

## Kernels and canonical homomorphisms

Def. Let  $\phi: G \rightarrow H$  be a homomorphism of groups. The **kernel** of  $\phi$  is the subset

$$\phi^{-1}(e) := \{g \in G \mid \phi(g) = e\}.$$

Prop. For any homom.  $\phi: G \rightarrow H$ ,  $\ker \phi$  is a normal subgroup of  $G$ .  
(Proof.)  $\{e\} \trianglelefteq H$  is normal. Homomorphisms pull normal subgroups back to normal subgroups.  $\square$

Ex. ①  $\phi: \mathbb{Z} \rightarrow \mathbb{Z}_n$        $\ker \phi = n\mathbb{Z}$   
 $k \mapsto k \pmod{n}$

②  $\phi: GL_n(\mathbb{R}) \rightarrow \mathbb{R}^*$        $\ker \phi = SL_n(\mathbb{R})$   
 $A \mapsto \det A$

③  $\phi: \mathbb{R} \rightarrow S^1 \subseteq \mathbb{C}$        $\ker \phi = \mathbb{Z}$   
 $t \mapsto \exp(2\pi i t)$

Prop. A homom.  $\phi: G \rightarrow H$  is injective iff  $\ker \phi = \{e\}$ .

(Proof.) Exercise.

Ex. Consider positive integers  $p, n$ , with  $p$  prime,  $\gcd(p, n) = 1$ .

Let's count the homomorphisms

$$\phi: \mathbb{Z}_p \rightarrow \mathbb{Z}_n.$$

$\ker \phi \leq \mathbb{Z}_p$  is a normal subgroup  $\Rightarrow \ker \phi = \{e\}$  or  $\ker \phi = \mathbb{Z}_p$

If  $\ker \phi = \mathbb{Z}_p$ , then  $\phi(k) = 0, \forall k \in \mathbb{Z}_p$ . This is a homom.

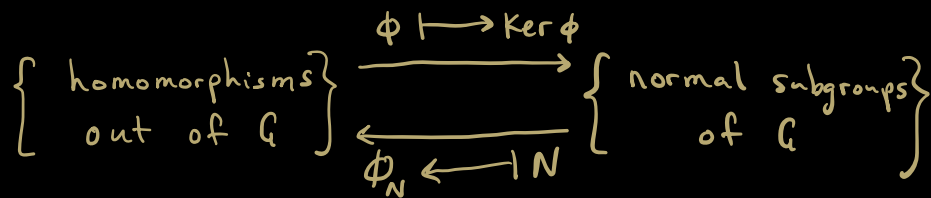
If  $\ker \phi = \{e\}$ , then  $\phi$  is injective.

So  $\phi(\mathbb{Z}_p)$  is a subgroup of order  $p$ .

But  $p \nmid n$ , so no such  $\phi$  can exist.

There is only one homom.  $\phi: \mathbb{Z}_p \rightarrow \mathbb{Z}_n$  — the trivial one.

## The isomorphism theorems



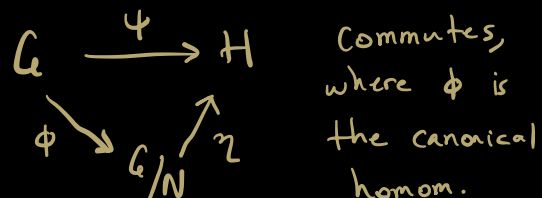
Def. Let  $N \leq G$  be a normal subgroup. The **canonical homomorphism** (or **natural homomorphism**)  $\phi: G \rightarrow G/N$  is defined by  $\phi(g) := gN$ .

Exercise. Verify that  $\phi: G \rightarrow G/N$  is a homom. with  $\ker \phi = N$ .

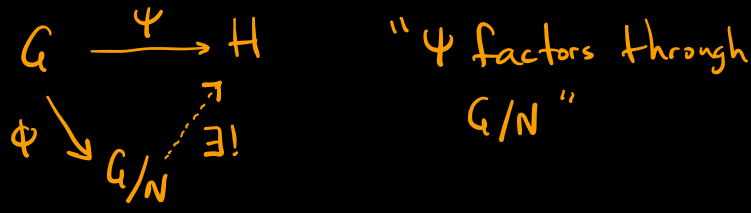
## The first isomorphism theorem

Let  $\psi: G \rightarrow H$  be any homom. of groups, and let  $N = \ker \psi$ .

Then there is a unique isomorphism  $\eta: G/N \rightarrow \psi(G)$  for which the diagram



$\left\{ \begin{array}{l} \text{isomorphisms} \\ \text{out of } G/N \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{homomorphisms out} \\ \text{of } G \text{ with } \text{Ker} = N \end{array} \right\}$



(Proof.) Given  $\Psi: G \rightarrow H$  as described, define

$$\eta: G/N \rightarrow \Psi(G) \subseteq H$$

$$gN \mapsto \Psi(g).$$

- NTS;  $\eta$  well-defined
- ② homomorphism
  - ③ bijection

- ① Well-defined
- if  $g_1N = g_2N$ , then  $g_1^{-1}g_2 \in N$ ,  
 so  $\Psi(g_1^{-1}g_2) = e$   
 $\therefore \Psi(g_1^{-1})\Psi(g_2) = e$   
 $(\Psi(g_1))^{-1}\Psi(g_2) = e$   
 $\Psi(g_2) = \Psi(g_1) \checkmark$

② homomorphism

$$\eta((g_1N)(g_2N)) = \eta((g_1g_2)N)$$

$$= \Psi(g_1g_2)$$

$$= \Psi(g_1)\Psi(g_2)$$

$$= \eta(g_1N)\eta(g_2N) \checkmark$$

- ③ bijection
- if  $\eta(g_1N) = \eta(g_2N)$ ,  
 then  $\Psi(g_1) = \Psi(g_2)$   
 $\rightarrow \Psi(g_1^{-1}g_2) = e$   
 $\rightarrow g_1^{-1}g_2 \in N \rightarrow g_1N = g_2N \checkmark$
- Automatically surjective onto its image.  $\square$

Ex ① Let  $g \in G$  be an elt. of order  $n$ . Define  $\Psi: \mathbb{Z} \rightarrow G$   
 $k \mapsto g^k$ .

Then  $\text{Ker } \Psi = n\mathbb{Z}$ . F.I.T. gives an isomorphism  
 $\eta: \mathbb{Z}/n\mathbb{Z} \rightarrow \langle g \rangle \subseteq G$ .

Moreover,  $\psi = \eta \circ \phi$ , where  $\phi: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$   
 $k \mapsto k \pmod{n}$ .

② Consider  $\psi: \mathbb{R} \rightarrow SO_2(\mathbb{R})$

$$t \mapsto \begin{pmatrix} \cos(2\pi t) & -\sin(2\pi t) \\ \sin(2\pi t) & \cos(2\pi t) \end{pmatrix}.$$

$\ker \psi = \mathbb{Z}$ , so  $\psi$  factors through  $\phi: \mathbb{R} \rightarrow \mathbb{R}/\mathbb{Z}$ .

i.e., F.I.T. gives  $\eta: \mathbb{R}/\mathbb{Z} \rightarrow \psi(\mathbb{R}) \subseteq SO_2(\mathbb{R})$

OTOH, F.I.T. applied to  $\mathbb{R} \rightarrow S^1$  from above  
gives an isomorphism  $\mathbb{R}/\mathbb{Z} \rightarrow S^1$ .

Conclusion:  $\psi(\mathbb{R}) \cong S^1$   
 $\uparrow$  what is this?

Q. When we pass from  $G$  to  $G/N$ , what happens  
to the subgroups (normal or otherwise) of  $G$ ?

Ex. Consider  $N = SL_2(\mathbb{R})$  inside of  $G = GL_2(\mathbb{R})$ .

Another subgroup of  $G$  is

$$H = O(2) = \{A \in GL_2(\mathbb{R}) \mid A^T A = I\}.$$

Notice: •  $H \leq G$  is NOT a normal subgroup.

e.g., conjugating by  $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R})$

does not preserve  $O(2)$ .

•  $H$  does not contain  $N$  — plenty of matrices

with  $\det A = 1$  do not satisfy  $A^T A = I$ .

So what happens to  $H$  when we pass to the quotient  $G/N$ ?  
i.e., how do we squish  $N$  out of  $H$ ?