Last time: group homomorphisms
+ subgroups

Recall:

Defn Let G, H be groups.
A map $\phi: G \to H$ is called a homomorphism if
$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$$
$\forall\, g_1, g_2 \in G$.

Defn ϕ is called a group isomorphism, or isomorphism, if ϕ is also a bijection.

Isomorphism is NOT equality, just as bijection of sets is not.

Ex: A set of five bananas is not equal to a set of five apples.

But we classify groups up to isomorphism. Just as we classify sets up to bijection.

Exer If $\phi: G \to H$ is an isomorphism, then $\phi^{-1}: H \to G$ is an isomorphism.

Pf Need to show ϕ^{-1} is a homomorphism. (It's obviously a bijection.)

$$\begin{aligned}
\phi^{-1}(h_1 h_2) &= \phi^{-1}(\phi(g_1)\phi(g_2)) && \phi \text{ surjection} \quad (1)\\
&= \phi^{-1}(\phi(g_1 g_2)) && \phi \text{ homomorphism}\\
&= \phi^{-1}\circ\phi\,(g_1 g_2) && \text{notation}\\
&= g_1 g_2 && \text{definition of } \phi^{-1}\\
&= \phi^{-1}(h_1)\cdot\phi^{-1}(h_2) && \text{defn of } g_1, g_2 \text{ in } (1).
\end{aligned}$$
//

Rmk
- $\mathrm{id}_G: G \to G$ is a homomorphism.
- if $G \xrightarrow{\phi} H$, $H \xrightarrow{\psi} K$ are homomorphisms, $\psi\circ\phi$ is a homomorphism.
- If $H \subset G$ is a subgroup, then the inclusion map $H \to G$ is a homomorphism.

Defn Let X be a set. We write

$$\mathrm{Aut}(X)$$

or

$$\mathrm{Aut}_{set}(X)$$

for the set of bijections from X to itself.

Prop'n $\mathrm{Aut}(X)$ is a group under composition.

Pf (1) Composing functions is associative:

$$(f \circ g) \circ h = f \circ (g \circ h).$$

(2) $\mathrm{id}_X : X \to X$, $x \mapsto x$

is unit. $f \circ \mathrm{id}_X = \mathrm{id}_X \circ f$

(3) f^{-1} is f's inverse:

$$f \circ f^{-1} = \mathrm{id}_X = f^{-1} \circ f. \quad //$$

Defn Let

$$\underline{n} = \{1, \cdots, n\}.$$

Then

$$\mathrm{Aut}_{\mathrm{Set}}(\underline{n}) =: S_n$$

is the symmetric group on a set of n elements.

Ex

$\underline{n=1}$: $\mathrm{Aut}(\{1\})$ is the group w/ one element.

$\underline{n=2}$: $\mathrm{Aut}(\{1,2\})$ has two elements.

$$\mathrm{id}: \begin{array}{l} 1 \mapsto 1 \\ 2 \mapsto 2 \end{array}, \quad \sigma: \begin{array}{l} 1 \mapsto 2 \\ 2 \mapsto 1 \end{array}$$

and $\sigma \circ \sigma = \mathrm{id}$.

$\underline{n=3}$: S_3 has $3!$ elements.

We'll learn more about its structure soon.

Def'n ① Let X be a set,

and G a group.

A group action of G on X is a homomorphism

$\phi: G \longrightarrow \mathrm{Aut}(X)$.

Def'n ② A left group action of G on X is a map

$$G \times X \longrightarrow X$$
$$(g, x) \longmapsto gx$$

such that

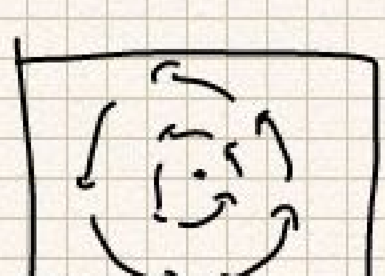
- $1x = x$
- $g(hx) = (gh)x$.

Example Let $S^1 = \{ z \in \mathbb{C} \mid |z| = 1 \}$

Define $\phi: S^1 \longrightarrow \mathrm{Aut}(\mathbb{C})$

$$z \longmapsto f_z$$

where $f_z(w) := z \cdot w$ (rotation by z).



Philosophy: Given a group action $G \to \mathrm{Aut}_{Set}(X)$, we can break X into <u>orbits</u>.

$\forall\ x \in X$,

$$\mathcal{O}_x := \{y \mid y = gx\}$$

Ex

$$\mathbb{C} = \coprod_{r \in \mathbb{R}_{\geq 0}} \mathcal{O}_r,$$

where $\mathcal{O}_r = \{ z \mid z = re^{i\theta} \}$

$=$ Circle of radius r.

$$\mathcal{O}_0 = \{0\} \subset \mathbb{C}.$$

Set $X/G :=$ set of orbits.

We can then count elements of X (if X is finite) in by counting orbits one by one.

Ex G a group.

$\forall\ g \in G$, we have

a bijection

$$\phi_g : G \longrightarrow G$$
$$x \longmapsto gx.$$

This is a bijection since:

- $y \in G \Rightarrow y = g(g^{-1}y)$
$$= \phi_g(g^{-1}y)$$

- $\phi_g(y) = \phi_g(y') \Rightarrow gy = gy'$
$$\Rightarrow y = y'.$$

Moreover,

$$\phi_{g_1g_2}(x) = (g_1g_2)(x)$$
$$= g_1(g_2(x))$$
$$= \phi_{g_1} \circ \phi_{g_2}(x)$$

so the map

$$\phi : G \longrightarrow \mathrm{Aut}_{Set}(G)$$
$$g \longmapsto \phi_g$$

is a homomorphism i.e., every group acts on itself.

If $H < G$ is a subgroup, then

- $H \to G \to \mathrm{Aut}_{Set}(G)$

  is a group action.

More concretely, we have

$$\begin{aligned} \phi_h : G &\longrightarrow G \\ x &\longmapsto h \cdot x. \end{aligned}$$

$\forall\, h \in H$.

We'll show that if G is finite, then

$$|O_x| = |H| \;\; \forall\, x \in G.$$

# of elements in O_x

# of elements in H.

Hence $$G = \coprod O_x$$

$$\Rightarrow \;\; |G| = \underbrace{\sum}_{\substack{\text{summing} \\ \text{over set of orbits}}} |H|$$

$\Rightarrow$ $|H|$ divides $|G|$.

This is <u>Lagrange's</u> <u>Theorem</u>.