Alg - 8

G is a group, $x \in G$. Suppose
$\exists\, n \in \mathbb{N}$ s.t. $x^n = e$. Prove that
$\exists\, m \in \mathbb{N}$ s.t $x^{-1} = x^m$

$$f(x) = Ax + b$$

A, a

Prop $G \xrightarrow{f} G' \xrightarrow{g} G''$ homo

$g \circ f$ is homo if the G, G' & G'' are groups

Proof $(g \circ f) : G \to G''$. Let $a, b \in G$

then $(g \circ f)(ab) = g(f(ab))$

$= g(f(a) f(b))$ as f is homo

$= g(f(a)\, g(f(b))$ as g is homo

$f(a), f(b) \in G'$

& $g : G' \to G''$ homo

(V.)

$= (g \circ f)(a)(g \circ f)(b)$ ($\because$ f is homo.)

$\Rightarrow g \circ f$ is homo

Prop: $G \xrightarrow{f} G'$ is homo

$\ker f = \{e\} \iff f$ is injective.

Proof

$\Rightarrow$ Assume $\ker f = \{e\}$. To prove f is injective. Suppose $f(a) = f(b)$ for $a, b \in G$. Then $f(ab^{-1})$

$= f(a) f(b^{-1})$ (f is homo)

$= f(a) f(b)^{-1}$

$= f(b) f(b)^{-1}$

$= e'$

$\Rightarrow ab^{-1} \in \ker f = \{e\}$

$ab^{-1} = e \Rightarrow a = b$ proving f is injective

Conversely. assume f is injective

To show $\ker f = \{e\}$. Let $a \in \ker f$

To show $\ker f = \{e\}$. We

then $f(a) = e' = f(e) \Rightarrow a = e$

as f is injective, proved $\ker f = \{e\}$

$f: G \to G'$ homo

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

- $\ker f \leq G$ (subgroup)
- $axa^{-1} \in \ker f$, $\forall a \in G$, $\forall x \in \ker f$.

$f: (\mathbb{R}, +) \to (\mathbb{R}, +)$

$f(x) = x^3$ not homo

$f(a+b) \neq f(a) + f(b)$ for some a & b

Ex G is a group, $a \in G$ fixed

$f: \mathbb{Z} \to G$ by $f(m) = a^m$

then f is a homo: $f(n+m) = a^{n+m} = a^n \cdot a^m$

$= f(n) f(m)$

$\Rightarrow f$ is homo

$\ker f = \{m \in \mathbb{Z} : f(m) = e = a^m\}$

Case I $\ker f = \{0\}$. This means
a is of infinite order.
$a^n \neq e \quad \forall n \neq 0$.

Here seen that $\ker f \leq \mathbb{Z}$
$\Rightarrow \ker f = \langle d \rangle$, $d \in \mathbb{N}$ is
the smallest
element of $\ker f$

d is the period of a

Herstein denotes period of a is d
by $o(a) = d$ & called d
order of a

Gallian: $o(a) = |a|$ for period
or order
$|a| \in \mathbb{N}$ smallest s.t.
$a^{|a|} = e$.

order of an element $a \in G$
$\ldots \; 1 \; a \in G$

order of ...

= period of $a \in G$

Order of a group (means
$|G| = \#G$ = number of element in G
i.e. G is finite, $|G| = \#G$
is called the
order of G

$$\#\left(\mathbb{Z}/n\mathbb{Z}\right) = \left|\mathbb{Z}/n\mathbb{Z}\right| = n.$$

$$|S_3| = \#S_3 = 6$$

$a \in G$, $o(a) = d$, $|\langle a \rangle| = d$

Thm $G \xrightarrow{f} G'$ is homo. G & G' are groups

(1) $H \leq G \Rightarrow f(H) \leq G'$

(2) $H' \leq G' \Rightarrow f^{-1}(H') = H \leq G$
subgroup

(1) Proof: $a', b' \in f(H) = \{f(h) \in G' : h \in H\}$

(1) Proof: $a, b \in f(H)$

To show $ab \in f(H)$

$a' = f(a)$, for some $a \in H$

$b' = f(b)$, for some $b \in H$

$b'^{-1} = f(b^{-1})$ f is homo

Know H is a group $\Rightarrow ab \in H$

Now $a'b'^{-1} = f(a)f(b^{-1}) = f(ab^{-1})$, f is homo

$\in f(H)$

as $ab^{-1} \in H$, H is a subgroup

$\Rightarrow f(H)$ is a subgroup

(2) $\underline{H = f^{-1}(H') \leq G}$ of $H' \leq G'$

$a, b \in H \Rightarrow f(a), f(b) \in H' \leq G'$

$\Rightarrow f(a)f(b)^{-1} \in H'$ as $H' \leq G'$.

$\Rightarrow f(a)f(b^{-1})$

$=$

$f(ab^{-1})$

Thus $a'b'^{-1} = f(ab^{-1}) \in f(H)$

where $a' = f(a)$ & $b' = f(b)$

$\Rightarrow ab^{-1} = f^{-1}(a'b'^{-1}) \in H$.

show $H = f^{-1}(H')$ is a subgroup

Thm G, G' are groups, $f: G \to G'$ is hom

(1) $a \in G$, $d = |a| = o(a)$, then

$o(f(a)) \mid d$.

(2) $x, y \in G$ & $f(x) = f(y) \iff x \ker f = y \ker f$

(3) If $x' = f(x)$ then $f^{-1}(x') = \{a \in G : f(a) = x'\}$

$= x \ker f$.

Notation. $x \ker f \overset{\text{Def}}{=} \{xa \in G : a \in \ker f\}$

Proof (1) $\because d = |a| = o(a)$, d is period of a

d

Proof (1) Since $a^d = e$ cl.

$$e' = f(e) = f(a^d) = f(a)$$

d is an exp of $f(a)$

$\Rightarrow |f(a)| = o(f(a)) \mid d.$

(2) $\Rightarrow$ Assume $f(x) = f(y)$. To prove $x\ker f = y\ker f$ ($a\ker f \subseteq y\ker f \subseteq x\ker f$)

$A = B \iff A \subseteq B \wedge B \subseteq A.$

first $f(x) = f(y) \Rightarrow xy^{-1} \in \ker f.$

$\Rightarrow yx^{-1} = (xy^{-1})^{-1} \in \ker f.$

$a \in x\ker f \Rightarrow a = xh$ for some $h \in \ker f$ i.e. $f(h) = e'$

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

$f(y^{-1}x) = f(y)^{-1} f(x) = f(y)^{-1} f(y) = e'$

$\Rightarrow y^{-1}x \in \ker f.$

$\Rightarrow y^{-1}x \in \ker f$.

$t = y^{-1}a \in \ker f$.

$yt = x \Rightarrow a = xh$

$= (yt)h$

$= y(th)$

$= yc$, $c = th$

$\in \ker f$.

Thus shown, $x\ker f \subseteq y\ker f$

Similarly show $y\ker f \subseteq x\ker f$.

(3) Given $f(x) = x'$

for $a \in G$.

To show $f^{-1}(x') = x\ker f$.

i.e. $f^{-1}(x') \subseteq x\ker f$

and $x\ker f \subseteq f^{-1}(x')$

Let $a \in f^{-1}(x') \Rightarrow f(a) = x'$

$= f(x)$

$f(x^{-1}a) = f(x^{-1})f(a)$ as f is hom

$= f(a)^{-1}f(a)$

$= x'^{-1}x'$.

$= e'$

$x^{-1}a = h \in \ker f$

$a = xh \in x\ker f$.

Similarly show $x\ker f \subseteq f^{-1}(x')$

$s \in a\ker f$

$s = xh$. $h \in \ker f$.

$s \in f^{-1}(x')$

$f(s) = f(xh) = f(x)f(h)$

$= x'e'$

$= x'$

$\Rightarrow s \in f^{-1}(x')$

i.e. $f^{-1}(x') = x\ker f$.

Q. $f^{-1}(x') = x$ why ?

Def: (1) A hom $f: G \to G'$ is called an isomorphism iff f is bijective map

So isomorphism is a bijective homomorphism

$G \cong G'$ means G & G' are isomorphic & write $G \overset{f}{\cong} G'$ when iso f is specified.

Isomorphic groups are undistinguishable ✓

Ex 1. $\ln : ((0,\infty), \cdot) \to (\mathbb{R}, +)$ is an iso

2. $\exp : (\mathbb{R}, +) \to ((0,\infty), \cdot)$ is an iso

is an iso

3 $(\mathbb{C}^*, \cdot) \xrightarrow{\varphi} ((0,\infty), \cdot)$

$\varphi(z) = |z|$. φ is hmo

$\ker\varphi = S^1 = \{z \in \mathbb{C}^* : |z| = 1\}$

is a subgroup of $\mathbb{C}^*$

called the circle group.

$$\mathbb{C}^*/S^1 \simeq (0,\infty)$$

↑ quotient group

Def. An isomorphism $f : G \to G$ is called an automorphism.

$Iso(G, G')$ = the set of all isomorphisms from G to G'

$\mathrm{Auto}(G)$ = the set of all automorphisms on G

Thm $f \in \mathrm{Iso}(G, G')$
then $f^{-1}: G' \to G$ is a homo.
The inverse of an isomorphism is an isomorphism

$f \in \mathrm{Iso}(G, G')$
$\Rightarrow f^{-1} \in \mathrm{Iso}(G', G)$

Proof: $f: G \to G'$ is iso.
$f^{-1}: G' \to G$ exists
To prove f^{-1} is homo
$a', b' \in G'$, $\exists\, a, b \in G$
s.t. $f(a) = a'$ & $f(b) = b'$
$a'b' = f(a)f(b) = f(ab)$ as

$a'b' = f(a)f(b) = f(ab)$ as f is homo

$\Rightarrow ab = f^{-1}(a'b')$

$\Rightarrow f^{-1}(a'b') = ab = f^{-1}(a')f^{-1}(b')$

i.e. f^{-1} is homo.

$\ln : (\mathbb{R}_{>0}, \cdot) \to (\mathbb{R}, +)$ iso

$\ln^{-1} = \exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$ is iso

Thm Let G be a group Then

(1) $Aut(G) \leq Perm(G)$

(2) In fact $Aut(G) \leq Perm(G)$

i.e. it is a subgroup

Proof, $f, g \in Aut(G)$

$f \circ g^{-1} \in Aut(G)$

$\ldots$ g^{-1} is auto

$f \circ g$

g^{-1} is bijective homo, so g^{-1} is auto

$f \circ g^{-1}$ is bijection & homo

Ex. G is a group. $a \in G$

$T_a : G \to G$ defined by

$L_a(x) = T_a(x) = ax$ is called a left translation

$R_a(x) = xa$, called a right translation of G by a.

$L_a \circ L_b = L_{ab}$ $(T_a \circ T_b = T_{ab})$

$(L_a \circ L_b)(x) = L_a(L_b(x))$ def $\circ$

$= a(L_b(x))$ def L_a

$= a(bx)$ def L_b

$= (ab)x$ assoc. of product

$= L_{ab}(x)$ $\forall x \in G$

$= L_{ab}(x) \quad \forall x \in G$

$\Rightarrow L_a \circ L_b = L_{ab}$

$\Rightarrow L_a$ is bijective & $L_a^{-1} = L_{a^{-1}}$

$L_{ab} = L_a \circ L_b = L_e = I_G$

$ab = e \qquad a = b^{-1}$

$L_a \in \mathrm{Perm}(G)$.

Define $\varphi : G \longrightarrow \mathrm{Perm}(G)$ by $\varphi(a) = L_a = T_a$. Then φ is a hmo: $\varphi(ab) = L_{ab} = L_a \circ L_b$

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

$\Rightarrow \varphi$ is a hmo.

$\ker \varphi = ?$ Let $a \in \ker \varphi$

$\varphi(a) = e_{\ldots} = I_G$

$$\varphi(a) = e_{\mathrm{Perm}(G)} = I_G$$

$$\Rightarrow L_a = I_G \Rightarrow L_a(x) = I(x) \quad \forall x \in G$$

$$\Rightarrow ax = x \quad \forall x \in G$$

$$\underline{\underline{a = e}}.$$

$\ker \varphi = \{e\} \Rightarrow \varphi$ is injective

$\varphi : G \to \mathrm{Perm}(G)$ defined by $\varphi(a) = L_a$ is an injective homo (rarely surjective, never surjective except for $G = \{e\}, \mathbb{Z}/2\mathbb{Z}$.)

$\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ G & $\mathrm{Perm}(G)$

X is a finite set

$f: X \to X$ is injective $\iff$ f is surjective

$\varphi: \mathbb{Z}/2\mathbb{Z} \to \mathrm{Perm}(\mathbb{Z}/2\mathbb{Z})$

$\varphi(a) = L_a$ is injective

Fix $a \in G$, a group

$C_a: G \to G$ defined

$C_a(x) = axa^{-1}$ is (1) homo

(2) bijection

$\Rightarrow C_a$ is automorphism

called an inner automorphism.