- subgroups, homomorphism
- Isomorphisms, symmetric groups

MATH 113 LECTURE 8 NOTES

we can use homomorphisms to construct new subgroups

Proposition If G, H groups, $K \leq G$, $L \leq H$ and if $\varphi: G \to H$ is a homomorphism, then

(1) $\varphi(K) = \{\varphi(k) \mid k \in K\}$ is a subgroup in H. — image of φ.

(2) $\varphi^{-1}(L) = \{g \in G \mid \varphi(g) \in L\}$ is a subgroup in G. — this notation is standard. pre-image of φ.

Proof:

(1) Since $e_G \in K$, $\varphi(e_G) = e_H \in \varphi(K) \Rightarrow \varphi(K)$ is nonempty.

If $x, y \in \varphi(K)$ then $x = \varphi(k_1)$, $y = \varphi(k_2)$ for some k_1, k_2.

$xy^{-1} = \varphi(k_1)\varphi(k_2)^{-1} = \varphi(k_1)\varphi(k_2^{-1}) = \varphi(k_1 k_2^{-1})$ (middle 2 equalities from homomorphism)

$\Rightarrow xy^{-1} \in \varphi(K)$ since $k_1 k_2^{-1} \in K$ (as K is a subgroup)

(2) Need to check $\varphi^{-1}(L)$ nonempty.

Since $\varphi(e_G) = e_H$ and $e_H \in L \Rightarrow e_G \in \varphi^{-1}(L)$ $\therefore \varphi^{-1}(L)$ nonempty

If $x, y \in \varphi^{-1}(L)$, then $\varphi(x) \in L$, $\varphi(y) \in L$ (middle 2 implications by homomorphism)

$\Rightarrow \varphi(x)\varphi(y)^{-1} \in L \Rightarrow \varphi(x)\varphi(y^{-1}) \in L \Rightarrow \varphi(xy^{-1}) \in L \Rightarrow xy^{-1} \in \varphi^{-1}(y)$.

$\therefore \varphi^{-1}(L)$ is a subgroup by subgroup criterion.

Definition If $\varphi: G \to H$ is a homomorphism, then the kernel of φ = $\varphi^{-1}(\{e_H\})$

$\ker \varphi = \varphi^{-1}(\{e_H\}) = \{g \in G \mid \varphi(g) = e_H\}$

$\varphi(G) = \{\varphi(g) \mid g \in G\}$ is the image of φ.

$\ker \varphi \leq G$

$\varphi(G) \leq H$

Theorem A group homomorphism $\varphi: G \to H$ is injective if and only if $\ker \varphi = \{e_G\}$ (i.e. kernel is trivial).

Proof

Suppose φ is injective. Let $x \in \ker\varphi$. $\varphi(x) = e_H$.
But we know that $\varphi(e_G) = e_H$ so $x = e_G$ by injectivity.
$\therefore \ker(\varphi) = \{e_G\}$.

Suppose $\ker\varphi = \{e_G\}$.
If $\varphi(x) = \varphi(y)$ for some $x, y \in G$ then
$$\varphi(x)\varphi(y)^{-1} = \varphi(y)\varphi(y)^{-1} = e_H$$
$$\Rightarrow \varphi(xy^{-1}) = e_H \Rightarrow xy^{-1} = e_G \quad (\because xy^{-1} \in \ker\varphi)$$
$$\Rightarrow x = y$$
$\therefore \varphi$ is injective.

Example

$\det : GL_n(\mathbb{C}) \to \mathbb{C}^\times$
($n\times n$ invertible matrices in $\mathbb{C}$ with matrix mult) ($\mathbb{C}\setminus\{0\}$ with multiplication)

$\ker\det = \{M \in GL_n(\mathbb{C}) \mid \det M = 1\}$

This is also called $SL_n(\mathbb{C})$
special linear

Definition

An <u>isomorphism</u> is a bijective homomorphism
If there exists an isomorphism $\varphi: G \to H$, say G and H are <u>isomorphic</u>.

- ~~φ has an inverse function φ^{-1}~~
- φ^{-1} is automatically also a homomorphism.

Lemma

If $\varphi: G \to H$ is an isomorphism, then $\varphi^{-1}: H \to G$ is also an isomorphism.
(φ^{-1} exists because isomorphisms are bijective).

Proof:

If $x, y \in H$, need to check
$$\varphi^{-1}(x)\varphi^{-1}(y) = \varphi^{-1}(xy)$$

$\Leftrightarrow \varphi(\varphi^{-1}(x)\varphi^{-1}(y)) = \varphi(\varphi^{-1}(xy))$ since φ is a bijection

(by homomorphism) $\Leftrightarrow \varphi(\varphi^{-1}(x))\varphi(\varphi^{-1}(y)) = \varphi(\varphi^{-1}(xy))$

$\Leftrightarrow xy = xy$

φ^{-1} is automatically a bijection as it is the inverse of a bijection

$\therefore$ Property of being isomorphic is symmetric. i.e. If G is isomorphic to H, then H is also isomorphic to G.

Note also if $\varphi: G \to H$
$\psi: H \to K$ are isomorphisms, then
$\varphi \circ \psi$ $\psi \circ \varphi: G \to K$ is also an isomorphism.

Suffices to check $\psi \circ \varphi$ is a homomorphism and is bijective.
Composition of bijections is a bijection so $\psi \circ \varphi$ is a bijection.

$\psi(\varphi(g_1 g_2)) = \psi(\varphi(g_1)\varphi(g_2)) = \psi(\varphi(g_1))\,\psi(\varphi(g_2))$ $\therefore$ $\psi \circ \varphi$ is a homomorphism.

G	b
a	ab

$\xrightarrow{\text{same as applying } \varphi \text{ entrywise}}$

H	$\varphi(b)$
$\varphi(a)$	$\varphi(a)\varphi(b) = \varphi(ab)$

So an isomorphism simply relabels the elements of the groups, keeping the multiplication the same.
For almost all purposes, isomorphic groups are the same.
(Δ symmetries of Δ, if you don

Russell's paradox

Problem when trying to define equivalence relation using isomorphism. To do so, you need a set.
What is the set of all groups? Russell's paradox.

Last time we showed any cyclic group is isomorphic to one of $(\mathbb{Z}, +)$ or $(\mathbb{Z}/d\mathbb{Z}, +)$ for some $d \in \mathbb{Z}_{>0}$.

Common Abbreviations

group $\to$ gp
subgroup $\to$ subgp
homomorphism $\to$ hom
isomorphism $\to$ iso

Symmetric Groups

If X is a set,

$Sym(X) = \{ \text{bijections} : X \to X \}$ is a group with composition as the operation.

lemma

If $f: X \to Y$ is a bijection, then $Sym(X)$ is isomorphic to $Sym(Y)$ via

$\varphi(g)$ $\quad \varphi: Sym(X) \to Sym(Y)$

$\varphi(g) = f \circ g \circ f^{-1}$

$$f^{-1}: Y \to X$$
$$g: X \to X \quad \therefore f \circ g \circ f^{-1}: Y \to Y$$
$$f: X \to Y \quad \in Sym(Y)$$

since all functions are bijections

Suffices to check that φ is a homomorphism.

$$\varphi(g_1)\varphi(g_2) = f \circ g_1 \circ f^{-1} \circ f \circ g_2 \circ f^{-1}$$
$$= f \circ g_1 \circ g_2 \circ f^{-1} = f \circ g_1 g_2 \circ f^{-1}$$
$$= \varphi(g_1 g_2).$$

Hence, if X finite, there is a bijection $X \to \{1, 2, \dots, |X|\}$

just label the items.

Hence, studying $Sym(X)$ is essentially the same as studying $Sym(\{1, 2, \dots, |X|\})$.

Common to abbreviate $Sym(\{1, 2, \dots, n\})$ to Sym_n $\left(\text{sometimes } S_n, \ \Sigma_n \right)$

How to write a bijection? i.e. an element of Sym_n

If $g \in Sym_n$, g is determined by a list $g(1), g(2), \dots, g(n)$

(one line notation of g)

$4321 \circ 2134 = 3421$

Two line notation
$$\begin{array}{l} 1 \ 2 \ 3 \ 4 \quad \leftarrow \text{input.} \\ 4 \ 3 \ 2 \ 1 \quad \leftarrow \text{one line notation below} \end{array}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \begin{array}{l} \text{apply} \\ \text{apply} \end{array} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 4 & 3 & 1 & 2 \end{pmatrix}$$

Inverse: swap order of rows

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{swap} \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$