

Recall: A map  $\phi: G \rightarrow H$  is a homomorphism if

$$\begin{array}{ccc} G \times G & \xrightarrow{o_G} & G \\ \phi \times \phi \downarrow & \curvearrowright & \downarrow \phi \\ H \times H & \xrightarrow{o_H} & H \end{array}$$

Prop. If  $\phi: G \rightarrow H$  is a homomorphism, then

①  $\phi(e_G) = e_H$ ;

②  $\phi(g^{-1}) = (\phi(g))^{-1}, \forall g \in G$ ;

③ if  $K \leq G$ , then  $\phi(K) \leq H$ ;

④ if  $K \leq H$ , then  $\phi^{-1}(K) \leq G$ ;

⑤ if  $K \trianglelefteq H$ , then  $\phi^{-1}(K) \trianglelefteq G$ .

(Proof of ④ + ⑤.)

§  $K \leq H$ . We'll apply the subgroup criteria to  $\phi^{-1}(K) \leq G$ .

• Nonempty:  $\phi(e_G) = e_H \in K \Rightarrow e_G \in \phi^{-1}(K)$ .

• Pick  $g_1, g_2 \in \phi^{-1}(K)$ . Then  $\phi(g_1), \phi(g_2) \in K$ .

So

$$\phi(g_1 g_2^{-1}) = \phi(g_1) \phi(g_2^{-1}) = \phi(g_1) (\phi(g_2))^{-1} \in K,$$

and thus  $g_1 g_2^{-1} \in \phi^{-1}(K)$ .

Further §  $K \trianglelefteq H$ . i.e.,  $hKh^{-1} = K, \forall h \in H$ .

We NTS  $g\phi^{-1}(K)g^{-1} \subseteq \phi^{-1}(K), \forall g \in G$ .

Pick  $g' \in \phi^{-1}(K)$ . Then

$$\phi(g g' g^{-1}) = \phi(g) \phi(g') \phi(g^{-1}) \in \phi(g) K (\phi(g))^{-1} = K,$$

so  $g g' g^{-1} \in \phi^{-1}(K)$ . So  $g\phi^{-1}(K)g^{-1} = \phi^{-1}(K)$ . ▣

Def. Given a homomorphism  $\phi: G \rightarrow H$ , the Kernel of  $\phi$  is the subset  $\ker \phi := \phi^{-1}(e_H)$ .

Cor. The kernel of a homomorphism is a normal subgroup.  
(Proof.) Given  $\phi: G \rightarrow H$ ,  $\ker \phi = \phi^{-1}(\{e_H\})$  is the preimage of a normal subgroup of  $H$ .

Apply property ⑤. ▮

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

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

③  $\phi: \mathbb{R} \rightarrow S^1 \leq \mathbb{C}^*$  has  $\ker \phi = \mathbb{Z} \trianglelefteq \mathbb{R}$   
 $t \mapsto e^{2\pi i t}$

Prop. A homomorphism is injective iff its kernel is trivial.

(Proof.) Let  $\phi: G \rightarrow H$  be a homom.

§  $\phi$  is injective. Then

$$\ker \phi = \{g \in G \mid \phi(g) = e_H\}.$$

But  $\phi(g) = e_H$  iff  $\phi(g) = \phi(e_G)$  iff  $g = e_G$ .

So  $\ker \phi = \{e_G\}$ .

§  $\ker \phi = \{e_G\}$ . Pick  $g_1, g_2 \in G$  s.t.  $\phi(g_1) = \phi(g_2)$ .

Then  $\phi(g_1 g_2^{-1}) = \phi(g_1) (\phi(g_2))^{-1} = e_H$ , so

$g_1 g_2^{-1} \in \ker \phi. \therefore g_1 g_2^{-1} = e_G, \text{ so } g_1 = g_2.$  ▮

Ex.  $\nexists p, n \in \mathbb{N}$  have  $\gcd(p, n) = 1$ , with  $p$  prime.  
Then the only homom.  $\mathbb{Z}_p \rightarrow \mathbb{Z}_n$  is  $\phi(k) := 0$ .

If  $\phi: \mathbb{Z}_p \rightarrow \mathbb{Z}_n$  is any homom., then  $\text{Ker } \phi \trianglelefteq \mathbb{Z}_p$ , so  $\text{Ker } \phi = \{0\}$  or  $\text{Ker } \phi = \mathbb{Z}_p$ .

If  $\text{Ker } \phi = \{0\}$ , then  $\phi$  is injective, so  $\phi(\mathbb{Z}_p) \leq \mathbb{Z}_n$  of order  $p$ .

Since  $p \nmid n$ , this is impossible, so  $\text{Ker } \phi = \mathbb{Z}_p$ .

## The first isomorphism theorem

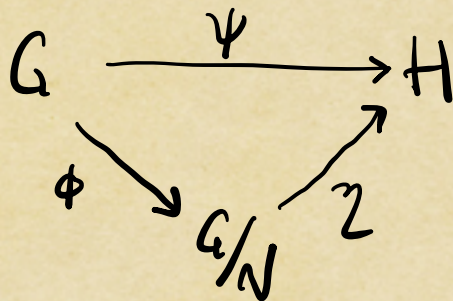
normal subgroups = "subgroups we can crush to be the identity"

kernels = "subgroups crushed to the identity by homomorphisms"

Now: normal subgroups = kernels

Def. Given  $N \trianglelefteq G$ , the canonical homomorphism  $\phi: G \rightarrow G/N$  is defined by  $\phi(g) := gN$ .

Thm. [First Isomorphism Theorem] Let  $\psi: G \rightarrow H$  be a homomorphism and let  $N = \text{Ker } \psi$ . Then there is a unique isomorphism  $\eta: G/N \rightarrow \psi(G)$  such that the following diagram commutes:



(Proof.) Given  $\Psi: G \rightarrow H$  and  $N = \text{Ker } \Psi$ , we

define  $\eta: G/N \rightarrow \Psi(G)$

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

NTS  $\eta$  is well-defined.

§  $g_1N = g_2N$ . Then  $g_1^{-1}g_2 \in N$ , so

$$e_H = \Psi(g_1^{-1}g_2) = (\Psi(g_1))^{-1}\Psi(g_2),$$

and therefore  $\Psi(g_1) = \Psi(g_2)$ .

$$\text{So } \eta(g_1N) = \eta(g_2N). \checkmark$$

$$\text{Homom: } \eta((g_1N)(g_2N)) = \eta((g_1g_2)N)$$

$$= \Psi(g_1g_2) = \Psi(g_1)\Psi(g_2)$$

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

$$\text{Inj: } \eta(g_1N) = \eta(g_2N) \Rightarrow \Psi(g_1) = \Psi(g_2)$$

$$\Rightarrow \Psi(g_1^{-1}g_2) = e_H$$

$$\Rightarrow g_1^{-1}g_2 \in N$$

$$\Rightarrow g_1N = g_2N. \checkmark$$

Surj: Every elt. of  $\Psi(G)$  has the form  $\Psi(g)$ .  $\checkmark$



$$\underline{\text{Ex.}} \quad \Psi: \mathbb{R} \rightarrow \text{SO}_2(\mathbb{R})$$

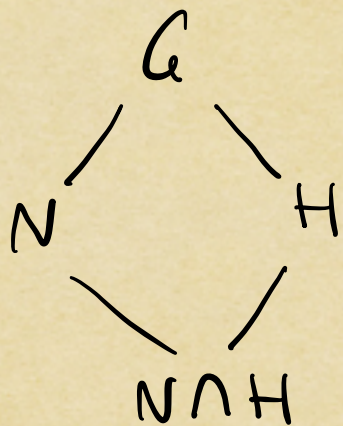
$$t \mapsto \begin{pmatrix} \cos(2\pi t) & -\sin(2\pi t) \\ \sin(2\pi t) & \cos(2\pi t) \end{pmatrix}$$

$$\text{Ker } \Psi = \mathbb{Z}$$

$$\text{F.I.T. : } \eta: \mathbb{R}/\mathbb{Z} \xrightarrow{\sim} \Psi(\mathbb{R})$$

Isomorphism theorems tell us about the structure of  $G/N$ .

What if we have  $N \trianglelefteq G$  and  $H \leq G$  with neither  $N \subseteq H$  nor  $H \subseteq N$ ?



What happens to  $H$  when we pass to  $G/N$ ?