Chap 14: homomorphism.

Def: If G and H are groups, a homomorphism from G to H is a function $f: G \to H$ s.t. $\forall a, b \in G$, $f(ab) = f(a) f(b)$.

If there exists a homomorphism from G to H s.t. $f(G) = H$, we say that H is a homomorphic image of G.

Ex: 1. $f: \mathbb{Z} \to \mathbb{Z}_q$ $\quad$ $\mathbb{Z}_q$ is a homomorphic image of $\mathbb{Z}$

$n \mapsto n \bmod q$.

2. $\det: GL(n, \mathbb{R}) \to \mathbb{R}^*$

$GL(n,\mathbb{R}) = \{\text{nonsingular } n\times n \text{ matrices}\}$

operation = matrix product.

3. $f: \mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_n$ $\quad$ $\bar{k}_1 = \bar{k}_2 \Leftrightarrow (mn) \mid k_1 - k_2 \Rightarrow n \mid k_1 - k_2$

$\bar{k}^{mn} \longmapsto k \bmod n$. $\quad$ $\Rightarrow f$ is well-defined.

$\bar{k}^{mn} = k \bmod mn$, $\quad$ $k \bmod n = \bar{k}^n$

$$f(\bar{k}_1 + \bar{k}_2) = f(\overline{k_1 + k_2}) = (k_1 + k_2) \bmod n = \overline{(k_1+k_2)}^n = \bar{k}_1^n + \bar{k}_2^n$$
$$= f(k_1) + f(k_2).$$

Thm: Let G and H be groups, and $f: G \to H$ a homomorphism. Then

(i) $f(e) = e$, and

(ii) $f(a^{-1}) = f(a)^{-1}$ for every element $a \in G$.

Pf: (i) $f(a) = f(a \cdot e) = f(a) f(e) \Rightarrow f(e_1) = e_2$

(ii) $f(a) f(a^{-1}) = f(a \cdot a^{-1}) = f(e_1) = e_2 \Rightarrow f(a)^{-1} = f(a^{-1})$

Def: $a \in G$. A conjugate of a is an element of the form xax^{-1} where $x \in G$

Ex: In S_3, the conjugates of (12) are:

$e\cdot(12)e^{-1} = (12)$. $(12)(12)(12)^{-1} = (12)$. $(13)(12)(13)^{-1} = (13)(12)(13) = (1)(23)$

$(23)(12)(23)^{-1} = (23)(12)(23) = (13)(2) = (13)$. $(123)(12)(123)^{-1} = (123)(12)(132)$

$= (1)(23)$

$(132)(12)(132)^{-1} = (132)(12)(123) = (13)(2)$

$\pi(a_1 \cdots a_k)\pi^{-1} = (\pi(a_1) \cdots \pi(a_k))$. (Chap 8 E.1).

Def: $H < G$. H is called a normal subgroup of G if it is closed w.r.t. conjugates, that is, if $\forall a \in H$ and $\forall x \in G$, $xax^{-1} \in H$. Denoted by $H \triangleleft G$.

Normal subgroup: closed w.r.t. products, inverses and w.r.t. conjugates.

Def: Let $f: G \to H$ be a homomorphism. The kernel of f:

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

Thm: Let $f: G \to H$ be a homomorphism.

(i) The kernel of f is a normal subgroup of G and

(ii) The range of f is a subgroup of H. (denoted by $\mathrm{ran}(f)$)

Pf. (i) · $x, y \in \ker(f) \Rightarrow f(x) = f(y) = e \Rightarrow f(x\cdot y) = f(x)f(y) = e$

So closed under products

· $f(x^{-1}) = f(x)^{-1} = e_2^{-1} = e_2 \Rightarrow$ closed under inverses

· $\forall x \in \ker(f), g \in G$. $f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g)\cdot e_2 f(g)^{-1} = e_2$

$\Rightarrow \ker(f)$ is closed w.r.t. conjugates

$\Rightarrow \ker(f) \triangleleft G$

(ii). $f(x)\cdot f(y) = f(xy) \Rightarrow \mathrm{ran}(f)$ is closed w.r.t. products.

$f(x)^{-1} = f(x^{-1}) \Rightarrow \mathrm{ran}(f)$ is ...... inverses

$\Rightarrow \mathrm{ran}(f)$ is a subgroup of H: $\mathrm{ran}(f) < H$.

<u>Exer</u>: A.1 : $f: \mathbb{Z}_8 \to \mathbb{Z}_4 \iff \begin{pmatrix} 0&1&2&3&4&5&6&7 \\ 0&1&2&3&0&1&2&3 \end{pmatrix}$

$\bar{n}^8 \mapsto \bar{n}^4$

A.4. $f: D_4 \to S_2 = \mathbb{Z}_2$

$D_4 = \langle a, b \mid a^2 = e, b^4 = e, ba = ab^3 \rangle = \{e, a, b, b^2, b^3, ab, ab^2, ab^3\}$

$\begin{matrix} e & a & b & b^2 & b^3 & ab & ab^2 & ab^3 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{matrix}$

reflection

a: changes sides (reverse orientation)

b: keeps sides. (preserve orientation)

rotation.

A.6 $B \subset A$ $h: P_A \to P_B$

$h(C) = C \cap B$

$A = \{1,2,3\}$
$B = \{1,2\}$

$h = \begin{pmatrix} \phi & \{1\} & \{2\} & \{3\} & \{1,2\} & \{1,3\} & \{2,3\} & A \\ \phi & \{1\} & \{2\} & \phi & \{1,2\} & \{1\} & \{2\} & \{1,2\} \end{pmatrix}$

$P_A = \mathbb{Z}_2^{|A|} \longrightarrow P_B = \mathbb{Z}_2^{|B|}$

$h(C_1 * C_2) = ((C_1 - C_2) \cup (C_2 - C_1)) \cap B$
$= ((C_1 - C_2) \cap B) \cup ((C_2 - C_1) \cap B)$
$= ((C_1 \cap B) \cap (B - C_2)) \cup ((C_2 \cap B) \cap (B - C_1))$
$= ((C_1 \cap B) - (C_2 \cap B)) \cup ((C_2 \cap B) - (C_1 \cap B))$
$= h(C_1) * h(C_2)$

B. 1. $\phi(f+g) = (f+g)(0) = f(0) + g(0) = \phi(f) + \phi(g)$.

B. 4. $f(x \cdot y) = |xy| = |x||y| = f(x) \cdot f(y)$.

C. 2. $f: G \to H$ a homomorphism. Then f is injective iff $\ker(f) = \{e\}$.

<u>Pf</u>: • f injective and $f(x) = e_2 = f(e_1) \Rightarrow x = e_1 \Rightarrow \ker(f) = \{e\}$

• assume $\ker(f) = \{e\}$. $f(x) = f(y) \Rightarrow f(xy^{-1}) = f(x)f(y)^{-1} = e_2 \Rightarrow xy^{-1} = e_1 \Rightarrow x = y$

So f is injective.

D.1 $S_3 = \{e, (12), (13), (23), (123), (132)\}$

$|S_3| = 6$. If $H < S_3$, then $|H| \,\big|\, \underset{6}{\overset{\shortparallel}{|S_3|}} \Rightarrow |H| = 1, 2, 3$ or 6.

case 1: $|H| = 1 \Rightarrow H = \{e\}$. case 2: $|H| = 6 \Rightarrow H = S_3$.

case 3: $|H| = 3 \Rightarrow (G:H) = 2 \overset{\text{Fact}}{\Longrightarrow} H \triangleleft G$

Fact (E.1): If H has index 2 in G, then H is normal.

Pf: $(G:H) = 2 \Rightarrow G = H \sqcup Ha$ for any $a \notin H \Rightarrow Ha = aH$ $\forall a \notin H$

$= H \sqcup aH$ $\Updownarrow$ $a^{-1}Ha = H$

On the other hand $Hh = hH$ $\forall h \in H$. So $x^{-1}Hx = H$ $\forall x \in G$

So H is a normal subgroup of G.

Alternatively: $|H| = 3 \Rightarrow H = \langle a \rangle$ because 3 is prime with $\mathrm{ord}(a) = 3$

$\Rightarrow H = \{e, (123), (132)\} = \langle (123) \rangle = \langle (132) \rangle$

$\Rightarrow H = \{\text{even permutations}\} \subset S_3$

$\forall x \in S_3$, $h \in H$ $\quad xhx^{-1} \in H$: odd · even · odd^{-1} is even
even · even · even^{-1} is even

Case 3: $|H| = 2 \Rightarrow H = \langle b \rangle$ with $\mathrm{ord}(b) = 2$.

$\Rightarrow H = \langle (12) \rangle$ or $\langle (13) \rangle$ or $\langle (23) \rangle$

$(23)(12)(23)^{-1} = (23)(12)(23) = (13)(2) = (13) \notin \langle (12) \rangle$

$\Rightarrow \langle (12) \rangle$ is not normal.

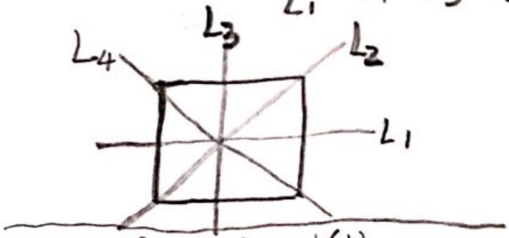
Similarly $\langle (13) \rangle$, $\langle (23) \rangle$ are not normal

So all normal subgroups of S_3 are $\{e\}$, S_3, $A_3 = \{\text{even permutations}\}$

90° counterclockwise

rotations: $\{e, b, b^2, b^3\}$

reflections: $\{a, ab, ab^2, ab^3\}$
$\quad\;\; \uparrow\;\; \uparrow\;\; \uparrow\;\; \uparrow$
$\quad\; L_1\; L_4\; L_3\; L_2$



$(ab^2)^2 = ab^2ab^2 = a^2b^6b^2 = e$

D.1(b). $G = D_4 = \{e, b, b^2, b^3, a, ab, ab^2, ab^3\}$.

$H < D_4 \Rightarrow |H| \mid 8 \Rightarrow |H| = 1, 2, 4$ or 8

Case 1: $|H| = 1 \Rightarrow H = \{e\}$.

Case 2: $|H| = 8 \Rightarrow H = D_4$

Case 3: $|H| = 4 \Rightarrow (G:H) = 2 \Rightarrow H \triangleleft G$.

Case 3.a $H \cong \mathbb{Z}_4 \Rightarrow H = \langle b \rangle = \langle b^3 \rangle$.

Case 3.b $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$: order 2 elements: b^2, a, ab, ab^2, ab^3 $\leftarrow (ab^3)^2 = ab^3ab^3 = a^2b^9b^3 = e$

b^2: rotation by 180°

$(ab)^2 = abab = a^2b^3b = e$

- b^2 commutes with ab^k: $b^2 \cdot ab^k = ab^{6+k} = ab^{2+k} = ab^k \cdot b^2$

- ab^k commutes with ab^l iff $k \equiv l \bmod 2$:

$ab^k \cdot ab^l = a^2 b^{3k+l} = b^{3k+l}$

$ab^l \cdot ab^k = a \cdot ab^{3l} \cdot b^k = b^{3l+k}$

$b^{3k+l} = b^{3l+k}$ iff $4 \mid 3k+l-(3l+k)$
$\Updownarrow$
$4 \mid 2k-2l$
$\Updownarrow$
$2 \mid k-l$

so all the possible $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$:

(i) $\langle b^2, a \rangle = \{e, b^2, a, ab^2\} = \langle b^2, ab^2 \rangle = \langle a, ab^2 \rangle$

(ii) $\langle b^2, ab \rangle = \{e, b^2, ab, ab^3\} = \langle b^2, ab^3 \rangle = \langle ab, ab^3 \rangle$

Case 4: $|H| = 2 \Rightarrow H = \langle x \rangle$ with $\mathrm{ord}(x) = 2$ i.e. $H = \{e, x\}$

$\Rightarrow x = b^2$, or a, or ab, or ab^2, or ab^3

$H \triangleleft G$ iff $\forall y \in G,\ y \cdot x \cdot y^{-1} \in H$ iff $yxy^{-1} = x$ (since $yxy^{-1} = e \Rightarrow x = e$)

so $\{e, x\} \triangleleft G$ iff $x \in$ Center of D_4 and $\mathrm{ord}(x) = 2$

$\Rightarrow x = b^2 \Rightarrow H = \{e, b^2\} \triangleleft D_4$

So all normal subgroups of H are:

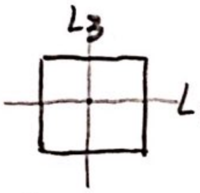
$\{e\}$, D_4, $\langle b \rangle = \langle b^3 \rangle = \{e, b, b^2, b^3\}$, $\{e, b^2, a, ab^2\}$, $\{e, b^2, ab, ab^3\}$, $\{e, b^2\}$.

Homomorphisms associated to normal subgroups.

case 1: $\{e\} = \ker(id : D_4 \to D_4)$

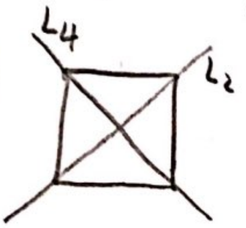
case 2: $D_4 = \ker\{f : D_4 \to \{e\})$

case 3: (3.a) $\langle b \rangle = \ker\{f : D_4 \to \mathbb{Z}_2\}$. $f(x) = \begin{cases} 0 & \text{if } x \text{ keeps sides} \\ 1 & \text{if } x \text{ reverses sides.} \end{cases}$

3.b.(i) 

$f : D_4 \to S_2$ induced permutation on $\{L_1, L_3\}$

$\ker(f) = \{e, b^2, a, ab^2\}$.

3.b.(ii) 

$f : D_4 \to S_2$ induced permutation on $\{L_2, L_4\}$

$\ker(f) = \{e, b^2, ab, ab^3\}$

case 4: $f : D_4 \longrightarrow S_2 \times S_2$ $\quad \ker(f) = \langle b^2 \rangle$.

$x \longmapsto$ (permutation on $\{L_1, L_3\}$, permutation on $\{L_2, L_4\}$)

D.4. $H \triangleleft G \Leftrightarrow \forall a, b \in G$, $ab \in H$ iff $ba \in H$

Pf: "$\Rightarrow$" $ab \in H \overset{H \triangleleft G}{\Rightarrow} b(ab)b^{-1} = ba \in H$

$ba \in H \overset{H \triangleleft G}{\Longrightarrow} a(ba)a^{-1} = ab \in H$

"$\Leftarrow$" $\forall x \in G, h \in H$. $h = (hx) \cdot x^{-1} \in H \Rightarrow x^{-1} h x \in H$

$\Rightarrow H \triangleleft G$.

E.4: $[G, G] = \langle aba^{-1}b^{-1} ; a, b \in G \rangle$ $\qquad [G, G] < H < G$.

$\forall x \in G$, $h \in H$, $xhx^{-1} = (xhx^{-1} \cdot h^{-1}) \cdot h \in [G, G] \cdot H \subset H$

$\Rightarrow H \triangleleft G$.