6. Homomorphisms and isomorphisms

Object of study: groups $(G, *)$

binary operation : $G \times G \to G$

(1) associative : $(ab)c = a(bc)$ $\forall a,b,c \in G$

(2) $\exists e \in G$: $ae = a = ea$ $\forall a \in G$

(3) $\forall a \in G$ $\exists a^{-1} \in G$: $a a^{-1} = e = a^{-1} a$

Morphism between objects:

Def: Let $(G, *)$ and $(H, *)$ be two groups.
A map $\phi : G \to H$ is a (group) homomorphism
if $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$ for all $g_1, g_2 \in G$

A homomorphism is an isomorphism if it is bijective.

Lemma: Let $\phi : G \to H$ be a homomorphism. Then
(1) $\phi(e_G) = e_H$
(2) $\phi(g^{-1}) = \phi(g)^{-1}$ for all $g \in G$
(3) $\phi(g^n) = \phi(g)^n$ " , $n \in \mathbb{Z}$

proof:
(1) $\phi(e_G) = \phi(e_G \cdot e_G) = \phi(e_G)\phi(e_G)$; now multiply by $\phi(e_G)^{-1}$
$\Rightarrow e_H = \phi(e_G)$
(2) $\phi(e_G) = \phi(g g^{-1}) = \phi(g)\phi(g^{-1})$; hence by (1) $\phi(g^{-1}) = \phi(g)^{-1}$
(3) for $n \geq 0$, $\phi(g^n) = \phi(\underbrace{g \cdots g}_{n-\text{times}}) = \phi(g) \cdots \phi(g) = \phi(g)^n$
for $n < 0$,
$\phi(g^n) = \phi((g^{-n})^{-1}) = \phi(g^{-n})^{-1} = (\underbrace{\phi(g) \cdots \phi(g)}_{-n \text{ times}})^{-1} = \phi(g)^n$

Cor: Let $\phi : G \to H$ be a homomorphism. Then $o(\phi(g)) \mid o(g)$.

Ex: G, H any groups; $\phi(g) = e_H$ for all g defines a homomorphism
Ex: $a \in G$; $c_a(g) = a^{-1} g a$ for all g defines an isomorphism with inverse $c_{a^{-1}}$.

A homomorphism from G to G is an endomorphism; an isomorphism called an autom

Ex: $\mathbb{Z} \xrightarrow{\phi} \mathbb{Z}/n\mathbb{Z}$ is a homomorphism as $\overline{m+k} = \overline{m} + \overline{k}$
$k \longmapsto \overline{k}$

Ex: H a subgroup of G; $H \hookrightarrow G$ is a homomorphism

Ex: $\det : GL_n \mathbb{R} \longrightarrow \mathbb{R}^* = (\mathbb{R} \setminus \{0\}, \text{mult})$ is a homomorphism
as $\det(AB) = \det A \det B$

Ex: $\text{sign}: S_n \longrightarrow \{\pm 1\}$ is a homomorphism

Ex: linear maps $(V, +) \longrightarrow (W, +)$ are homomorphisms of the underlying Abelian groups

Prop: Any endomorphism ϕ of $\mathbb{Z}$ is of the form $\phi(x) = n x$ for some $n \in \mathbb{Z}$

proof: Put $\phi(1) = n$. Then $\phi(-1) = -n$, and for $k \geq 0$

$$\phi(k) = \phi(\underbrace{1 + \dots + 1}_{k\text{-times}}) = \underbrace{\phi(1) + \dots + \phi(1)}_{k\text{-times}} = n k$$

and for $k < 0$

$$\phi(k) = -\phi(-k) = -n(-k) = nk.$$

Note: A homomorphism $\phi : G \to H$ is determined by the image of the generators of G.

Def: Let $\phi : G \to H$ be a homomorphism of groups. Define

(1) the kernel of ϕ $\quad \ker \phi := \{ g \in G \mid \phi(g) = e \} \leq G$

(2) the image of ϕ $\quad \operatorname{im} \phi := \{ \phi(g) \mid g \in G \} \leq H$

Def: A subgroup H is normal in G if $gH = Hg \quad \forall g \in G$
or equivalently $g^{-1} h g \in H \quad \forall g \in G, h \in H$

Write $H \trianglelefteq G$ if H is a normal subgroup.

$gH = Hg \iff \forall h \in H \; \exists \tilde{h} \in H : g\tilde{h} = hg \iff \forall h : g^{-1} h g \in H$

<u>Prop:</u> If $\phi : G \to H$ is a homomorphism then
(a) the kernel is a normal subgroup of G : $\ker\phi \trianglelefteq G$
(b) and the image is a subgroup of H : $\mathrm{im}\,\phi \leqslant H$.

<u>proof:</u> (a) $e_G \in \ker\phi$ as $\phi(e_G) = e_H$;
if $a, b \in \ker\phi$ then $ab \in \ker\phi$ and $a^{-1} \in \ker\phi$ as
$$\phi(ab) = \phi(a)\phi(b) = e_H \cdot e_H = e_H \text{ and } \phi(a^{-1}) = \phi(a)^{-1} = e_H.$$
So $\ker\phi$ is a subgroup of G;
if $a \in \ker\phi$ and $g \in G$ then $g^{-1}ag \in \ker\phi$ as
$$\phi(g^{-1}ag) = \phi(g^{-1})\phi(a)\phi(g) = \phi(g)^{-1} e_H \phi(g) = e_H$$
So $\ker\phi$ is a normal subgroup.

(b) $e_H \in \mathrm{im}\,\phi$ as $\phi(e_G) = e_H$;
if $h_1, h_2 \in H$ then $\exists\, g_1, g_2 \in G : \phi(g_i) = h_i$;
so $\phi(g_1 g_2) = \phi(g_1)\phi(g_2) = h_1 h_2$ and $\phi(g_1^{-1}) = \phi(g_1)^{-1} = h_1^{-1}$
hence $h_1 h_2, h_1^{-1} \in \mathrm{im}\,\phi$.

<u>Prop:</u> ϕ is 1-1 iff $\ker\phi = \{e_G\}$

<u>proof:</u>
$$\phi(a) = \phi(b)$$
$$\iff e_H = \phi(a)\phi(b)^{-1} = \phi(ab^{-1})$$
$$\iff ab^{-1} \in \ker\phi$$
So, if $\ker\phi = \{e\}$ then $a = b$ and ϕ is 1-1, and
if $a \neq e \in \ker\phi$ then $\phi(a) = \phi(e)$ and ϕ is not 1-1.

<u>Goal:</u> For normal subgroups $N \trianglelefteq G$ the cosets $G/N = \{gN \mid g \in G\}$ form again a group and
for $\phi : G \to H$
$$\mathrm{im}\,\phi \cong G/\ker\phi$$
This will be achieved in Sections 7 and 8.

7. Normal Subgroups and Quotient Groups

Let G be a group.

Remarks: (0) If G is abelian then all subgroups are normal.

(1) $\{e\}$ and G are normal subgroups.

(2) $x \in N \trianglelefteq G$

$\Rightarrow \quad Conj(x) := \{ g^{-1} x g \mid g \in G \} \subset N$

conjugacy class of x

Fact: A subgroup is normal iff it is a union of conjugacy classes.

(3) Fact: If $H \leq G$ and $|G/H| = 2$ then $H \trianglelefteq G$

as $G/_H = \{H, gH\}$ for some $g \notin H$ and ${}_H\backslash G = \{H, Hg\}$, and

so $gH = G \setminus H = Hg$

Ex: $A_n \trianglelefteq S_n$ as $|S_n/A_n| = 2$. (Also conjugation preserves "evenness")

$C_n \trianglelefteq D_{2n}$ as $|D_{2n}/C_n| = 2$

Def: G is simple if $\{e\}$ and G are the only normal subgroups.

Ex: $G = C_p$ p prime is simple as by Lagrange $\{e\}$ and C_p are the only subgroups

$G = A_5$ $|A_5| = 5!/2 = 60$

$Conj(e)$	size 1
$Conj((12)(34))$	size 15
$Conj((123))$	size 20
$Conj((12345))$	size 12
$Conj((21345))$	size 12

Recall:
$\sigma^{-1}(12345)\sigma = (\sigma(1), \dots, \sigma(5))$

Note: If $N \trianglelefteq A_5$ then $e \in N$, $|N| \mid 60$ (by Lagrange). Hence, by Fact 2, $N = e$ or $N = A_5$

Def: The centre of G, denoted $Z(G)$, is the set

$$Z(G) = \{ x \in G \mid gx = xg \quad \text{for all } g \in G \}$$

Note: $x \in Z(G)$ iff $Conj(x) = \{x\}$

Prop: $Z(G)$ is a normal subgroup of G.

Ex: $Z(S_n) = \{e\}$ $\qquad Z(GL_n(\mathbb{R})) = \{ \lambda I_n \mid \lambda \in \mathbb{R} \setminus \{0\} \}$

Prop: Let $H \leq G$.

(a) The binary operation $*$ on G/H given by
$$(g_1 H)(g_2 H) = (g_1 g_2) H$$
is well-defined if and only if $H \trianglelefteq G$

(b) If $H \trianglelefteq G$ then $(G/H, *)$ is a group (with identity $eH = H$ and $(gH)^{-1} = g^{-1}H$)

Def: If $H \trianglelefteq G$ then G/H is called the *quotient group*

proof: (a) Assume $H \trianglelefteq G$.

If $g_1 H = k_1 H$, $g_2 H = k_2 H$ then $k_1^{-1} g_1, k_2^{-1} g_2 \in H$

So $g_1 g_2 H = k_1 k_2 H$
$$\iff (k_1 k_2)^{-1} g_1 g_2 \in H$$
$$\iff k_2^{-1} k_1^{-1} g_1 g_2 \in H$$
$$\iff \underbrace{k_2^{-1} \underbrace{(k_1^{-1} g_1)}_{\in H} k_2}_{\in H \text{ as } H \trianglelefteq G} \underbrace{(k_2^{-1} g_2)}_{\in H} \in H$$

Conversely, if $*$ is well-defined then for $h \in H$, $g \in G$
$$g^{-1} h g H = g^{-1}H * hH * gH$$
$$= g^{-1}H * gH$$
$$= H$$
and so $g^{-1} h g \in H$.

(b) Associativity of $*$ is inherited from the mult. in G;
The identity is $eH = H$;
The inverse is given by $(gH)^{-1} = g^{-1}H$ for all $g \in G$

Ex: $C_n \trianglelefteq D_{2n}$ and $D_{2n}/C_n \cong C_2$

$V_4 \trianglelefteq S_4$ and $S_4/V_4 \cong S_3$

$V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$

as $(12)V_4 \, (123)V_4 = (13)V_4 = \{(13), (143), (24), (123)\}$

$\neq (123)V_4 \, (12)V_4 = (23)V_4 = \{(23) \dots\}$

Note: $H \trianglelefteq G$

Then $\phi : G \to G/H$ is a group homomorphism
$g \mapsto gH$ with $\ker \phi = H$.

So $H \leq G$ is a normal subgroup if and only if $H = \ker \phi$ for some homomorphism.

Ex: $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$

$\ker(\det) = \{ A \in GL_n(\mathbb{R}) \mid \det A = 1 \} =: SL_n(\mathbb{R})$

Then $SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$

Ex: $H = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}) \mid a, b, c, d \in n\mathbb{Z} \}$

$\phi : GL_2(\mathbb{Z}) \to GL_2(\mathbb{Z}/n\mathbb{Z})$ is a group homom.

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}$

$\ker \phi = H$ and hence $H \trianglelefteq GL_2\mathbb{Z}$

Alternative interpretation of product in G/H.

Given any subsets $S, T \subseteq G$, define

$$S \cdot T = \{ st \in G \mid s \in S, t \in T \} \subseteq G.$$

For $S = g_1 H$, $T = g_2 H$ two cosets of a subgroup $H \leq G$

$$g_1 H g_2 H = \{ g_1 h_1 g_2 h_2 \mid h_1 \in H, h_2 \in H \}$$

This may or may not be a coset of H in G.

If $H \trianglelefteq G$, then $gH = Hg$ for all $g \in G$, then

$$\begin{aligned} (g_1 H)(g_2 H) &= g_1 (H g_2) H && \text{as mult in } G \text{ is assoc} \\ &= g_1 (g_2 H) H && \text{as } Hg_2 = g_2 H \\ &= g_1 g_2 H && \text{as } HH = H \end{aligned}$$

8. The First Isomorphism Theorem

Th: Let $\phi : G \to H$ be a homomorphism of groups.
Then (1) $\operatorname{im}\phi \leq H$ is a subgroup
(2) $\ker\phi \trianglelefteq G$ is a normal subgroup
(3) $G/\ker\phi \xrightarrow{\cong} \operatorname{im}\phi$ is an isomorphism
$\bar{\phi} : g.\ker\phi \longmapsto \phi(g)$

By Lagrange's Theorem,

Cor: If G is finite then $|G| = |\ker\phi|\,|\operatorname{im}\phi|$

proof of Th: (1) + (2) proved in section 6
(3) Let $g_1, g_2 \in G$.
Then $g_1 \ker\phi = g_2 \ker\phi$
$\iff g_1^{-1} g_2 \in \ker\phi$
$\iff \phi(g_1^{-1} g_2) = \phi(g_1)^{-1}\phi(g_2) = e$
$\iff \phi(g_1) = \phi(g_2)$
Hence, $\bar{\phi}$ is well-defined $_{(\Rightarrow)}$ and injective $_{(\Leftarrow)}$

For all $\phi(g) \in \operatorname{im}\phi$, $\bar{\phi}(g\ker\phi) = \phi(g)$
so $\bar{\phi}$ is surjective.

$\bar{\phi}$ is a homomorphism, as
$\bar{\phi}(g_1 \ker\phi)\bar{\phi}(g_2 \ker\phi)$
$= \phi(g_1)\,\phi(g_2) = \phi(g_1 g_2) = \bar{\phi}(g_1 g_2 \ker\phi)$

Ex: $\operatorname{sign} : S_n \to \{\pm 1\}$
$\operatorname{im}(\operatorname{sign}) = \{\pm 1\}$, $\ker(\operatorname{sign}) = A_n \implies S_n/A_n \cong \{\pm 1\}$

Ex: $\exp : \mathbb{R} \to S^1 = \{ z \in \mathbb{C} \mid |z| = 1 \}$
$\operatorname{im}(\exp) = S^1$, $\ker(\exp) = \mathbb{Z} \implies \mathbb{R}/\mathbb{Z} \cong S^1$

Ex: G a group

$\phi(x) := x^2$ defines a homomorphism

iff G is abelian: $\forall x, y \in G$

$$\phi(xy) = \phi(x)\,\phi(y)$$
$$\Longleftrightarrow (xy)^2 = x^2 y^2$$
$$\Longleftrightarrow xyxy = xxyy$$
$$\Longleftrightarrow yx = xy$$

$\longrightarrow$ $G = S^1 = \{ z = e^{2\pi i t} \mid t \in \mathbb{R} \}$

$\ker \phi = \{ z \mid z^2 = 1 \} = \{ \pm 1 \}$

$\Rightarrow \quad S^1 / \{\pm 1\} \simeq S^1$

$\longrightarrow$ $G = \mathbb{Z}_6 = \{ \bar{0}, \bar{1}, \dots, \bar{5} \}$

$\ker \phi = \{ \bar{n} : 2\bar{n} = \bar{0} \} = \{ \bar{0}, \bar{3} \}$

$\Rightarrow \quad \mathbb{Z}_6 / \langle \bar{3} \rangle = \langle \bar{2} \langle \bar{3} \rangle \rangle \simeq \langle \bar{2} \rangle \simeq C_3$

$\longrightarrow$ $G = \mathbb{Z}_5 = \{ \bar{0}, \dots, \bar{4} \}$

$\ker \phi = \{ \bar{0} \}$

$\Rightarrow \quad \mathbb{Z}_5 / \{\bar{0}\} \simeq \mathbb{Z}_5$

$\boxed{\text{Notation: } \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n}$

$$\begin{tikzcd} m\mathbb{Z} \arrow[d] \arrow[r, mapsto] & \bar{0} \\ \mathbb{Z} \arrow[d, two heads] \arrow[dr, "\cdot k"] & \\ \mathbb{Z}_m \arrow[r] & \mathbb{Z}_n \end{tikzcd}$$

Prop: The map $\phi : \mathbb{Z}_m \to \mathbb{Z}_n$ given by $\phi(r \bmod m) = (kr \bmod n)$ is well-defined iff n divides km.

Note: As $\mathbb{Z}_m$ is cyclic ϕ is determined by $\phi(1 \bmod m) = k \bmod n$ and every homomorphism is of the above form.

proof: If ϕ is well-defined then $\phi(\bar{0}) = \phi(\bar{m}) = km \bmod n$
$= 0 \bmod n$
and $n \mid km$

Conversely, if $n \mid km$, then

$$m \mid (r_1 - r_2) \Rightarrow n \mid k(r_1 - r_2)$$

or equivalently, $r_1 \equiv r_2 \pmod m \Rightarrow kr_1 \equiv kr_2 \pmod n$

Hence, ϕ is well defined.

Problem: How many homomorphisms are there

(i) $\mathbb{Z}_6 \to \mathbb{Z}_{12}$

(ii) $\mathbb{Z}_{12} \to \mathbb{Z}_7$

(iii) $\mathbb{Z}_{10} \to D_{16}$

(i) $\phi(1) = k$ for $12 \mid 6 \cdot k$ $\boxed{6}$

so $k = 2, 4, 6, 8, 10, 12 \equiv 0$

(ii) $\phi(1) = k$ for $7 \mid 12 \cdot k$ $\boxed{0}$

so $k = 7 \equiv 0$

(iii) $\mathbb{Z}_{10}$ is abelian $\Rightarrow$ $\text{im}\,\phi \leq D_{16}$ is an abelian subgroup;

hence $\text{im}\,\phi \leq C_8$ or one of $\{e, s\} \cong C_2$

s a reflection

$\text{im}\,\phi \leq C_8 \cong \mathbb{Z}_8$:

so $\phi(\bar{1}) = k$ for $8 \mid 10 \cdot k$

so $k = 0, 4$

so $\text{im}\,\phi = \{e\}$ or $\text{im}\,\phi = \{e, r^4\}$

rotational generator

$\text{im}\,\phi \in \{e, s\} \cong \mathbb{Z}_2$

so $\phi(\bar{1}) = k$ for $2 \mid 10 \cdot k$

so $k = 0, 1$

so $\text{im}\,\phi = \{e\}$ or $\text{im}\,\phi = \{e, s\}$

Hence, there are 10 possible homomorphisms:

$\bar{1} \mapsto e$

$\bar{1} \mapsto r^4$

$\bar{1} \mapsto s, rs, r^2 s, \ldots, r^7 s$

$\boxed{10}$

G, H groups

$\mathrm{Hom}(G,H) = \{\phi : G \to H \mid \phi$ is a homomorphism$\}$

Determine $|\mathrm{Hom}(G,H)|$:

Every $\phi : G \to H$ factors as:

$$\phi : G \twoheadrightarrow G/\ker\phi \xrightarrow{\simeq} \mathrm{im}\,\phi \hookrightarrow H$$

Step by step approach:

① Find all normal subgroups N of G.
They are the potential kernels

② For each N find the (number $n(N)$ of) subgroups of H which are isomorphic to G/N. They are the potential images

③ For each N with $n(N) > 0$ find (the order of) $\mathrm{Aut}\, G/N = \{\varphi : G/N \to G/N \mid \varphi$ an isomorp$\}$
These are the possible ways of mapping $G/\ker\phi$ onto the image.

Then $|\mathrm{Hom}(G,H)| = \sum_{N \trianglelefteq G} n(N) \times |\mathrm{Aut}(G/N)|$.

Ex: $\mathrm{Hom}(D_8, A_4)$

① Conjugacy classes of $D_8 = \langle r, s \mid r^4 = s^2 = (sr)^2 = e\rangle$ are:
$\mathrm{Conj}(e) = \{e\}$, $\mathrm{Conj}(r) = \{r, srs = r^{-1} = r^3\}$, $\mathrm{Conj}(r^2) = \{r^2\}$
$\mathrm{Conj}(s) = \{s, r^2 s\}$, $\mathrm{Conj}(rs) = \{rs, r^3 s\}$
$\Rightarrow N = \{e\}, \langle r^2\rangle, \langle r\rangle \simeq C_4, \{e, r^2 s, r^2, s\} \simeq V_4, D_8$

②	$n(N)$		③ $\mathrm{Aut}\, G/N$
$D_8/e = D_8$	$= 0$	as $8 \nmid 12$	
$D_8/\langle r^2\rangle \simeq V_4$	$= 1$	V_4	$GL_2\mathbb{F}_2 \simeq S_3$
$D_8/\langle r\rangle \simeq C_2$	$= 3$	pairs of transpositions	1
$D_8/\langle r^2, s\rangle \simeq C_2$	$= 3$	"	1
$D_8/\langle r^2, rs\rangle \simeq C_2$	$= 3$		1
$D_8/D_8 \simeq e$	$= 1$		1

$\Rightarrow |\mathrm{Hom}(D_8, A_4)| = 0 + 6 + 3 + 3 + 3 + 1 = 16$