Last updated: Oct 30, 2024

Abstract Algebra Notes Week 9 Wed, Oct 30 2024

Proposition 3.21 *Let G be a group and a and b be any two elements in G. Then the equations $ax = b$ and $xa = b$ have unique solutions in G.*

This is why the Cayley table is like sudoku

To prove that a subset $K \subseteq G$ is a subgroup, prove:

(1) The identity of G is in K

(2) For all $a, b \in K$, $ab \in K$

(K is closed under the group operation)

(3) For all $a \in K$, $a^{-1} \in K$

(K is closed under taking inverses)

Recall Lemma for cosets:

$a \in bH$ iff $aH = bH$ iff $a^{-1}b \in H$

(Lemma 6.3)

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)

(3) $gNg^{-1} = N$

(only one conjugate subgroup)

Prop 1 Let $f: G \to H$ be a group homomorphism.
(Prop 11.4) part 4

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

then the preimage / inverse image / pullback of H′

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

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 $x = f^{-1}(J)$. Then $f(x) \in J$ by def of preimage.

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

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 The kernel of a group homomorphism $f: G \to H$
(Thm 11.5) is a normal subgroup of G.

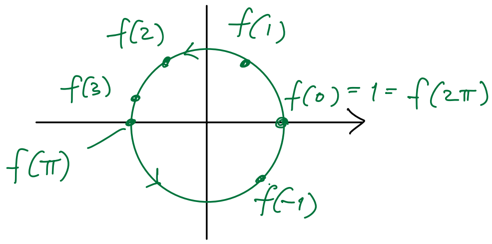
Proof $\{e_H\}$ is a normal subgroup of H, so by above
$\ker f \overset{\text{def}}{=} f^{-1}(\{e_H\})$ is a normal subgroup of G.

Alternate proof See week 8 Practice Problem 4 Solutions

Ex (Ex 11.7) Consider the "wrapping function"

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

$f(\theta) = \cos\theta + i \sin\theta$ 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 θ is an integer multiple of 2π,

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

Note Observe that this is a cyclic subgroup of $(\mathbb{R}, +)$ generated by 2π:

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

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

$= \mathbb{T}$, "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 Prop 3.21, 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 $\underset{(\Rightarrow)}{\text{Lemma}}$ 3, $b \operatorname{Ker} f = a \operatorname{ker} f$.

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 $\operatorname{Ker} f$. $\square$

Ex Let $f: \mathbb{C}^* \to \mathbb{C}^*$

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

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

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

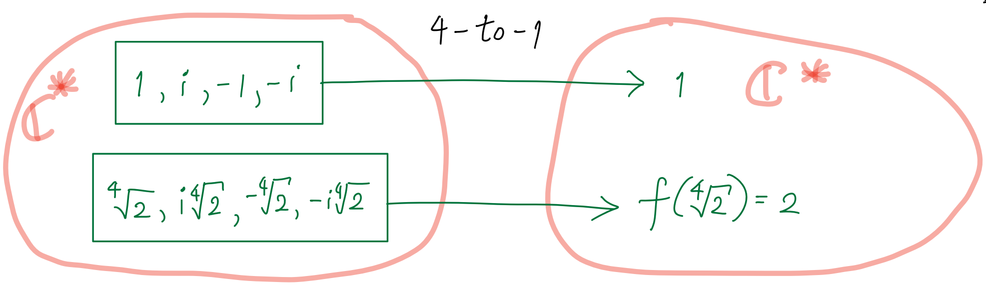
For example, let's find the pullback / fiber of 2, $f^{-1}(\{2\})$, all elements that are sent to 2.

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

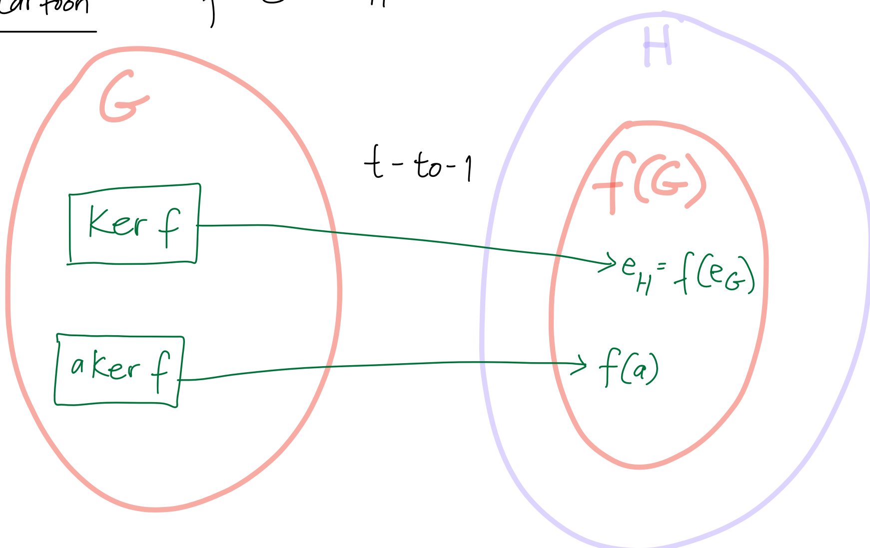
$$f^{-1}(\{2\}) = \sqrt[4]{2}\ \ker f = \{\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}\},$$ and

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

Cartoon



General cartoon $f: G \to H$



Def Given a normal subgroup $N \trianglelefteq G$, the natural or canonical map

$$\pi : G \longrightarrow G/N$$

is defined by

$$\pi(g) = gN$$

Facts. The natural mapping π is a homomorphism:

$$\pi(g_1 g_2) = g_1 g_2 N \underset{|}{=} (g_1 N)(g_2 N) = \pi(g_1)\,\pi(g_2)$$

because N is normal, coset multiplication is well-defined

- The kernel of π is N

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

- π is surjective:

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

$$gN = \pi(g)$$

1st Isomorphism Thm (Thm 11.10)

- 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 $aK \cdot bK \overset{def}{=} abK$.

   $i(aK \cdot bK) = i(abK)$ 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 $G/\ker f \cong f(G)$

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

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 $\mathbb{Z}_n \overset{\text{def}}{:=} \{0, 1, 2, 3, \dots, n-1\}$

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

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

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

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

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

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,

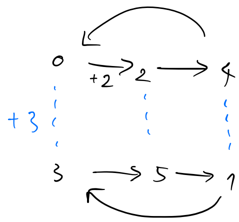
then $\ker f = \{0\}$ and

$$\mathbb{Z}/\ker f = \mathbb{Z} \underset{\uparrow}{\cong} f(\mathbb{Z}) = G$$

again by the 1st iso thm. $\square$

Finite & finitely generated abelian groups (Sec 13.1)

Recall: $\mathbb{Z}_6 \cong \mathbb{Z}_3 \times \mathbb{Z}_2$ but $\mathbb{Z}_8 \not\cong \mathbb{Z}_2 \times \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$



because $\mathbb{Z}_8$ has an elt of order 8, the number 1, but every elt x in $\mathbb{Z}_2 \times \mathbb{Z}_4$ & $(\mathbb{Z}_2)^3$ satisfies $x^4 = 0$.

Prop 1 (a) If $\gcd(n, m) = 1$ then $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$

Pf Suppose $\gcd(n, m) = 1$.

Claim: $(1,1) \in \mathbb{Z}_n \times \mathbb{Z}_m$ has order nm.

Let k be the order of $(1,1) \in \mathbb{Z}_n \times \mathbb{Z}_m$
Then $\underbrace{(1,1) + (1,1) + \cdots + (1,1)}_{k} = (k,k) = 0$

This means n divides k and m divides k.
So $k = \operatorname{lcm}(n, m)$.
But since $\gcd(n,m) = 1$, $\operatorname{lcm}(n,m) = nm$.

Since we know (from def of direct products) that the order of $\mathbb{Z}_n \times \mathbb{Z}_m$ is nm,

$\langle (1,1) \rangle$ must generate $\mathbb{Z}_n \times \mathbb{Z}_m$.

So $\mathbb{Z}_n \times \mathbb{Z}_m$ is a cyclic group of order nm, thus it is isomorphic to $\mathbb{Z}_{nm}$.

Prop 1(b) If $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$ then $\gcd(n,m) = 1$

Pf Suppose $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$.

Then $\mathbb{Z}_n \times \mathbb{Z}_m$ has an elt (a,b) of order nm $\}$ $(*)$
(Since $1 \in \mathbb{Z}_{nm}$ has order nm).

For convenience, switch to "multiplicative notation".

Let C_n denote a cyclic group of order n, and
let C_m denote a cyclic group of order m.

Let e_1 and e_2 denote the identities of C_n and C_m, resp.

Let $a \in C_n$ and $b \in C_m$ such that
$C_n = \langle a \rangle$ and $C_m = \langle b \rangle$

Then $a^n = e_1$ and if $0 < j < n$ then $a^j \neq e_1$

$b^m = e_2$ and if $0 < j < m$ then $b^j \neq e_2$

Then the order of (a,b) must be the smallest
multiple of n and of m, $\operatorname{lcm}(n,m)$.

Since (a,b) has order nm (from $(*)$),
$\operatorname{lcm}(n,m) = nm$. So the greatest common
divisor of n and m is 1. $\square$

Classification Thm of Finite Abelian Groups

Every finite abelian group A is isomorphic to a direct product of cyclic groups. i.e.

$$A \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_j}$$

where each n_i is a prime power, i.e. $n_i = p_i^{d_i}$ where p_i is prime, $d_i \in \mathbb{Z}_{>0}$

Ex Up to isomorphism, there are 6 abelian groups of order $200 = 2^3 \cdot 5^2$

$= 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5$

	By Prime powers		By divisors (Applying Prop 1)
$\mathbb{Z}_{200} \underset{\text{by Prop 1}}{\cong}$	$\mathbb{Z}_8 \times \mathbb{Z}_{25}$	$222 \mid 55$	$\mathbb{Z}_{200}$
	$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{25}$	$2 \mid 22 \mid 55$	$\mathbb{Z}_{100} \times \mathbb{Z}_2$
	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$	$2 \mid 2 \mid 2 \mid 55$	$\mathbb{Z}_{50} \times \mathbb{Z}_2 \times \mathbb{Z}_2$
$\mathbb{Z}_{40} \times \mathbb{Z}_5 \cong$	$\mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_5$	$222 \mid 5 \mid 5$	$\mathbb{Z}_{40} \times \mathbb{Z}_5$
	$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5$	$2 \mid 22 \mid 5 \mid 5$	$\mathbb{Z}_{20} \times \mathbb{Z}_{10}$
	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$	$2 \mid 2 \mid 2 \mid 5 \mid 5$	$\mathbb{Z}_{10} \times \mathbb{Z}_{10} \times \mathbb{Z}_2$

Classification of finitely generated abelian group

Every finitely generated abelian group A is isomorphic to a direct product of cyclic groups, i.e

$$A \cong \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}} \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_j}$$

Non abelian groups are much more mysterious