Lecture 4

Friday, January 30, 2015 9:54 AM

2 $|G|$ = cardinality of $G = \# G = \mathrm{card}(G)$

I $|g|$ = order of $g \in G = \mathrm{ord}(g)$

Homomorphisms & siblings thereof

Motivating question: When are 2 groups the same?

Necessary prior: How do we compare groups?

We use functions to compare sets, but groups have more structure

$$\begin{tikzcd}
(g,g') \arrow[r, mapsto] \arrow[d, mapsto, bend right] & (\varphi(g),\varphi(g')) \arrow[d, mapsto, bend left] \\
G\times G \arrow[r, "\varphi\times\varphi"] \arrow[d, "\cdot"'] & H\times H \arrow[d, "*"] \\
G \arrow[r, "\varphi"'] & H \\
g\cdot g' \arrow[r, mapsto, bend right] & \varphi(g\cdot g') = \varphi(g)*\varphi(g')
\end{tikzcd}$$

`$ \varphi $`

fn on sets

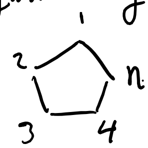
Defn φ is a <u>homomorphism</u> $G \longrightarrow H$ if

1. fn on underlying sets
2. $\forall g,g' \in G.\ \varphi(gg') = \varphi(g)\varphi(g')$.

I.e. φ "respects structure" or "preserves mult."

e.g. ① $\mathrm{id}: G \longrightarrow G$ is a hom

② $D_{2n} \xrightarrow{\varphi} S_n$

symmetry of  $\longmapsto$ associated permutation of $\{1, 2, \dots, n\}$

D_{2n} & S_n have composition as operation and φ obviously preserves comp'n.

③ $\mathbb{Z}_4 \xrightarrow{f} \mathbb{Z}_2$

$x \longmapsto$ remainder of x after div by 2

$0 \longmapsto 0$

$1 \longmapsto 1$

$2 \longmapsto 0$

$3 \longmapsto 1$

Homomorphism?

$\boxplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\longmapsto$

✓

$\boxplus$	0	1	0	1
0	0	1	0	1
1	1	0	1	0
0	0	1	0	1
1	1	0	1	0

$$f(x \boxplus y) = f(x) \boxplus f(y)$$

(4) $\mathbb{Z}_2 \longrightarrow \mathbb{Z}_4$

$x \longmapsto 2x$

$0 \longmapsto 0$

$1 \longmapsto 2$

$$\begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \longmapsto \begin{array}{c|cc} & 0 & 2 \\ \hline 0 & 0 & 2 \\ 2 & 2 & 0 \end{array}$$

<u>Exc</u> Analogous homs $\mathbb{Z}_{mn} \xrightarrow{\text{red}} \mathbb{Z}_n$

$\mathbb{Z}_n \xrightarrow[\cdot m]{} \mathbb{Z}_{mn}$

(5) $\{\pm 1\} \longrightarrow \mathbb{Z}_2$

$1 \longmapsto 0$

$-1 \longmapsto 1$

$$\begin{array}{c|cc} \cdot & 1 & -1 \\ \hline 1 & 1 & -1 \\ -1 & -1 & 1 \end{array} \longmapsto \begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$$

<u>Theorinition</u> A homomorphism $\varphi: G \longrightarrow H$ is an <u>isomorphism</u> if the following equivalent conditions hold:

(1) A homomomorphism $\varphi^{-1}: H \longrightarrow G$ exists s.t. $\varphi \circ \varphi^{-1} = id_H$ & $\varphi^{-1} \circ \varphi = id_G$

(2) φ is bijective. (as a fn).

<u>Note</u> · Isomorphic groups are "the same" wrt all structural properties

· Often write $\varphi: G \xrightarrow{\cong} H$, $\varphi: G \cong H$, $G \xrightarrow[\cong]{\varphi} H$ when φ is an iso $G \longrightarrow H$.

Defn Groups G, H are isomorphic if $\exists$ iso $\varphi: G \xrightarrow{\cong} H$.
We write $G \cong H$ in this case.

Pf of Theorinition ① $\Rightarrow$ ② : Having an inverse as a fn is equivalent to being a bijection.

② $\Rightarrow$ ① : Must check that φ^{-1} (the fn) is in fact a homomorphism. Suppose

$$\varphi^{-1}(h) = g, \quad \varphi^{-1}(h') = g' \text{ so that}$$

$$\varphi(g) = h, \quad \varphi(g') = h' \text{ whence}$$

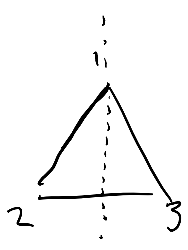
$$\varphi(gg') = \varphi(g)\varphi(g') = hh'$$

since φ is a hom

Thus $\varphi^{-1}(hh') = gg' = \varphi^{-1}(h)\varphi^{-1}(h')$, as desired. $\square$

e.g. ① $id: G \xrightarrow{\cong} G$

② $\varphi: D_6 \xrightarrow{\cong} S_3$



$$r \longmapsto (1\ 2\ 3)$$
$$s \longmapsto (2\ 3)$$

observe: everything in S_3 is a product of these cycles

$\Downarrow$

φ is surjective

φ is a surj b/w sets of cardinality $6 \Rightarrow \varphi$ is bij.

③ $\varphi : \mathbb{Z} \xrightarrow{\cong} \mathbb{Z}$

$n \longmapsto -n$

$$\varphi(m+n) = -(m+n) = (-m) + (-n) = \varphi(m) + \varphi(n)$$

bijective ✓

<u>Note</u> Isos $G \to G$ are called automorphisms.

<u>Non-e.g.</u> $\mathbb{Z}_4 \to \mathbb{Z}_2$ & $\mathbb{Z}_2 \to \mathbb{Z}_4$ are not isos.

④ $\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}_{>0}, \cdot)$

$$\exp(x+y) = \exp(x) \cdot \exp(y)$$

$\log : (\mathbb{R}_{>0}, \cdot) \longrightarrow (\mathbb{R}, +)$

$$\log(xy) = \log(x) + \log(y)$$

Thus $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$.

<u>Thm</u> If $\varphi : G \to H$ is an <u>isomorphism</u>, then

① $|G| = |H|$

② G is abelian iff H is abelian

③ $\forall x \in G$. $|x| = |\varphi(x)|$.

e.g. $S_3 \not\cong \mathbb{Z}_6$ have same cardinality : 6

S_3 nonabelian

$\mathbb{Z}_6$ abelian

Ψ

1 has order 6

no order 6 elts of S_3.

Lemma If $\varphi : G \to H$ is a hom, then $\varphi(1_G) = 1_H$.

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