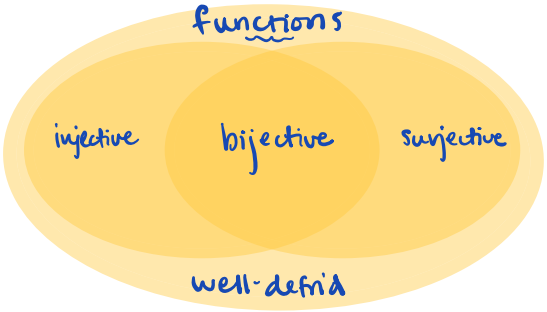
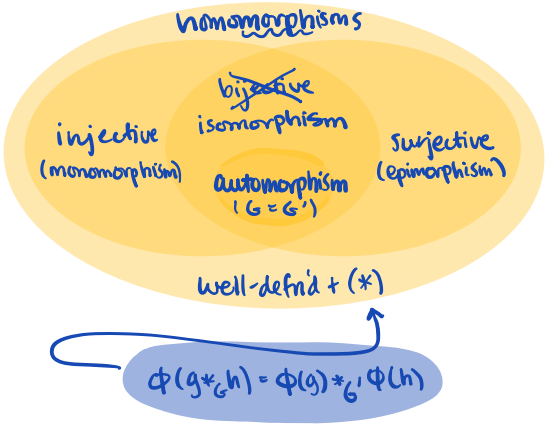
# Group Homomorphisms

Recall: for sets: $f: A \to B$ ⇝ now, for groups: $\phi: G \to G'$




Does the fn $\phi: G \to G'$ satisfy...

(1) $\phi(e_G) = e_{G'}$?

(2) $\phi(g^{-1}) = \phi(g)^{-1}$?

(3) $\phi(g^k) = \phi(g)^k$?

If the answer to any of these is "NO" then $\phi$ can't satisfy (*)!

Checking (1)-(3) isn't enough (in general) to know $\phi$ satisfies (*).
These conditions are necessary, not sufficient.

**Ex** $\mathbb{Z} \xrightarrow[x \mapsto x^2]{Sq} \mathbb{Z}$ is not a homomorphism

Pf/ It's a function, but it doesn't satisfy (*):

$$(x+y)^2 \neq x^2 + y^2 \quad (\text{e.g. } x = y = 1).$$

**Ex**. $\mathbb{Z} \xrightarrow{n\cdot} \mathbb{Z}$ is an endomorphism (homomorphism s.t. $G = G'$)

Pf/ Multiplication is a well-defn'd function, and (*) encodes distribution:

$$n\cdot(x+y) = n\cdot x + n\cdot y \quad \forall x, y \in \mathbb{Z}.$$

**Ex**. $\mathbb{Z} \xrightarrow{-1\cdot} \mathbb{Z}$ is an automorphism (this is called an "involution")

Pf/ Multiplication by -1 is a bijection (its inverse is itself!) and satisfies (*) by the previous ex.

**Note** $id: \mathbb{Z} \to \mathbb{Z}$ is a different automorphism!
We can consider the set $Aut(G) = \{\text{automorphisms of } G\}$.
In fact:

**Prop.** $Aut(G)$ is a group! (under composition)

**Ex**. What is $Aut(\mathbb{Z})$? **Claim** $Aut(\mathbb{Z}) = \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$ (gp iso)

Pf/ We first establish $Aut(\mathbb{Z}) = \{\pm 1\}$ as a set. We've already discussed $\supseteq$ so we just need to show $\subseteq$. Let $\phi \in Aut(\mathbb{Z})$. Since $\phi$ is a homomorphism, $\phi(0) = 0$ and $\phi(n) = \phi(1+1+\cdots+1) = \phi(1) + \cdots + \phi(1) = n\cdot\phi(1)$. That is, $\phi$ can be described

as "multiplication by $\phi(1)$". This is a bijection iff $\phi(1) \in \{1, -1\}$.

Now we show $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ as groups. Consider $f: \{\pm 1\} \to \mathbb{Z}/2\mathbb{Z}$ which sends $+1 \mapsto 0$ and $-1 \mapsto 1$. (Note: this is the only choice since $f(id) = 0$ necessarily.) To check $f$ is a group homomorphism, the only non-trivial part to check is

$$\begin{aligned} f(-1 \circ -1) &= f(id) \\ &= 0 \\ &\equiv 1 + 1 \\ &= f(-1) + f(-1). \end{aligned}$$

□

**Prop** If $\phi: G \to G'$ is a group homomorphism, then

① $H \leq G \Rightarrow \phi(H) \leq G'$ $= \{g \in G \mid \phi(g) \in H'\}$

② $H' \leq G' \Rightarrow \phi^{-1}(H') \leq G$ (not nec. a gp hom!)

Pf/ ① Let $H \leq G$. Since $e \in H$ and $\phi$ is gp hom,

$$e = \phi(e) \in \phi(H).$$

Now suppose $g, g' \in \phi(H)$. Then $g = \phi(h)$ and $g' = \phi(h')$ for some $h, h' \in H$. Thus $h \cdot h' \in H$ and so

$$g \cdot g' = \phi(h) \cdot \phi(h') = \phi(h \cdot h') \in \phi(H).$$

Finally, if $g \in \phi(H)$, so $g = \phi(h)$ for some $h \in H$, then $h^{-1} \in H$ so

$$g^{-1} = \phi(h)^{-1} = \phi(h^{-1}) \in \phi(H).$$

Hence $\phi(H) \leq G'$.

② Now let $H' \leq G'$. Since $e \in H'$, we can consider $\phi^{-1}(e) = \{g \in G \mid \phi(g) = e\}$ ($\ker(\phi)$), and since $\phi$ is gp hom we know $e \in \phi^{-1}(e) \subseteq \phi^{-1}(H')$. Now suppose $g, g' \in \phi^{-1}(H')$. By defn, $\phi(g), \phi(g') \in H'$ so $\phi(g) \cdot \phi(g') = \phi(g \cdot g') \in H'$. Hence $g \cdot g' \in \phi^{-1}(H')$.

Finally, if $g \in \phi^{-1}(H')$ then $\phi(g) \in H'$ so $\phi(g)^{-1} = \phi(g^{-1}) \in H'$ and therefore $g^{-1} \in \phi^{-1}(H')$. □

**Ex/Defn** The kernel of $\phi: G \to G'$ is $\ker(\phi) := \phi^{-1}(e)$. We just showed $\ker\phi \leq G$.

**Prop.** $\phi$ is injective $\iff \ker\phi = e$.

Pf/ ($\Rightarrow$) If $x \in \ker\phi$, then $\phi(x) = e = \phi(e)$ so injectivity implies $x = e$.

($\Leftarrow$) Suppose $\phi(x) = \phi(y)$. Then

$$\begin{aligned} e &= \phi(y)\,\phi(x)^{-1} \\ &= \phi(y)\,\phi(x^{-1}) \\ &= \phi(yx^{-1}) \end{aligned}$$

So $yx^{-1} \in \ker\phi$. If $\ker\phi = e$, this says $yx^{-1} = e$, i.e. $y = x$. So $\phi$ is injective. □

**Ex/Defn** The image of $\phi: G \to G'$ is $\mathrm{im}(\phi) = \phi(G)$. We showed $\mathrm{im}\phi \leq G'$.

**Prop.** $\phi$ is surjective $\iff \operatorname{im}\phi = G'$.

Pf/($\Rightarrow$) We know $\subseteq$, so just need to show $\operatorname{im}\phi \supseteq G'$. Given $g' \in G'$, $\exists g \in G$ s.t. $\phi(g) = g'$ since $\phi$ is surjective. Then by defn, $g' \in \operatorname{im}\phi$.

($\Leftarrow$) Let $g' \in G'$. Then since $G' = \operatorname{im}\phi = \{\phi(g) \in G' \mid g \in G\}$ there exists $g \in G$ s.t. $g' = \phi(g)$. This is the defn of $\phi$ being surjective. $\square$

**Rmk** $\phi: G \to G'$ is gp isomorphism (1) is gp hom and (2) is bij (↳ inj ↳ surj) and (2) holds $\iff$ $\ker\phi = e \leq G$, $\operatorname{im}\phi = G'$.

( also $\iff \exists$ inverse $\phi^{-1}: G' \to G$ )

**Ex.** Consider the group $G$ w/ Cayley table:

| $*$ | ♡ | ◇ | ♤ | ♧ |
|---|---|---|---|---|
| ♡ | ♡ | ◇ | ♤ | ♧ |
| ◇ | ◇ | ♡ | ♧ | ♤ |
| ♤ | ♤ | ♧ | ♡ | ◇ |
| ♧ | ♧ | ♤ | ◇ | ♡ |

**Claim** $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = K_4$ "klein 4 gp"

Pf/ Define $\phi: G \to K_4$ by

♡ $\mapsto (0,0)$ ♤ $\mapsto (0,1)$

◇ $\mapsto (1,0)$ ♧ $\mapsto (1,1)$.

This is bijective, and can check it's a hom using the Cayley table. (exc)

**Note** Could have defined $\phi$ by

♡ $\mapsto (0,0)$ ♤ $\mapsto (1,0)$

◇ $\mapsto (0,1)$ ♧ $\mapsto (1,1)$

This is a different isomorphism! ($\Rightarrow$ isos not nec. unique)

Call it $\phi'$. Note $\phi' = \phi \circ \text{swap}$, where $\text{swap} \in \operatorname{Aut}(\mathbb{Z}/2 \times \mathbb{Z}/2)$ swaps the two factors, i.e. switches $(1,0) \leftrightarrow (0,1)$.

**Q.** Given $n \in \mathbb{Z}_{\geq 1}$, how many groups (up to isomorphism) are there of order $n$?

"**A.**" Well...

$n=1$ : $e$ | 1

$n=2$ : $\mathbb{Z}/2$ | 1

$n=3$ : $\mathbb{Z}/3$ | 1

$n=4$ : $\mathbb{Z}/2$, $K_4$ | 2

$n=5$ : $\mathbb{Z}/5$ | 1

⋮

Wikipedia has a list for $n \leq 30$

in general, this is very hard!! (believed impossible in general)

↝ simplify by adding restrictions:

- $n = p$ prime : $\mathbb{Z}/p$
- $G$ is simple : "classification of finite simple gps" (monster group) (check out: $H \leq G \Rightarrow H = e$ or $G$)
- $G$ solvable : ...
- $|G| = pq$ primes $p, q$ : ...

Sylow Thms (to be discussed) will be helpful!

~break~ minute sheet:
- what's ur fave gp (so far)
- what's something you found confusing / interesting
- do you know what you're gonna be for Halloween?

## Group Work

(1) (a) Prove $\mathrm{Aut}(G)$ is a group ($G$ is a group)

(b) Given two groups $G, G'$, is $\mathrm{Hom}(G,G') = \{\phi : G \to G' \mid \text{gp hom}\}$ a group? If yes, prove it. If not, can you add conditions (put restrictions on $\phi$) to make it a group?

Bonus: When is the resulting gp Abelian?

(2) Let $(A, +, 0)$ be an Abelian gp and $u, v : A \to A$ homomorphisms. Define $f, g : A \to A$ by

$$f(a) = a - v(u(a)) \quad \text{and} \quad g(a) = a - u(v(a)).$$

Show $\ker f \cong \ker g$.

(3) Let $G$ be a finite group and $\phi : G \to G$ an automorphism s.t. $\phi(g) = g \Rightarrow g = e$. Prove

(a) every elmt of $G$ is of the form $g^{-1}\phi(g)$

(b) if $\phi$ is an involution ($\phi \circ \phi = id$) then $\phi = i$ is inversion and $G$ is an Abelian gp of odd order.