

Recall

let  $f: A \rightarrow B$

The set  $f(C) = \{f(x) \mid x \in C\} \subseteq B$   
is the image of  $C$  in  $B$

Lemma

If  $\phi: G \rightarrow G'$  is an injective  
group homomorphism, then

$$\phi(G) \leq G'$$

and

$\phi: G \rightarrow \phi(G)$  is an isomorphism

Proof

$$\phi(G) = \{\phi(g) \mid g \in G\} \subseteq G' \quad \text{s.t.}$$

1) let  $x', y' \in \phi(G)$  since  $\phi$   
is injective,

$$\exists! x, y \in G, \quad \phi(x) = x' \wedge \phi(y) = y'$$

(so  $\phi$  is closed)

Consider  $x' \cdot y' = \phi(x) \cdot \phi(y) = \phi(x \cdot y)$   
 where  $x, y \in G$  thus  $x', y' \in \phi(G)$

2) Let  $e$  be identity of  $G$   
 $e'$  " " "  $G'$

$$\phi(e) \in \phi(G) \subseteq G'$$

$$\begin{aligned} \text{Consider } e' \cdot \phi(e) &= \phi(e) = \phi(e \cdot e) \\ &= \phi(e) \cdot \phi(e) \end{aligned}$$

by cancellation of  $G$

$$e' \cdot \phi(e) = \phi(e) \cdot \phi(e) \Rightarrow e' = \phi(e)$$

3) Let  $x' \in \phi(G)$ , then

$$\exists! x \in G, \phi(x) = x'$$

$$\text{Consider } e' = \phi(e) = \phi(x x^{-1}) \overset{\text{by homomorphism}}{=} \phi(x) \cdot \phi(x^{-1})$$

$$\text{hence } (x')^{-1} = \phi(x^{-1}), \text{ so } (x')^{-1} \in \phi(G)$$

$$\therefore \phi(G) \subseteq G'$$

since

$\phi: G \rightarrow G'$  is an injective homomorphism

$\phi: G \rightarrow \phi(G)$  is a bijective homomorphism

$$\text{so } G \cong \phi(G) \text{ and } \phi(G) \leq G'$$

## Cayley's Theorem

Every group is isomorphic to a group of permutations

Proof

let  $G$  be a group

Define  $\phi: G \rightarrow S_G$  by  $\phi(x) = \lambda_x$  for  $x \in G$

where  $\lambda_x: G \rightarrow G$  is defined by

$$\lambda_x(g) = x \cdot g$$

Notice  $\lambda_x$  is injective bcs

$$\forall g_1, g_2 \in G \quad \lambda_x(g_1) = \lambda_x(g_2) \Leftrightarrow x \cdot g_1 = x \cdot g_2 \\ \Rightarrow g_1 = g_2$$

$\lambda_x$  is surjective bcs

$$\forall h \in G, \exists g \in G \quad \lambda_x(g) = x \cdot (x' \cdot h) \\ = (x \cdot x') \cdot h \\ = eh = h$$

Therefore  $\lambda_x$  is a permutation of  $G$   
 bcs it is bijective f.n from  $G$  onto  $G$

Notice  $\phi$  is also injective

$$\forall x, y \in G \Leftrightarrow \lambda_x = \lambda_y \Leftrightarrow \forall g \in G, x \cdot g = y \cdot g \Rightarrow x = y$$

And  $\phi$  is homomorphic

$$\begin{aligned} \forall x, y \in G \quad \phi(x) \cdot \phi(y) &\Leftrightarrow \lambda_x \cdot \lambda_y \\ &= \lambda_x \circ \lambda_y \\ &= \lambda_{xy} = \phi(xy) \end{aligned}$$

By previous lemma, since

$\phi: G \rightarrow S_G$  is an injective homomorphism

$$\phi(G) \leq S_G \quad \wedge \quad G \cong \phi(G)$$

Example

$(\mathbb{Z}_3, +_3)$  Find left regular representation

$+_3$	0	1	2
0	0	1	2

$$\begin{array}{c|ccc} 1 & 1 & 2 & 0 \\ 2 & 2 & 0 & 1 \end{array}$$

let  $\lambda_0: \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$      $\lambda_0(n) = 0 +_3 n \quad \forall n \in \mathbb{Z}_3$

$\lambda_1: \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$      $\lambda_1(n) = 1 +_3 n$

$\lambda_2: \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$      $\lambda_2(n) = 2 +_3 n$

Then op on  $\phi(\mathbb{Z}_3) = \{\lambda_0, \lambda_1, \lambda_2\} \subseteq S_{\mathbb{Z}_3}$

$\cdot$	$\lambda_0$	$\lambda_1$	$\lambda_2$
$\lambda_0$	$\lambda_0$	$\lambda_1$	$\lambda_2$
$\lambda_1$	$\lambda_1$	$\lambda_2$	$\lambda_0$
$\lambda_2$	$\lambda_2$	$\lambda_0$	$\lambda_1$