ $\phi(e) = \phi(e \circledast e)$

$\Rightarrow \phi(e) \boxed{*} \phi(e)$

$\Rightarrow \phi(e)$ "Since ϕ is an isomorphism"

$\Rightarrow \phi(e) \boxed{*} \phi(e) = \phi(e) \circledast e'$ "Since e' is an identity"

$\Rightarrow \phi(e) = e'$

Property 2 $\Longrightarrow$ For any $x \in G$,

$$x \cdot x^{-1} = e \Rightarrow \phi(x \cdot x^{-1}) = \phi(e)$$

$$\Rightarrow \phi(x \cdot x^{-1}) = e'$$

$$\Rightarrow \phi(x) \cdot \phi(x^{-1}) = e'$$

$\boxed{\text{QED}}$

Note! : The concept of isomorphism indicates the relation of being isomorphic on a set of groups. We can then say that this relation is an <u>equivalence</u> <u>relation</u>

Example 1: $H = \{id, \alpha: \begin{matrix} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{matrix}, \alpha^2: \begin{matrix} 1 \mapsto 3 \\ 2 \mapsto 1 \\ 3 \mapsto 2 \end{matrix}\}$

and $H \subset S_3$

then, H is isomorphic to $\mathbb{Z}_3$ via,

$$\phi : H \to \mathbb{Z}_3, \text{ where } \begin{aligned} \phi(id) &= [0] \\ \phi(\alpha) &= [1] \\ \phi(\alpha^2) &= [2] \end{aligned}$$

Example 2: $G = \{1, i, -1, -i\}$ ← "The Fours Roots of Unity"
under multiplication
and is isomorphic to
$\mathbb{Z}_4$, where $\mathbb{Z}_4 = G'$

Remember $\Rightarrow \mathbb{Z}_4 = \{[0],[1],[2],[3]\}$

So,

$$\phi : \begin{aligned} 1 &\mapsto [0] \\ i &\mapsto [1] \\ -1 &\mapsto [2] \\ -i &\mapsto [3] \end{aligned} \qquad \underline{\text{or}} \qquad \begin{aligned} &\phi : G \to G' \\ &\phi(1) = [0] \\ &\phi(i) = [1] \\ &\phi(-1) = [2] \\ &\phi(-i) = [3] \end{aligned}$$

Example 3: Let $G = (\mathbb{R}, +)$ and $G' = (\mathbb{R}^{>0}, \cdot)$

Note! $(\mathbb{R}, \cdot)$ is not a valid group

so, $\phi : (\mathbb{R}, +) \to (\mathbb{R}^{>0}, \cdot)$ is an isomorphism

then, $\phi : (\mathbb{R}, +) \to (\mathbb{R}^{>0}, \cdot)$

$x \mapsto e^x$, where ϕ is the bijection.

Since ϕ is an isomorphism, $e^{x+y} = e^x \cdot e^y$

then, $\phi(x+y) = \phi(x) \cdot \phi(y)$

Example 4: Let $(m,n)=1$ } relatively prime

$$\phi : \mathbb{Z}_n \to \mathbb{Z}_n$$

$[x] \mapsto [mx]$ is an automorphism

Proof: $\phi([x]+[y]) = \phi([x+y])$

$$\Downarrow$$

$$[m(x+y)]$$

then, $\phi([x])+\phi([y]) = [mx]+[my] = [m(x+y)]$

$\Longrightarrow$ Property of Theorem 3.26 is satisfied ✓

What remains now is to check bijectivity,

Lemma: ϕ is injective $\Longleftrightarrow (\phi(x)=e \Leftrightarrow x=e)$

Proof of Lemma: "$\Longrightarrow$" This is clearly understood

"$\Longleftarrow$" Let $\phi([x]) = \phi([y])$

$$\Longrightarrow \phi([x] \underset{+[y]}{}) = [0]$$

$\Rightarrow [x]+[-y] = [0]$

Assumption

$$\Longrightarrow [x]=[y]$$

What remains to be shown: $\phi([x]) = [0]$

$$\Longrightarrow [x]=[0]$$

Proof: $\phi([x]) = [0] \Longrightarrow [mx]=[0]$

$$\Longrightarrow n \mid mx$$

$\Rightarrow n | x \Rightarrow [x] = [0]$ $\boxed{\text{QED}}$

Chapter 3 Section 6 - Homomorphisms

Defn: Let $(G, \circledast)$ and $(G', \boxed{*})$ be groups

say that, $\phi : G \to G'$ is a homomorphism

$$\Longleftrightarrow \phi(x \circledast y) = \phi(x) \boxed{*} \phi(y)$$

Defn: 1) If $G = G'$, we call ϕ as an endomorphism

2) If ϕ is surjective, we call ϕ an epimorphism

3) If ϕ is injective, we call ϕ ~~an~~ a monomorphism

Example 1: $\phi : \mathbb{Z} \to \mathbb{Z}_n$

$x \mapsto [x]$

then, $\phi(x+y) = [x+y] = [x] + [y] = \phi(x) + \phi(y)$

$\Rightarrow$ ϕ is a surjective homomorphism (aka epimorphism)

Example 2: $GL(n, \mathbb{R}) \to (\mathbb{R}^{\neq 0}, \cdot)$

$A \mapsto \det(A)$

Note!: $GL(n, \mathbb{R})$ is the group of all "$n \times n$" invertible matrices. GL indicates "general linear".

then, the homomorphism property is $\det(AB) = \det(A) \cdot \det(B)$

Recall: $\phi : G \to G'$ is a homomorphism

$$\Longleftrightarrow \forall x, y \in G : \phi(x \circledast y) = \phi(x) \boxed{*} \phi(y)$$

$\Rightarrow$ $G = G'$ is an endomorphism

$\Rightarrow$ ϕ surjective $\Rightarrow$ ϕ is an epimorphism

$\Rightarrow$ ϕ injective $\Rightarrow$ ϕ is a monomorphism

<u>Example 1:</u> $\phi : \mathbb{Z} \to \mathbb{Z}_n$

$$x \mapsto [x]$$

It is an epimorphism? Answer: Yes

It is a monomorphism? Answer: NO

<u>Example 2:</u> $\phi : \mathbb{Z} \to \mathbb{Z}$

$$x \mapsto 3x$$

Check the homomorphic property: $\phi(x+y) = 3(x+y)$

$= 3x + 3y = \phi(x) + \phi(y)$ ✓

so, $3x + 3y \Rightarrow x \overset{=}{\neq} y \Longrightarrow \boxed{x = y}$

<u>Example 3:</u> $\det : GL(n, \mathbb{R}) \longrightarrow (\mathbb{R}^{\neq 0}, \circ)$

$$\det(AB) = \det A \cdot \det B$$

<u>Example 4:</u> $\phi : \mathbb{Z}_6 \to \mathbb{Z}_{12}$

$$[0]_6 \mapsto [0]_{12}$$

$$[1]_6 \longmapsto [1]_{12}$$
$$\vdots$$
$$[5]_6 \longmapsto [5]_{12}$$

This is <u>not</u> a homomorphism because of the following,

$$\phi([3]+[4]) = \underbrace{\phi([1])}_{\text{using } \mathbb{Z}_7}$$

$$= [1]$$

On the other hand, $\phi([3]) + \phi([4])$

$$= [3]+[4] = \underbrace{[7]_{12}}_{\text{using } \mathbb{Z}_{12}}$$

Theorem 3.28

The following statements still hold true:

1) $\phi(e) = e'$

2) $\phi(x)^{-1} = \phi(x^{-1})$

<u>Proof:</u> The proof in the case of isomorphisms did not use the concept of bijectivity.

<u>Defn:</u> The Kernel

Let $\phi : G \to G'$ be a homomophism

then, the kernel of ϕ is the following set,

$$\ker \phi = \{x \in G : \phi(x) = e'\}$$

The identity element in G'

Remark/Lemma

$\phi : G \to G'$ is a homomorphism and injective

$\iff \ker \phi = \{e\}$

Proof: " $\Rightarrow$ "

This part of the proof is trivial, because if ϕ is injective, then "e" is the only element within the kernel of ϕ.

" $\Leftarrow$ "

Let $\phi(x) = \phi(y)$ and $1 \cdot \phi(y)^{-1}$

$\Rightarrow \phi(x)\phi(y)^{-1} = e'$

$\Rightarrow \phi(x)\phi(y^{-1}) = e'$ "By Property 2 of Theorem 3.28"

$\Rightarrow \phi(xy^{-1}) = e'$

$\Rightarrow \ker \phi = \{e\}$, because we assume $\phi(xy^{-1}) = e'$ follows Property 1 of Thm. 3.28

Proposition: $\ker \phi$ is a subgroup of G

Proof: $\ker \phi$ must be checked to be nonempty $\Rightarrow e \in \ker \phi$ ✓

Let $x, y \in \ker \phi \Rightarrow \phi(xy) = \phi(x)\phi(y)$

$= e' \cdot e' = e' \Rightarrow \phi(xy) \in \ker\phi$ ✓

then, let $x \in \ker\phi \Rightarrow \phi(x^{-1}) = \phi(x)^{-1} = (e')^{-1}$
$= e'$ ✓

Remark: There are more things that are valid concerning $\ker\phi$

This works when $e = 1$

$$\Rightarrow \forall g \in G : \forall x \in \ker\phi : gxg^{-1} \in \ker\phi$$

the element "x" and not a multiplication sign.

Proof:
$$\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g^{-1})$$
$$= \phi(g)\phi(x)\phi(g)^{-1}$$
$$= \phi(g)\phi(g)^{-1}$$
$$= \boxed{e'}$$

The term $\phi(x)$ drops off because $\phi(x) = e'$ as $\phi(x) \in \ker\phi$.

Remark: We will talk about "normal subgroups" later on.

Theorem: Let $\phi : G \to G'$ be an epimorphism (aka surj. homomorphism). Let G be abelian. Then G' is abelian.

Proof: Let $x, y \in G'$

Because of surjectivity, $\exists a, b \in G : \phi(a) = x$
$\phi(b) = y$

then, $xy = \phi(a)\phi(b) = \phi(ab)$ ← Based on the homomorphism property

$= \phi(ba)$ ← The property of being abelian

$= \phi(b)\phi(a)$

$= yx$ $\boxed{\text{QED}}$

Theorem: Let $\phi: G \to G'$ be a surjective homomorphism (aka epimorphism). Let G be cyclic. Then G' is cyclic.

Proof: Let x be a generator of G

Claim: $\phi(x)$ is a generator of G'

Proof: Let $y \in G$ be arbitrary

Since ϕ is surjective, $\exists k : \phi(x^k) = y$

and $G = \langle x \rangle$; Note: $\phi(x^k)$

$= \phi(x) \cdot \ldots \cdot \phi(x)$

Theorem: Let $\phi: G \to G'$ be a homomorphism

Let H be a subgroup in G, then $\phi(H)$ is a subgroup in G'.

Proof: Check that H is nonempty, $\Longrightarrow$ $\phi(H)$ is also nonempty

if so

Let $x, y \in \phi(H) \Longrightarrow \exists a, b \in H : \phi(a) = x$
$\phi(b) = y$

then, $xy = \phi(a)\phi(b)$

$= \phi(ab)$, where $xy \in \phi(H)$ ✓

Let $x \in \phi(H)$ and $x = \phi(a)$ then,

then, $x^{-1} = (\phi(a))^{-1} = \phi(a^{-1})$ $a^{-1} \in H$

$\Longrightarrow x^{-1} \in \phi(H)$ $\boxed{\text{QED}}$

clic.

(x)

Theorem: Let $\phi : G \to G'$ be a homomorphism

Let $K \subset G'$ be a subgroup
then, $\phi^{-1}(K)$ is a subgroup of G

Proof: $\phi^{-1}(K)$ is nonempty because K is nonempty (in other words, since $e' \in K$, then $e \in \phi^{-1}(K) \neq \phi$) ✓

then, let $x, y \in \phi^{-1}(K)$

Claim: $\phi(xy) \in K$

then, $\phi(xy) = \phi(x)\phi(y)$, where $\phi(x)$ and $\phi(y) \in K$

then, $\phi(xy) \in K$ ✓

Let $x \in \phi^{-1}(K)$

then, we need to show $\phi(x^{-1}) \in K$

then, $\phi(x^{-1}) = \phi(x)^{-1}$, where $\phi(x) \in K$

then, $\underbrace{\phi(x^{-1}) \in K}_{x \in \phi^{-1}(K)}$ $\boxed{QED}$