Math 128A, Mon Nov 02

- 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: Ch. 10. Reading for Wed: Ch. 11.
- PS08 outline due today, full version due Wed.
- Problem session, Fri Nov 06, 10:00–noon on Zoom.

Remember: Next week, we meet on Mon Nov 09 only.
(Wed Nov 11 is Veterans Day.)

Recap of homomorphisms

Definition

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

op in G

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

op in $\overline{G}$

(replace * with + as appropriate)

Definition

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

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

"By their kernels shall ye know them"

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

We also saw that homomorphisms preserve or reduce a lot of element structure, e.g., $\operatorname{ord}(\varphi(g))$ divides $\operatorname{ord}(g)$.

Images and pullbacks

Definition

If $\varphi : X \to Y$ is a map, $S \subseteq X$, and $T \subseteq Y$, then

$$\varphi(S) = \{\varphi(x) \mid x \in S\}$$
$$= \{y \in Y \mid y = \varphi(x) \text{ for some } x \in S\}$$

image of S under phi

The fact that we write phi^{-1} doesn't mean phi is invertible

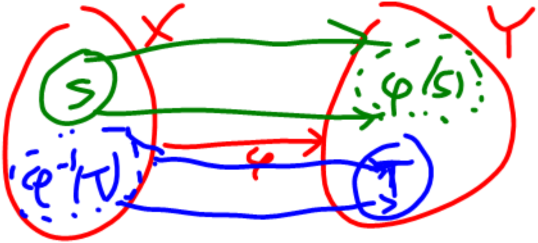
$$\varphi^{-1}(T) = \{x \in X \mid \varphi(x) \in T\}$$

inverse image, or pullback, of T

$\varphi(\varphi^{-1}(T)) \subseteq T$

(but maybe not =)

I.e., $\varphi^{-1}(T)$ is the set of all inputs x that produce an output in T; and $\varphi(S)$ is the set of all outputs y that are hit by some input in S. Picture:



Homomorphisms preserve, reduce, pull back subgp structure

THM

Suppose $\varphi : G \to \overline{G}$ is a homomorphism, $a, b, g \in G$, $K = \ker \varphi$. Suppose also $H \leq G$, $\overline{H} \leq \overline{G}$. Then:

1. $\varphi(H)$ is a subgroup of $\overline{G}$.
2. If H cyclic, $\varphi(H)$ cyclic.
3. If H abelian, $\varphi(H)$ abelian.

Converse is not true

4. If $H \lhd G$, then $\varphi(H) \lhd \varphi(G)$. (But $\varphi(H)$ might not be normal in all of G.)
5. If $|K| = n$, then φ is an n-to-1 map. (In particular, if K is trivial, then φ is one-to-one.) "by their kernels shall ye know them"
6. $\varphi^{-1}(\overline{H})$ is a subgroup of G.

etc.

Key point to remember is that $\varphi(H)$ might be less complicated than H, and $\varphi^{-1}(\overline{H})$ might be more complicated than $\overline{H}$.

Proof of 6:

$\ker\varphi = \varphi^{-1}(\{\bar{e}\})$

(A) $\bar{H} \le \bar{G}$, $\varphi: G \to \bar{G}$

(0) We know: $\varphi(e) = \bar{e}$

Since $\bar{e} \in \bar{H}$, $e \in \varphi^{-1}(\bar{H})$.

(C) $\varphi^{-1}(\bar{H}) \neq \emptyset$

1. (A) $a, b \in \varphi^{-1}(\bar{H})$

defn of φ^{-1}

So $\varphi(a) \in \bar{H}$, $\varphi(b) \in \bar{H}$

B/c $\bar{H}$ subgp, $\varphi(a)\varphi(b) \in \bar{H}$

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

So $\varphi(ab) \in \bar{H}$

(C) $ab \in \varphi^{-1}(\bar{H})$

(C) $\varphi^{-1}(\bar{H}) \le G$.

Pullbacks

$a \in \varphi^{-1}(\bar{H}) \iff \varphi(a) \in \bar{H}$

2 similar: A $a \in \varphi^{-1}(\bar{H})$

$\varphi(a) \in \bar{H}$

B/c $\bar{H}$ subgp, $\varphi(a)^{-1} \in \bar{H}$

But $\varphi(a)^{-1} = \varphi(a^{-1})$

So $\varphi(a^{-1}) \in \bar{H}$

C $a^{-1} \in \varphi^{-1}(\bar{H})$

Kernels are normal subgroups

Thm. Suppose $\varphi : G \to \overline{G}$ is a homomorphism, $a, b, \cancel{g} \in G$, $K = \ker\varphi$. Then:

1. K is a normal subgroup of G.
2. $\varphi(a) = \varphi(b)$ if and only if $aK = bK$.

"By their kernels shall ye know them"

Pf 1 $K = \ker\varphi = \varphi^{-1}(\{\bar{e}\})$, so $K \leq G$

K normal (NST)

A $a \in K = \ker\varphi$, $x \in G$

defn of homomorphism

Then $\varphi(xax^{-1}) = \varphi(x)\varphi(a)\varphi(x)^{-1}$

$= \varphi(x)\bar{e}\varphi(x)^{-1}$ defn of kernel of phi

$= \varphi(x)\varphi(x)^{-1} = \bar{e}$

So $\varphi(xax^{-1}) = \bar{e}$.

$\subseteq$ $xax^{-1} \in \ker\varphi$

Pf 2 $\varphi(a) = \varphi(b)$

$\iff \varphi(b)^{-1}\varphi(a) = \bar{e}$ mult on L by $\varphi(b)^{-1}$

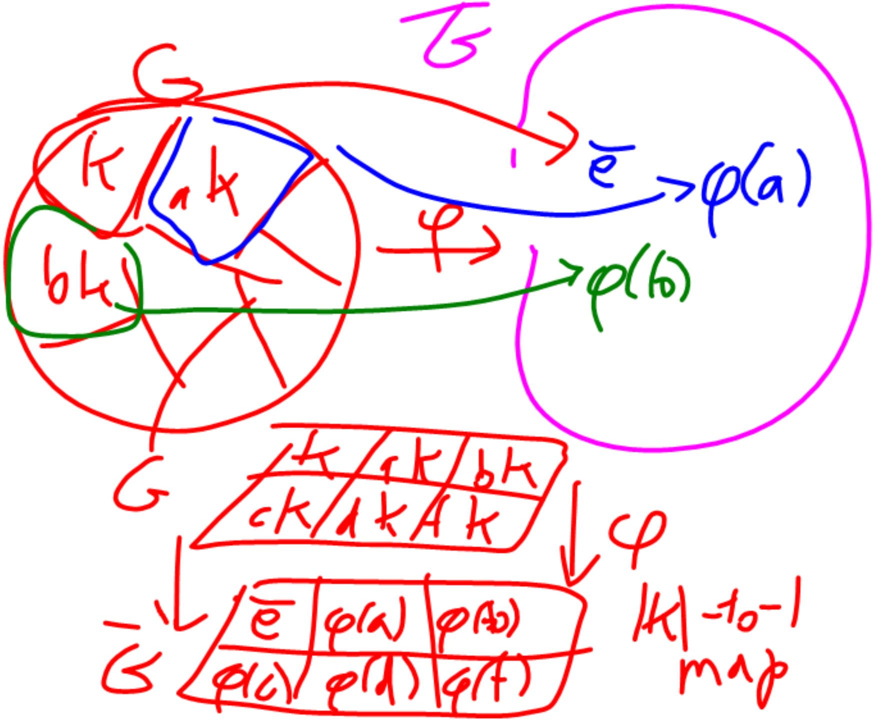
$\iff \varphi(b^{-1}a) = \bar{e}$ φ homom.

$\iff b^{-1}a \in K$ defn ker φ

$\iff b^{-1}a = k$ for $k \in K$

$\iff a = bk$ for $k \in K$ mult by b on L (h)

$\iff aK = bK$ $K = \ker\varphi$



$\bar{G}$
G
K
aK
bK
$\bar{e}$
$\varphi(a)$
$\varphi(b)$
φ
G
K | aK | bK
cK | dK | fK
φ
$\bar{G}$
$\bar{e}$ | $\varphi(a)$ | $\varphi(b)$
$\varphi(c)$ | $\varphi(d)$ | $\varphi(f)$
$|K|$-to-1 map

Example

$\varphi : \mathbf{Z}_{20}^{+} \to \mathbf{Z}_{20}^{+}$ given by $\varphi(x) = 2x$.

$\varphi(x+y) = 2(x+y) = 2x+2y = \varphi(x)+\varphi(y)$

- For several $g \in \mathbf{Z}_{20}$, compare $\text{ord}(g)$ vs. $\text{ord}(\varphi(g))$:

$\text{ord}(3) = \boxed{20}$ $\quad \varphi(3) = 6$ $\quad \text{ord}(6) = \frac{20}{\gcd(6,20)} = \boxed{10}$

$\text{ord}(5) = \boxed{4}$ $\quad \varphi(5) = 10$ $\quad \text{ord}(10) = \boxed{2}$

$\text{ord}(4) = \boxed{5}$ $\quad \varphi(4) = 8$ $\quad \text{ord}(8) = \frac{20}{\gcd(8,20)} = \boxed{5}$

- Kernel $\varphi = \{0, 10\}$ $\quad \varphi$ is 2-to-1 map

$\varphi(\mathbf{Z}_{20}) = \{0, 2, 4, \ldots, 18\} \leq \mathbf{Z}_{20}$

$0, 10 \to 0 \quad 1, 11 \to 2 \quad 2, 12 \to 4 \quad \ldots$

rho ρ

The First Isomorphism Theorem

1IT

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

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

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

Φ = Phi

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

- 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

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

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

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

Theorem

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

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 $G \approx H \oplus K$.

Lemma

If G is the internal direct product of H and K, then for $h \in H$, $k \in K$, $hk = kh$.

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.