# Abstract Algebra Notes Day 9 Tue, Nov 4, 2025
# & Day 10 Tue, Nov 18, 2025

---

Recall ...

> **Prop:** Let $G$ be a group, and $a, b \in G$.
>
> The equation $ax = b$ has a unique solution in $G$.
>
> The equation $xa = b$ has a unique solution in $G$.
>
> This is why the Cayley table is like sudoku

> Recall Lemma for cosets: (Ch 7 pg 139)
>
> $a \in bH$ iff $aH = bH$ iff $a^{-1}b \in H$

> TFAE:
>
> (1) $gN = Ng$ for all $g \in G$ (def of $N \trianglelefteq G$)
> (all left cosets are right cosets)
>
> (2) $gng^{-1} \in N$ for all $g \in G$ and $n \in N$
>
> (closed under conjugation)

# Ch 10 Group homomorphism

**Prop 1** (Thm 10.2 part 8 on pg 197) Let $f: G \to H$ be a group homomorphism.

If $J \trianglelefteq H$, (J is a normal subgroup of H)

then the preimage / inverse image / pullback of $J$

$$f^{-1}(J) \overset{\text{def}}{=} \{ g \in G : f(g) \in J \}$$

is a normal subgroup of $G$.

**Proof** First, check the three conditions for being a subgroup (Exercise)

To prove that $f^{-1}(J)$ is normal in $G$,

we will show that $gxg^{-1} \in f^{-1}(J)$ for all $x \in f^{-1}(J)$ and $g \in G$:

Let $g \in G$ and $x \in f^{-1}(J)$. Then $f(x) \in J$ by def of preimage.

$$\begin{aligned} \text{So } f(gxg^{-1}) &= f(g)\, f(x)\, f(g^{-1}) \quad \text{since } f \text{ is a homomorphism} \\ &= f(g)\, f(x)\, [f(g)]^{-1} \\ &\in J \end{aligned}$$

since $f(g), [f(g)]^{-1} \in H$ and $f(x) \in J$ and $J$ is normal in $H$.

By def of preimage, $f(gxg^{-1}) \in J$ means $gxg^{-1} \in f^{-1}(J)$.

So $f^{-1}(J) \trianglelefteq G$ □

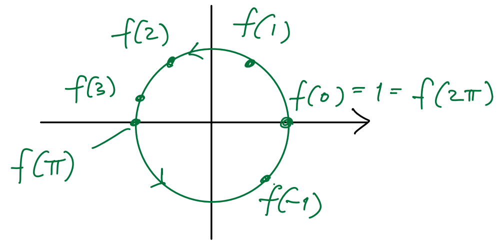
**Cor 2** (Cor pg 198) The kernel of a group homomorphism $f: G \to H$ is a normal subgroup of $G$.

**Proof** $\{e_H\}$ is a normal subgroup of $H$, so by above $\ker f \overset{\text{def}}{=} f^{-1}(\{e_H\})$ is a normal subgroup of $G$.

Ex (Ex 15 pg 202) Consider the "wrapping function"

$$f:(\mathbb{R},+) \longrightarrow (\mathbb{C}^*,\cdot)$$

$$f(\theta) = \cos\theta + i\sin\theta \text{ or } e^{i\theta}$$




This is a homomorphism because

$$f(x+y) = e^{i(x+y)} = e^{ix}e^{iy} = f(x)f(y)$$

Since $f(\theta)=1$ iff $\cos\theta = 1$ iff $\theta$ is an integer multiple of $2\pi$,

$$\ker f = \{2\pi n : n \in \mathbb{Z}\}$$

Note ker $f$ is a cyclic subgroup of $(\mathbb{R},+)$ generated by $2\pi$:

$$\cdots \longrightarrow -4\pi \xrightarrow{+2\pi} -2\pi \xrightarrow{+2\pi} 0 \xrightarrow{+2\pi} 2\pi \xrightarrow{+2\pi} 4\pi \xrightarrow{+2\pi} \cdots$$

$\operatorname{Im} f = \{e^{i\theta} : \theta \in \mathbb{R}\} = \{$ complex numbers w/ magnitude 1 $\}$

(See Day 4 notes) $= \mathbb{T}$, "the circle group"

---

Lemma 3 Let $f: G \to H$ be a group homomorphism, and $a,b \in G$.

$$f(a) = f(b) \text{ iff } \underbrace{a\ker f}_{\text{the coset of }\ker f\text{ containing }a} = \underbrace{b\ker f}_{\text{the coset of }\ker f\text{ containing }b}$$

Proof (Forward direction ($\Rightarrow$)) Suppose $f(b) = f(a)$.

By "Sudoku prop", there exists a unique $c \in G$ such that $b = ac$.

Then $f(b) = f(ac) = f(a)f(c) = f(b)f(c)$.

So $f(c) = e_H$ and $c \in \ker f$. Thus, $b = ac \in a\ker f$.

So $b\ker f = a\ker f$.

(Backward direction ($\Leftarrow$))

Suppose $a\ker f = b\ker f$. Then $b \in a\ker f$.

Then $b = ak$ where $k \in \ker f$ (that is, $f(k) = e_H$).

So $f(b) = f(ak) = f(a)f(k) = f(a)e_H = f(a)$. $\square$

**Lemma 4** Let $f: G \to H$ be a group homomorphism, and $a \in G$.

If $f(a) = y$, then $f^{-1}(\{y\}) \overset{\text{def}}{=} \{x \in G : f(x) = y\}$ is equal to

$a \operatorname{Ker} f$,

the coset of $\operatorname{Ker} f$ containing $a$.

**Proof** (First, prove $f^{-1}(\{y\}) \subset a \operatorname{Ker} f$)

Let $b \in f^{-1}(\{y\})$. Then $f(b) = y = f(a)$.

By Lemma 3, $b \operatorname{Ker} f = a \operatorname{ker} f$.
$(\Rightarrow)$

Thus, $b \in a \operatorname{Ker} f$.

(Second, prove $f^{-1}(\{y\}) \supset a \operatorname{Ker} f$)

Let $k \in \operatorname{Ker} f$. Then $f(ak) = f(a) f(k) = y e_H = y$.

So, by def, $ak \in f^{-1}(\{y\})$. $\square$

**Def** A function $f: G \to H$ is called a <u>$t$-to-1 function</u>

if the cardinality of $f^{-1}(\{y\})$ is $t$ for all $y \in f(G)$

**Note**: A <u>one-to-one</u> function is injective

**Prop 5** Let $f: G \to H$ be a group homomorphism, where $|\operatorname{Ker} f| = t$.

Then $f$ is a $t$-to-1 mapping.

**Pf** Let $y \in f(G) \overset{\text{def}}{=} \{f(x) : x \in G\}$, meaning $y = f(a)$ for some $a \in G$.

Then $f^{-1}(\{y\}) = \underbrace{a \operatorname{Ker} f}$

the coset of $\operatorname{Ker} f$ in $G$ containing $a$

Since $f^{-1}(\{y\})$ is a coset of $\operatorname{Ker} f$, $f^{-1}(\{y\})$

has the same cardinality as $\operatorname{Ker} f$. $\square$

<u>Ex</u> Let $f: \mathbb{C}^* \to \mathbb{C}^*$

$$f(z) = x^4$$

$\ker f = \{z : z^4 = 1\} = \{1, i, -1, -i\}$.

By above Prop, we know $f$ is a 4-to-1 mapping.

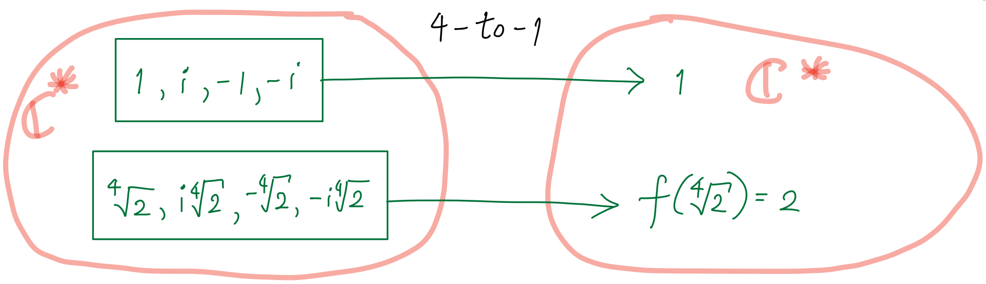
For example, let's find the pullback / fiber of 2, $f^{-1}(\{2\})$, all elements that are sent to 2.

We know $f(\sqrt[4]{2}) = 2$. So by above lemma,

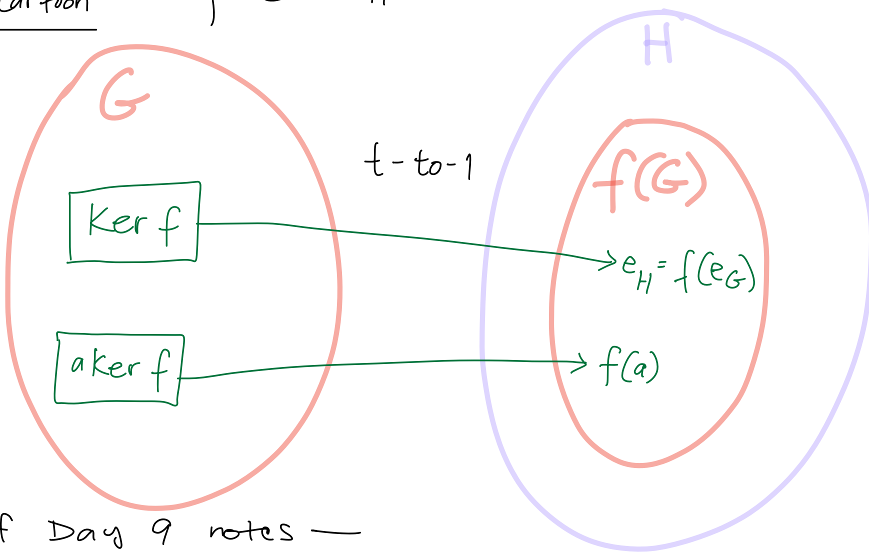
$$f^{-1}(\{2\}) = \sqrt[4]{2}\,\ker f = \{\sqrt[4]{2},\ i\sqrt[4]{2},\ -\sqrt[4]{2},\ -i\sqrt[4]{2}\},$$ and

this set is the coset of $\ker f$ containing $\sqrt[4]{2}$. □

<u>Cartoon</u>




<u>General cartoon</u> $f: G \to H$




— end of Day 9 notes —

— Start of Day 10 notes —

Def Given a normal subgroup $N \trianglelefteq G$,

the natural or canonical map

$$\pi : G \to G/N$$

is defined by

$$\pi(g) = gN$$

Facts. The natural mapping $\pi$ is a homomorphism:

$$\pi(g_1 g_2) = g_1 g_2 N = (g_1 N)(g_2 N) = \pi(g_1)\,\pi(g_2)$$

because $N$ is normal, coset multiplication is well-defined

• The kernel of $\pi$ is $N$

(Note This means every normal subgroup of $G$ is the kernel of a homomorphism from $G$)

• $\pi$ is surjective:

Each elt in the codomain $G/N$ is of the form

$$gN = \pi(g)$$

$\boxed{\text{1st Isomorphism Thm}}$ (or "Fundamental Thm of Group homomorphism")

Thm 10.3 (Jordan, 1870)

- 1st Iso Thm:
  Let $f: G \to H$ is a group homomorphism with $K = \ker f$
  Note that we've proven that $\ker f \triangleleft G$, so $G/K = \{xK \mid x \in G\}$ is a group (called quotient group).
- Let $i: G/K \longrightarrow H$ be defined by
  $gK \longmapsto f(g)$ for all $gK \in G/K$.

  Then $i$ is an injection $G/K \hookrightarrow H$.

  In particular, we have an isomorphism given by $i$

  $$G/K \xrightarrow{\cong} \operatorname{Im} f$$

---

1. Prove that $i$ is well-defined (that def of $i$ depends only on the coset):

   We need to show that if $aK = bK$ then $i(aK) = i(bK)$.

   Suppose $aK = bK$.

   By Lemma 3, $f(a) = f(b)$,
   $(\Leftarrow)$

   so $i(aK) = i(bK)$. $\boxed{1}$

2. Prove that $i$ is injective:
   We need to show that $i(aK) = i(bK)$ implies $aK = bK$.

   Suppose $i(bK) = i(aK)$.

   Then $f(b) = f(a)$ by def of $i$

   Then $aK = bK$ (by Lemma 3 $(\Rightarrow)$) $\boxed{2}$

3. Prove that $i$ is a homomorphism:
   We need to show that $i(aK \cdot bK) = i(aK)\, i(bK)$.
   Recall from the def of quotient groups that $aK \cdot bK \overset{\text{def}}{=} abK$.

   $i(aK \cdot bK) = i(ab\,K)$ by def of the binary operation of $G/K$.

   $= f(ab)$ by def of $i$

   $= f(a)\, f(b)$ since $f$ is a homomorphism

   $= i(aK)\, i(bK)$ by def of $i$. $\boxed{3}$

4. Prove that $i : G/K \longrightarrow f(G)$ is surjective:

We need to show that for each $h \in \overbrace{\mathrm{Im}(f)}^{\text{codomain}}$, there is $gK \in \overbrace{G/K}^{\text{domain}}$ with $i(gK) = h$.

Let $y \in \mathrm{Im}(f)$. By def, $\mathrm{Im}(f) = \{ f(g) \mid g \in G \}$, so there is $x \in G$ with $f(x) = y$

Then $i(xK) = f(x) = y$. $\boxed{4}$

<u>Note</u> (Con't of 1st Isomorphism Thm)

Let $f : G \longrightarrow H$ be a group homomorphism, and set $K = \ker f$. Then

the isomorphism $G/\ker f \cong f(G)$

$f = i \circ \underbrace{\pi}_{}$
the natural onto homomorphism $G \longrightarrow G/\ker f$

because
$$\begin{array}{ccc} G & \xrightarrow{f} & f(G) \\ x & \longmapsto & f(x) \end{array}$$
and
$$\begin{array}{ccccc} G & \xrightarrow{\pi} & G/K & \xrightarrow{i} & f(G) \\ x & \longmapsto & xK & \longmapsto & f(x) \end{array}$$

The diagram
$$\begin{tikzcd} G \arrow[r, "\pi"] \arrow[dr, "f"'] & G/K \arrow[d, dashed, "i"] \\ & f(G) \end{tikzcd}$$
, called a "commutative diagram" illustrates the 1st isomorphism Thm.

We say "the diagram commutes" to mean $f = i \circ \pi$.

<u>Note</u> This tells us that every group homomorphism can be written as a composition

(1-1 homomorphism) $\circ$ (onto homomorphism).

## Applications of the 1st Isomorphism Thm

**Example 1** Prove that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

**Proof** Recall that $\mathbb{Z}_n \overset{\text{def}}{:=} \{0, 1, 2, 3, \ldots, n-1\}$

$$n\mathbb{Z} \overset{\text{def}}{:=} \{\text{integer multiples of } n\}$$
$$= \{nz : z \in \mathbb{Z}\}$$
$$= \{\ldots, -n, 0, n, 2n, 3n, \ldots\}$$

Define $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$

by $z \longmapsto z \pmod{n}$

Let $K \overset{\text{def}}{:=} \ker f = \{\text{integer multiples of } n\} = n\mathbb{Z}$.

The elements of $\underbrace{\mathbb{Z}/K = \mathbb{Z}/n\mathbb{Z}}_{\text{quotient group}}$ are the cosets

$0 + n\mathbb{Z}$, $1 + n\mathbb{Z}$, $2 + n\mathbb{Z}$, ...., $n+1 + n\mathbb{Z}$
$K$, $1 + K$, $2 + K$, ..., $n+1 + K$

By the 1st Isomorphism Thm, $\mathbb{Z}/n\mathbb{Z} \cong \operatorname{Im}(f)$.

But $\operatorname{Im}(f) = \mathbb{Z}_n$, so $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

**Example 2** (back to the wrapping function)

Consider $f : (\mathbb{R}, +) \longrightarrow (\mathbb{C}^*, \cdot)$
$f(\theta) = \cos\theta + i\sin\theta$ or $e^{i\theta}$

with $\ker f = \langle 2\pi \rangle$.

By the 1st iso thm, $\mathbb{R}/\langle 2\pi \rangle \cong \underbrace{\mathbb{T}}_{\text{the circle group}}$

## Example 3 (Extra notes)

Let $G$ be a cyclic group w/ generator $g$.

Define a map $f: \mathbb{Z} \to G$ by

$$n \mapsto g^n$$

Then $f$ is a homomorphism since

$$f(m+n) = g^{m+n} = g^m g^n = f(m) f(n).$$

$f$ is surjective because by def $G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$.

If $|g| = m$, then $g^m = e$ and $\ker f = m\mathbb{Z}$

and $$\mathbb{Z}/\ker f = \mathbb{Z}/m\mathbb{Z} \underset{\substack{\uparrow \\ \text{by the 1st iso thm}}}{\cong} f(\mathbb{Z}) = G$$

If the order of $g$ is infinite,

then $\ker f = \{0\}$ and

$$\mathbb{Z}/\ker f = \mathbb{Z} \underset{\substack{\uparrow \\ \text{again by the 1st iso thm.}}}{\cong} f(\mathbb{Z}) = G \quad \square$$