Group Homomorphisms

Def: Let $\overset{*}{G}, \overset{\star}{H}$ be groups. A <u>group homomorphism</u> is a function

$$f : G \to H \quad \text{satisfying} \quad f(ab) = f(a)f(b)$$

$$f(a * b) = f(a) \star f(b)$$

Ex: $f : \mathbb{Z} \to \mathbb{Z}_n$

$$k \mapsto k \pmod n$$

$$f(j+k) = j+k = f(j) + f(k) \quad \checkmark$$

Ex: $f : \overset{+}{\mathbb{Z}}_3 \to S_3$

$$0 \longmapsto \text{identity}$$
$$1 \longmapsto (123)$$
$$2 \longmapsto (132)$$

$$f(k) = (123)^k \quad \text{so} \quad f(j+k) = (123)^{j+k} = (123)^j(123)^k = f(j)f(k)$$

$\boxed{\text{Aside}}$

$(123)(123)$: $1 \mapsto 2 \mapsto 3$, $2 \mapsto 3 \mapsto 1$, $3 \mapsto 1 \mapsto 2$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$(132) = (213) = (321)$$

$$(a_1 a_2 \dots a_r) = (a_r a_1 a_2 \dots a_{r-1})$$

Proposition: If $f : G \to H$ is a homomorphism, then

$$f(e_G) = e_H$$

Proof: $f(e_G e_G) = f(e_G)$
$\shortparallel$
$f(e_G) f(e_G)$

$$f(e_G)f(e_G) = f(e_G)$$
$$\underbrace{f(e_G)f(e_G)[f(e_G)]^{-1}} = f(e_G)[f(e_G)]^{-1}$$
$$f(e_G)\, e_H = e_H$$
$$f(e_G) = e_H \quad \square$$

Def: $f: G \to H$ homomorphism.
The **kernel** of f is
$$\ker(f) = \{g \in G \mid f(g) = e\}$$
The **image** of f is
$$\operatorname{img}(f) = \{h \in H \mid \exists g \in G \text{ with } f(g) = h\}$$

Prop: $\ker(f) \leq G$ and $\operatorname{img}(f) \leq H$.
Proof: Do it!

$\square$

Ex: $f: \mathbb{Z} \to \mathbb{Z}_n$, $f(k) = k$

$$\begin{aligned}\ker(f) &= \{k \in \mathbb{Z} \mid f(k) = 0\} \\ &= \{k \in \mathbb{Z} \mid k = 0 \text{ mod } n\} \\ &= \{k \in \mathbb{Z} \mid n \text{ divides } k\} = \{nj \mid j \in \mathbb{Z}\} = n\mathbb{Z}\end{aligned}$$

Ex: $f: \mathbb{Z}_6 \to \mathbb{Z}_3$
$$k \longmapsto 2k$$

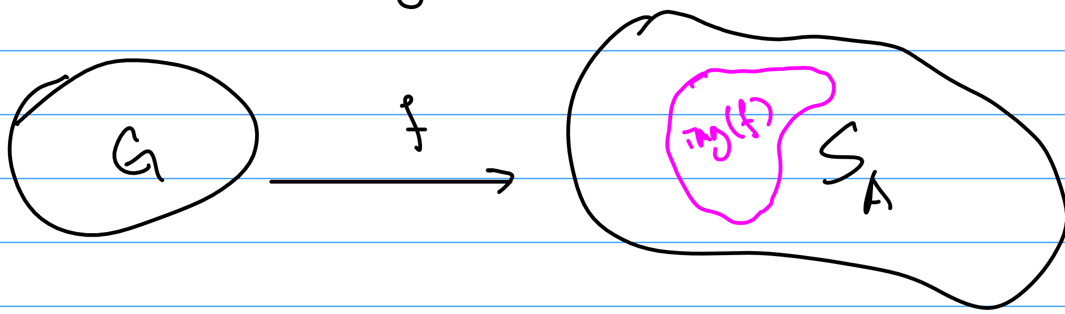
$$\ker(f) = \{0, 3\}.$$

Def: If $f: G \to H$ is a homomorphism
it's a <u>monomorphism</u> if its injective
it's a <u>epimorphism</u> if its surjective

Theorem (Cayley's Theorem):
If G is a group, then G is isomorphic to a group of permutations.

Proof: Idea is to define a monomorphism $G \xrightarrow{f} S_A$ for some set A.

Induce $G \to \text{Img}(f)$ isomorphism!!



Define $f: G \to S_A$ for $A = G$ (clever!)

$$g \longmapsto \sigma_g \qquad \sigma_g : A \to A$$
$$x \longmapsto gx$$

Claim 1: σ_g is a bijection

True since $\sigma_{g^{-1}}$ is an inverse function!

Thus for each $g \in G$, $\sigma_g \in S_A$.

Claim 2: $\sigma_g \sigma_h = \sigma_{gh}$

Proof: $(\sigma_g \sigma_h)(x) = \sigma_g(\sigma_h(x)) = \sigma_g(hx) = ghx = \sigma_{gh}(x)$ ✓

Thus $f: G \to S_A$, $g \mapsto \sigma_g$ is a homomorphism!

<u>Claim 3</u>: f is a monomorphism.

S'pose $f(g) = f(h)$. Then $\sigma_g = \sigma_h$.

$\Rightarrow \sigma_g(e) = \sigma_h(e) \Rightarrow g \cdot e = h \cdot e \Rightarrow g = h$ $\square$

<u>Theorem</u>: A homomorphism $f: G \to H$

is a monomorphism $\Leftrightarrow \ker(f) = \{e_G\}$.

<u>Proof</u>: S'pose $\ker(f) = \{e_G\}$.

Take $a, b \in G$ and suppose $f(a) = f(b)$

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

$\Longrightarrow ab^{-1} \in \ker(f) = \{e_G\}$. $ab^{-1} = e_G$

$a = b$ ✓

Conversely if f is a monomorphism, only one thing can get sent to e_H, and so $\ker(f) = \{e_G\}$ $\square$

<u>Products of Groups</u>

<u>Def</u>: Let $A_1, \dots, A_n$ be sets. The <u>cartesian product</u> is

$$\prod_{k=1}^{n} A_k = \{(a_1, \dots, a_n) \mid a_k \in A_k \ \forall\ 1 \le k \le n\}.$$

If $G_1, G_2, \dots, G_n$ are groups, we can do a product also!

Def: The <u>group product</u> or <u>direct product</u> or <u>product of groups</u> is $\prod_{k=1}^{n} G_k$ with operation

$$(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n) = (a_1b_1, a_2b_2, \dots, a_nb_n)$$

identity: $(e_{G_1}, e_{G_2}, \dots, e_{G_n})$. $= e$

inverses: $(a_1, a_2, \dots, a_n)^{-1} = (a_1^{-1}, a_2^{-1}, \dots, a_n^{-1})$.

Ex: $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(j,k) \mid j \in \mathbb{Z}_2, k \in \mathbb{Z}_3\}$
$\{(0,0), (1,0), (0,1), (1,1), (0,2), (1,2)\}$

$(1,1) + (1,1) = (0,2)$ ✓
$(0,2) + (1,1) = (1,0)$ ✓
$(1,0) + (1,1) = (0,1)$ ✓
$(0,1) + (1,1) = (1,2)$ ✓
$(1,2) + (1,1) = (0,0)$ ✓
$(0,0) + (1,1) = (1,1)$ ✓

$$\boxed{\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6}$$

Ex: $\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \dots \times \mathbb{Z}$ group operation = vector addition

Def: If $G_1, \dots, G_n$ are abelian with operation $+$ we write $G_1 \oplus G_2 \oplus \dots \oplus G_n$ in place of $G_1 \times G_2 \times \dots \times G_n$

$\bigoplus_{k=1}^{n} G_k$ " " $\prod_{k=1}^{n} G_k$

<u>direct sum</u> <u>group sum</u> <u>sum of groups</u>

Finitely Generated Abelian Groups

Theorem: (Fundamental Theorem for Abelian Groups - Prime Divisor Version)
If G is a finitely generated abelian group,

$$G \cong \mathbb{Z}_{p_1^{r_1}} \oplus \mathbb{Z}_{p_2^{r_2}} \oplus \cdots \oplus \mathbb{Z}_{p_n^{r_n}} \oplus \mathbb{Z}^s$$

where $p_1, \ldots, p_n$ are prime (not nec. distinct)

and $r_i \geq 1$ integers. Moreover this is unique up to permutation of the summands.

Ex: $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \not\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

$\quad\;\; \cong$

$\mathbb{Z}_4 \oplus \mathbb{Z}_2$

Ex: Abelian groups of order 28?

$$28 = 7 \cdot 2 \cdot 2$$

$$\boxed{\begin{array}{l} \bullet\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_7 \\ \bullet\ \mathbb{Z}_4 \times \mathbb{Z}_7 \end{array}}$$

$\cong \mathbb{Z}_{28}$

Ex: Abelian groups of order 24

$$24 = 3 \cdot 2 \cdot 2 \cdot 2$$

$\cong \mathbb{Z}_2 \times \mathbb{Z}_{12}$

- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$
- $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$
- $\mathbb{Z}_8 \times \mathbb{Z}_3$

$\cong \uparrow$ $\uparrow \mathbb{Z}_{24}$

$$(a_k a_{k+1} \cdots a_n)(a_{k-1} a_n) = (a_{k-1} a_k \cdots a_n)$$

$$(a_{n-1} a_n)(a_{n-2} a_n) = (a_{n-2} a_{n-1} a_n)$$

$$(a_{n-2} a_{n-1} a_n)(a_{n-3} a_n) = (a_{n-3} a_{n-2} a_{n-1} a_n)$$

$$\shortparallel$$

$$(a_{n-1} a_n)(a_{n-2} a_n)(a_{n-3} a_n)$$

$a R_\sigma b$ and $b R_\sigma c$.

$b \in orb_\sigma(a)$ and $c \in orb_\sigma(b)$

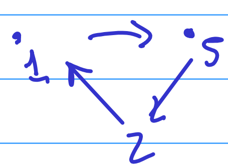
$b = \sigma^k(a)$ $\quad$ $c = \sigma^l(b)$

$$c = \sigma^l(\sigma^k(a)) = \sigma^{l+k}(a)$$

$$c \in orb_\sigma(a) \Rightarrow a R_\sigma c$$

$orb_\sigma(k) = \{\sigma^n(k) \mid n \in \mathbb{Z}\}$

$orb_\sigma(1)$, $orb_\sigma(2)$, $\ldots$ $orb_\sigma(6)$



$orb_\sigma(1) = \{1, 5, 2\}$

$\mathbb{Z}_2 \times \mathbb{Z}_2 \not\cong \mathbb{Z}_4$

$$\boxed{\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \iff (m,n) = 1}$$