Kernels and canonical homomorphisms

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

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

Prop. For any homom. $\phi: G \to H$, $\ker\phi$ is a normal subgroup of G.

(Proof.) $\{e\} \subsetneq H$ is normal. homomorphisms pull normal subgroups back to normal subgroups. ∎

Ex. ① $\phi: \mathbb{Z} \to \mathbb{Z}_n$ $\quad$ $\ker\phi = n\mathbb{Z}$

$$k \mapsto k \pmod{n}$$

② $\phi: GL_n(\mathbb{R}) \to \mathbb{R}^*$ $\quad$ $\ker\phi = SL_n(\mathbb{R})$

$$A \mapsto \det A$$

③ $\phi: \mathbb{R} \to S^1 \subsetneq \mathbb{C}$ $\quad$ $\ker\phi = \mathbb{Z}$

$$t \mapsto \exp(2\pi i t)$$

Prop. A homom. $\phi: G \to H$ 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

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

$\ker\phi \le \mathbb{Z}_p$ 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 ϕ is injective.

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

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

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

The isomorphism theorems

$$\left\{ \begin{array}{c} \text{homomorphisms} \\ \text{out of } G \end{array} \right\} \underset{\phi_N \,\leftarrow\!\shortmid\, N}{\overset{\phi \,\mapsto\, \ker\phi}{\rightleftarrows}} \left\{ \begin{array}{c} \text{normal subgroups} \\ \text{of } G \end{array} \right\}$$

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

__Exercise.__ Verify that $\phi : G \to G/N$ is a homom. with

$$\ker \phi = N.$$

The first isomorphism theorem

Let $\psi : G \to H$ be any homom. of groups, and let $N = \ker \psi$. Then there is a unique isomorphism $\eta : G/N \to \psi(G)$ for which the diagram

$$\begin{tikzcd} G \arrow[rr, "\psi"] \arrow[dr, "\phi"'] & & H \\ & G/N \arrow[ur, "\eta"'] & \end{tikzcd}$$

commutes, where ϕ is the canonical homom.

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

$$\begin{tikzcd} G \arrow[r, "\psi"] \arrow[dr, "\phi"'] & H \\ & G/N \arrow[u, dashed, "\exists!"'] \end{tikzcd}$$

"ψ factors through G/N"

(Proof.) Given $\psi : G \to H$ as described, define

$$\begin{aligned} \eta : G/N &\to \psi(G) \subseteq H \\ gN &\mapsto \psi(g). \end{aligned}$$

NTS: ① well-defined
② homomorphism
③ bijection

① <u>Well-defined</u>

if $g_1N = g_2N$, then $g_1^{-1}g_2 \in N$,

so $\psi(g_1^{-1}g_2) = e$

$\therefore \psi(g_1^{-1})\psi(g_2) = e$

$(\psi(g_1))^{-1}\psi(g_2) = e$

$\psi(g_2) = \psi(g_1)$ ✓

② <u>homomorphism</u>

$$\begin{aligned} \eta((g_1N)(g_2N)) &= \eta((g_1g_2)N) \\ &= \psi(g_1g_2) \\ &= \psi(g_1)\psi(g_2) \\ &= \eta(g_1N)\eta(g_2N) \checkmark \end{aligned}$$

③ <u>bijective</u>

if $\eta(g_1N) = \eta(g_2N)$,

then $\psi(g_1) = \psi(g_2)$

$\to \psi(g_1^{-1}g_2) = e$

$\to g_1^{-1}g_2 \in N \to g_1N = g_2N$ ✓

Automatically surjective onto its image. ∎

<u>Ex</u> ① Let $g \in G$ be an elt. of order n. Define $\psi : \mathbb{Z} \to G$, $k \mapsto g^k$.

Then $\ker\psi = n\mathbb{Z}$. F.I.T. gives an isomorphism

$$\eta : \mathbb{Z}/n\mathbb{Z} \to \langle g \rangle \subseteq G.$$

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

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

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

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

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

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

Conclusion: $\underbrace{\psi(\mathbb{R})}_{\text{what is this?}} \cong S^1$.

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?