Math 128A, Wed Nov 04

Class meets Mon Nov 9, but NOT on Wed Nov 11 (Veterans Day).

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, please turn off your camera and mute yourself.
- Exception: When we do groupwork, please turn both your camera and mic on. (Groupwork will not be recorded.)
- Please always have the chat window open to ask questions.
- Reading for today and Mon: Ch. 11. ← end of group theory!
- PS08 due today; PS09 outline due Mon.
- Problem session, Fri Nov 06, 10:00–noon on Zoom.

#8 cut

PS08 & 09

Recap of homomorphisms

Definition

$G, \overline{G}$ groups. To say that $\varphi : G \to \overline{G}$ is a **homomorphism** means that for all $a, b \in G$,

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Definition

If $\varphi : G \to \overline{G}$ is a homomorphism, we define the **kernel** of φ to be

$$\ker \varphi = \{a \in G \mid \varphi(a) = \overline{e}\},$$

where $\overline{e}$ is the identity in $\overline{G}$.

$\ker \varphi \lhd G$

"By their kernels shall ye know them"

The First Isomorphism Theorem

$\boxed{1IT}$

(Phi' Φ)

$\varphi : G \to \overline{G}$ $T = \ker\varphi$

$G/T \approx \varphi(G)$ $\varphi(G) \approx G/\ker\varphi$

In fact, we've already seen most of this: Define
$\Phi : (G/\ker\varphi) \to \varphi(G)$ by Φ

$$\Phi(a\ker\varphi) = \varphi(a).$$

two inputs give same output <=> same coset of kernel

- Since $\varphi(a) = \varphi(b)$ if and only if $a\ker\varphi = b\ker\varphi$, we see that Φ is well-defined (if) and one-to-one (only if).
- Φ is a homomorphism because φ is.

Example: G/Z Theorem (from Ch. 9)

Recall: $\mathrm{Inn}(G)$ is the group of all automorphisms of G of the form

Ch. 6

$$\varphi_a(x) = axa^{-1}, \quad (a \in G)$$

$\mathrm{Inn}(G) = \{\varphi_a\} \leq \mathrm{Aut}(G)$

the group of **inner automorphisms** of G.

Theorem

$G/Z(G) \approx \mathrm{Inn}(G)$.

$Z(G) = \{z \in G \mid zx = xz \ \forall x \in G\}$

THE METHOD:

1. Define a homomorphism $\Phi : G \to \mathrm{Inn}(G)$. (And check that Φ is a homomorphism!)
2. Calculate $\ker \Phi$. & $\Phi(G)$
3. Apply 1st IT: BAZINGA $\mathrm{Inn}(G) \approx G/\ker\Phi$

Review of Aut(G)

Aut(G) = { all isomorphisms f : G -> G }, with operation of composition.

So fg = $f \circ g$, where $f \circ g(x) = f(g(x))$

$(a \in G)$

The inner automorphism $\varphi_a : G \to G$ is:

$$\varphi_a(x) = axa^{-1}$$

Inn(G) = {all inner automorphisms of G}, which is a subgroup of Aut(G).

Because we look at Inn(G) as a subgroup of Aut(G), the operation in Inn(G) is composition because composition is the operation in Aut(G).

1. Def $\Phi : G \to \mathrm{Inn}(G)$

$\Phi(a) = \varphi_a$

$\left(\begin{array}{l} \varphi_a : G \to G \\ \varphi_a(x) = axa^{-1} \end{array} \right)$

Check Φ homom:

A $a, b \in G$

LHS: $\Phi(ab) = \varphi_{ab}$; $\varphi_{ab}(x) = (ab)x(ab)^{-1}$

RHS: $\Phi(a)\Phi(b) = \varphi_a \varphi_b = \varphi_a \circ \varphi_b$

$\varphi_a \circ \varphi_b(x) = \varphi_a(\varphi_b(x))$

$= \varphi_a(bxb^{-1})$

$$= a \underbrace{b x b^{-1} a^{-1}}_{} \quad \text{S\&S}$$

$$= (ab)\, x\, (ab)^{-1} = \varphi_{ab}(x)$$

So $\varphi_a \varphi_b = \varphi_{ab}$

Ⓒ $\Phi(ab) = \Phi(a)\Phi(b)$.

2. $\Phi(G) = \{\Phi(a) \mid a \in G\}$ defn image

$= \{\varphi_a \mid a \in G\}$ defn Φ

$= \mathrm{Inn}(G)$ defn $\mathrm{Inn}(G)$

$$\ker \Phi = \{a \in G \mid \varphi_a = id\}$$

Recall: Two functions are equal <=> they produce same output for any input.

$$\varphi_a = id \iff \forall x \in G \; \varphi_a(x) = id(x)$$

$$\iff \forall x \in G,\ \varphi_a(x) = x$$

defn φ_a

$$\iff \forall x \in G,\ axa^{-1} = x$$

$\cdot a$ on R

$$\iff \forall x \in G,\ ax = xa$$

$$\iff a \in Z(G) \quad \text{So } \ker \Phi = Z(G)$$

---

3. By 1IT, $\Phi(G) \simeq G/\ker\Phi \simeq G/Z(G)$

$$\Rightarrow \text{Inn}(G) \simeq G/Z(G)$$

☺

Note: The First Isomorphism Theorem is a particularly useful kind of result, in that it only proves facts for you, it also tells you what to prove.

That is: 1IT tells you that whenever you have a homomorphism, you should:

* Figure out what the image is; and
* Figure out what the kernel is.

And then 1IT tells you that the image is isomorphic to G/kernel.

Example: Internal direct products

Definition

To say that G is the **internal direct product** of H and K means:

- $H \lhd G$ and $K \lhd G$;
- $G = HK$; and
- $H \cap K = \{e\}$.

Theorem

If G is the internal direct product of H and K, then $G \approx H \oplus K$.

Proof: See PS09.

Normal subgroups are kernels

We saw that every kernel is a normal subgroup. Conversely, every normal subgroup is the kernel of some homomorphism:

Theorem

For $N \lhd G$, the map $\varphi : G \to (G/N)$ given by

$$\varphi(a) = aN$$

is a homomorphism with kernel N.

Proof isn't that interesting; point is more that normal subgroups and homomorphisms are really two different ways of looking at the same phenomenon.

__PS08#5__ $G = \mathbb{Z}_{125} \oplus \mathbb{Z}_5$

$\boxed{\text{Op'n} \; +}$

$H = \langle (\underbrace{5}_{\in \mathbb{Z}_{125}}, \underbrace{1}_{\in \mathbb{Z}_5}) \rangle$

$= \{(0,0), (5,1), (10,2), (15,3), (20,4), (25,0), \ldots\}$

mult gp: $\langle a \rangle = \{a^n\}$

$+$ gp: $\langle a \rangle = \{na\}$

Elts of G/H are cosets $a + H$.

$$(5,0)+H=\{(5,0),(10,1),(15,2),\ldots\}$$

$$+\ (7,2)+H=\{(7,2),(12,3),(17,4),\ldots\}$$

$$(12,3)+H=(17,4)+H$$

$$(12,2)+H=\{(12,2),(17,3),(22,4),\ldots\}$$

by defn

To find the order of (5,0)+H: Add (5,0)+H to itself until you get the identity, where the identity of G/H is (0,0)+H = H.

(Though note: (20,4)+H = H, since (20,4) is in H. More generally, for any h in H, h+H = H.)

Note: When we talk about the order of (5,0)+H as an element of G/H, this is different from the size of (5,0)+H as a subset of G.

Wayback machine: The Fundamental Theorem of Arithmetic

$$60 = 2 \cdot 2 \cdot 3 \cdot 5$$

Theorem

Let $n > 1$ be a positive integer.

1. *n is equal to a product of primes:*

$$n = p_1 p_2 \dots p_k.$$

2. *This product is unique, assuming $p_1 \leq p_2 \leq \dots \leq p_k$.*

Note that as a consquence, two numbers with different prime factorizations cannot be equal.

The Fundamental Theorem of Finite Abelian Groups

Theorem

Let G be a finite abelian group. $|G|>1$

1. *G is isomorphic to an external direct product of cyclic groups of prime power order:*

$$G \approx \mathbf{Z}_{p_1^{n_1}} \oplus \mathbf{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbf{Z}_{p_k^{n_k}}$$

2. *This product is unique, assuming that (a) $p_1 \leq p_2 \leq \cdots \leq p_k$ and (b) if $p_i = p_{i+1}$, then $n_i \leq n_{i+1}$. (I.e., parts corresponding to each prime appear in increasing order by prime, and prime powers appear in increasing order by prime.)*

Note that as a consquence, two finite abelian groups with different decompositions into external direct products of cyclic groups of prime power order cannot be isomorphic.

(Ch. 8)

<u>Ex</u> $\mathbb{Z}_{60} \approx \mathbb{Z}_{2^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$ is ab, ord 60

FT says! Not isomorphic.

Example: Classify finite abelian groups of order $7^3 11^4$