MATH 171 : LECTURE 8 DAGAN KARP

GROUP HOMOMORPHISMS

DEF: A HOMOMORPHISM OF A GROUP G TO A GROUP G' IS A MAP $\varphi: G \to G'$ SUCH THAT

$$\varphi(xy) = \varphi(x)\,\varphi(y) \quad \text{FOR ALL } x, y \in G.$$

NOTE: $(G, *)$, $(G', \star)$

$$\varphi(x * y) = \varphi(x) \star \varphi(y)$$

EX: $\varphi: \mathbb{Z} \to \mathbb{Z}$, $\varphi(a) = 2a$.

THEN $\varphi(a+b) = 2(a+b) = (a+b)+(a+b) = 2a+2b$

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

THUS φ IS A HOMOMORPHISM.

EX: FOR ANY GROUP G, THE IDENTITY MAP

$$\mathbb{1}_G : G \to G$$

DEFINED BY $\mathbb{1}_G(x) = x$ $\forall x \in G$ IS A HOMOMORPHISM.

EX: FOR ANY GROUPS G AND G', DEFINE $\varphi : G \to G'$ BY

$$\varphi(x) = 1.$$

THEN $\varphi(xy) = 1 = 1 \cdot 1 = \varphi(x)\varphi(y)$. THUS φ IS A HOMOMORPHISM, CALLED THE TRIVIAL HOMOMORPHISM.

EX: CONSIDER THE EXPONENTIAL MAP $\exp : \mathbb{R} \to \mathbb{R}^\times$ GIVEN BY $\exp(x) = e^x$.

THEN $\exp(x+y) = e^{(x+y)} = e^x e^y$. THUS THE EXPONENTIAL MAP IS A GROUP HOMOMORPHISM

PROP: LET $\varphi: G \to G'$ BE A GROUP HOMOMORPHISM.

LET $x \in G$, $n \in \mathbb{Z}$.

(1) $\varphi(1) = 1$

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

(3) $\varphi(x_1 \cdots x_n) = \varphi(x_1) \cdots \varphi(x_n)$

(4) $\varphi(x^n) = \varphi(x)^n$.

PF: (GROUPWORK?)

(1) $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)$. THUS

$$\varphi(1)^{-1} \cdot \varphi(1) = \varphi(1)^{-1} \varphi(1)\varphi(1) \Rightarrow 1 = \varphi(1)$$

(2) $\varphi(x^{-1})\varphi(x) = \varphi(x^{-1} x) = \varphi(1) = 1$. THUS

$$\varphi(x)^{-1} = \varphi(x^{-1})$$

(3) $\varphi(x_1 \cdots x_n) = \varphi(x_1 \cdot (x_2 \cdots x_n)) = \varphi(x_1)\varphi(x_2 \cdots x_n)$

INDUCE.

(4) USE (3). QED

PROP: LET $\varphi : G \to G'$ BE A HOM, $\psi : G' \to G''$ BE A HOM. THEN

$$\psi \circ \varphi : G \to G'' \text{ IS A HOM.}$$

PF: LET $x, y \in G$. THEN

$$\psi \circ \varphi(xy) = \psi(\varphi(xy)) = \psi(\varphi(x)\varphi(y)) = \psi(\varphi(x))\,\psi(\varphi(y))$$

$$= \psi \circ \varphi(x) \cdot \psi \circ \varphi(y). \quad \text{QED}$$

EX: LET $G = \mathbb{Z}_2$, $H = \langle (12) \rangle \leq S_3$

$+_2$	0	1
0	0	1
1	1	0

$\varphi \curvearrowright$

$\circ$	(1)	(12)
(1)	(1)	(12)
(12)	(12)	(1)

$\varphi(1) = (12) \qquad \varphi(0) = (1)$

NOTE: φ IS BIJECTIVE AND G AND H HAVE THE SAME STRUCTURE.

DEF: A MAP $\varphi: G \to G'$ IS AN **ISOMORPHISM** IFF IT IS A BIJECTIVE HOMOMORPHISM. WE SAY G AND G' ARE **ISOMORPHIC**, DENOTED $G \cong G'$.

EX: $D_3 \cong S_3$.

EX: THE IDENTITY MAP $1_G: G \to G$ IS A ISOMORPHISM FOR ALL GROUPS G.

EX: LET $\mathbb{R}_{>0}$ DENOTE THE POSITIVE REAL NUMBERS, WHICH IS A GROUP UNDER MULTIPLICATION. THEN

$$\exp: \mathbb{R} \to \mathbb{R}_{>0}$$

IS AN ISOMORPHISM. (ITS INVERSE IS THE NATURAL LOG)

PROP: LET $\varphi: G \to H$ BE AN ISOMORPHISM.

(1) $|G| = |H|$

(2) G IS ABELIAN $\iff$ H IS ABELIAN

(3) FOR ALL $x \in G$, $|x| = |\varphi(x)|$.

PF:

(1) φ IS A BIJECTION, SO $|G| = |H|$

(2) ($\Rightarrow$) LET $h_1, h_2 \in H$. THEN $\exists\, g_1, g_2 \in G$ s.t. $\varphi(g_i) = h_i$. THEN

$$h_1 h_2 = \varphi(g_1)\varphi(g_2) = \varphi(g_1 g_2) = \varphi(g_2 g_1)$$

$$= \varphi(g_2)\varphi(g_1) = h_2 h_1.$$

THUS H IS ABELIAN. ($\Leftarrow$) IS SIMILAR.

(3) LET $|x| = n$. THEN

$$\varphi(x)^n = \varphi(x^n) = \varphi(1) = 1.$$

SUPPOSE $\varphi(x)^m = 1$ FOR $m < n$. THEN

$\varphi(x^m) = \varphi(x)^m = 1$. BUT φ IS BIJECTIVE.

THUS $x^m = 1 \implies |x| = n$. THUS n IS THE SMALLEST INTEGER SUCH THAT $\varphi(x)^n = 1$.

IE $|\varphi(x)| = n = |x|$. QED.

DEF: AN ENDOMORPHISM OF G IS A HOMOMORPHISM FROM G TO G (ITSELF). AN AUTOMORPHISM IS AN ISOMORPHISM OF G TO G. THE GROUP OF AUTOMORPHISMS OF G IS THE GROUP

$$\text{AUT}(G) = \{\varphi : G \to G \mid \varphi \text{ IS AN ISO.}\}$$

UNDER COMPOSITION.

NOTE: THE COMPOSITION OF HOMOMORPHISMS IS A HOMOMORPHISM, AND THE COMPOSITION OF BIJECTIONS IS A BIJECTION. THUS THE COMPOSITION OF ISOMORPHISMS IS AN ISOMORPHISM. INDEED, ISOMORPHISM IS AN EQUIVALENCE RELATION ON GROUPS.

PROP: LET G BE A GROUP. FOR EACH $a \in G$,

DEFINE $\alpha_a : G \to G$ BY

$$\alpha_a(x) = axa^{-1}.$$

THEN α_a IS AN AUTOMORPHISM. IN FACT, DEFINE

$$\alpha : G \to \text{AUT}(G) \text{ BY}$$

$$\alpha(a) = \alpha_a.$$

THEN α IS A HOMOMORPHISM OF GROUPS.

PF: $\alpha_a(xy) = axya^{-1} = axa^{-1} \cdot aya^{-1} = \alpha_a(x)\alpha_a(y)$.

THUS α_a IS AN ENDOMORPHISM OF G.

SINCE $a \in G$, $a^{-1} \in G$. NOTE THAT

$$\alpha_{a^{-1}} \circ \alpha_a(x) = \alpha_{a^{-1}}(axa^{-1}) = a^{-1}axa^{-1}a = x.$$

ALSO $\alpha_a \circ \alpha_{a^{-1}}(x) = aa^{-1}xaa^{-1} = x$. THUS

$$\alpha_{a^{-1}} = (\alpha_a^{-1})$$

AND $\alpha_{a^{-1}} \circ \alpha_a = 1_G = \alpha_{a^{-1}} \circ \alpha_a$.

THUS α_a IS A BIJECTIVE HOMOMORPHISM. HENCE

$\alpha_a \in \text{AUT}(G)$.

ALSO, FOR $a, b \in G$,

$$\alpha(ab)(x) = \alpha_{ab}(x) = (ab)x(ab)^{-1}$$

$$= abxb^{-1}a^{-1} = \alpha_a \circ \alpha_b(x)$$

THUS $\alpha : G \to \text{AUT}(G)$ IS A GROUP HOM.

QED

DEF: $a \in G$. THE MAP $x \mapsto axa^{-1}$ IS CALLED AN INNER AUTOMORPHISM OF G

NOTE: IF G IS ABELIAN, AUT(G) IS TRIVIAL.
OTHERWISE $\exists a, x$ s.t. $ax \neq xa$ IE $x \neq axa^{-1}$
IE $\alpha_a \neq 1_G$, HENCE AUT(G) IS NONTRIVIAL.