Math 128A, Wed Oct 28

- 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. ~~9~~ 10
- PS07 due today.
- Problem session, Fri Oct 30, 10:00–noon on Zoom.

Math colloquium, 3pm today: Spatial graph theory, Erica Flapan
Email me for Zoom link

Factor groups

$\forall a \in G, aH = Ha \Leftrightarrow xHx^{-1} \subseteq H \; \forall x \in G$

Definition

For $H \lhd G$, the **factor group**, or **quotient group**, G/H is:

- **Set:** All (left) cosets aH. (Same as right cosets Ha because $aH = Ha$.)
- **Operation:** We define

$$(aH)(bH) = (ab)H.$$

Recall that this definition implies that, in the group G/H:

- **Identity** is the coset $eH = H$.
- **Inverse** of aH is $a^{-1}H$.

Ex If G = Z, H = nZ, then G/H is actually the definition of Z_n:
I.e., Z/nZ is isomorphic to Z_n.

Cauchy's Theorem for abelian groups

Theorem

Let G be an abelian group such that p divides $|G|$. Then G contains an element of order p.

Proof (cont): In last case from last time, we proceed by induction, and we ~~ahve~~: have:

$|G/N| < n$

- $x \in G$ such that $\mathrm{ord}(x) = q$ is prime, $q \neq p$;
- $N = \langle x \rangle$, which is normal because G abelian.
- $|G/N| = |G| / |N| = n/q$ is still divisible by p, so by induction, there exists an element aN of order p in G/N. $\star$

So $a \notin N$, $\underbrace{N}_{\text{id in } G/N} = \underbrace{(aN)^p}_{\text{order } p \text{ in } G/N} = a^p N$

$\Rightarrow a^p \in N$

$N = \langle x \rangle = \{e, x, \dots, x^{q-1}\}$

So $a^p = x^j \quad 0 \le j \le q-1$

$j=0$ $a^p = e$, $a \ne e$, so $\operatorname{ord}(a) = p$.

$j \ne 0$ $a^p = x^j$ has order q.

So a has order pq b/c $\gcd(p,q)=1$.

☆ G/N has elt order p

What do the elements of G/N look like? Well, they're cosets of N, and an arbitrary coset of N has the form aN for some a in G.
Note that a can't be in N because if a were in N, then aN=N would be the identity, which has order 1, not order p.

Internal direct products

XDP: $H \oplus K = \{(h,k) \mid h \in H, k \in K\}$

etc.

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 to come in Ch. 10; right now, application.

Groups of order p^2

Lag: $\text{ord}(a) = 1, p, p^2$
$a \in G$

Theorem

Suppose $|G| = p^2$, where p is prime. Then either $G \approx \mathbf{Z}_{p^2}$ or $G \approx \mathbf{Z}_p \oplus \mathbf{Z}_p$.

Sketch of proof: Suppose G not cyclic. Then every $a \neq e$ in G has order p.

w/ above,

Lemma: Every cyclic subgroup $\langle a \rangle$ of G is normal. (Proof of Lemma can be found in the text.)

So choose $a \neq e$ in G and $b \notin \langle a \rangle$. We see that:

* $\langle a \rangle, \langle b \rangle$ each $\lhd G$
* $\langle a \rangle \cap \langle b \rangle = \{e\}$
* $|\langle a \rangle \langle b \rangle| = \frac{p \cdot p}{1} = p^2$, so $G = \langle a \rangle \langle b \rangle$

So $G \approx \langle a \rangle \oplus \langle b \rangle$.

by IDP Thm

Gps of small order:

$\mathbb{Z}_2 \oplus \mathbb{Z}_3 \approx \mathbb{Z}_6$

$\gcd(2,3) = 1$

1. $G = \{e\}$
2. $G \simeq \mathbb{Z}_2$
3. $G \approx \mathbb{Z}_3$
4. $G \approx \mathbb{Z}_4$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$
5. $G \approx \mathbb{Z}_5$
6. $G \approx \mathbb{Z}_6$ or D_3
7. $G \approx \mathbb{Z}_7$
8. Five poss, 3 ab, 2 non-ab
9. $G \approx \mathbb{Z}_9$ or $\mathbb{Z}_3 \oplus \mathbb{Z}_3$
10. $G \approx \mathbb{Z}_{10}$ or D_5
11. $G \approx \mathbb{Z}_{11}$
12. Five poss, 2 ab, 3 non-ab.

$\mathbb{Z}_5 \oplus \mathbb{Z}_5 \not\simeq \mathbb{Z}_{25}$

25 $G \simeq \mathbb{Z}_{25}$ or $\mathbb{Z}_5 \oplus \mathbb{Z}_5$

$D_n \not\simeq \mathbb{Z}_k \oplus \mathbb{Z}_\ell$

$(n \geq 3)$

There is a fancier kind of product, called the semidirect product of groups, that allows us to construct every D_n as a semidirect product of Z_n and Z_2. (See 128B!)

To be proven in Ch. 10

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

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

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

Theorem

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

Again, proof in Ch. 10.

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

op in $\overline{G}$

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

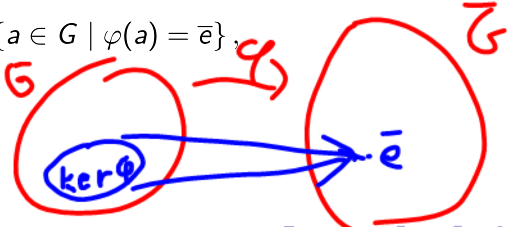
(I.e., a homomorphism is an isomorphism, but not requiring one-to-one or onto.)

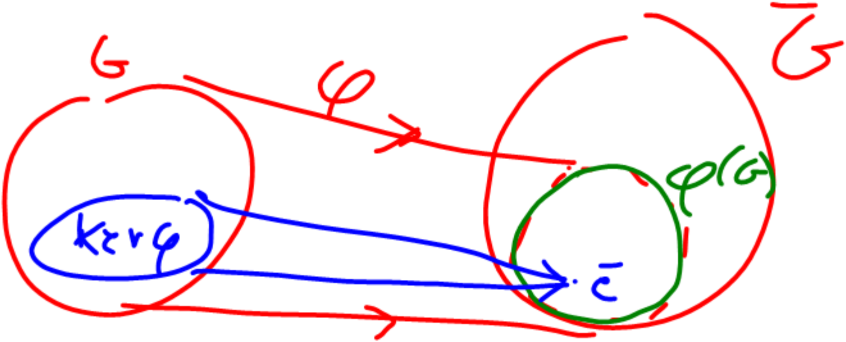
Definition

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 $\overline{G}$.





G
φ
$\bar{G}$
φ(G)
Kerφ
$\bar{e}$

Examples

inv $n \times n$ non-0 $\mathbb{R}$, op mult id I

Example

$G = GL(n, \mathbf{R})$, and det : $G \to \mathbf{R}^*$. Then det is a homomorphism because:

1'in al FTW

$$\det(AB) = \det A \det B$$

Kernel is: $= \{A \in G \mid \det A = 1\} = SL(n, \mathbb{R})$

Example

$G = \mathbf{R}^+$ (positive reals, operation multiplication), and consider log : $G \to \mathbf{R}$ (all reals, operation $+$). Then log is a homomorphism because:

$$\log(\underbrace{ab}_{\text{op in } \mathbb{R}^+}) = \log a \underbrace{+}_{\text{op in } \mathbb{R}} \log b$$

Kernel is: $= \{a \in \mathbb{R}^+ \mid \log a = 0\} = \{1\}$

Example

$G = \mathbf{Z}_{20}$, and consider $\varphi : \mathbf{Z}_{20} \to \mathbf{Z}_{20}$ given by $\varphi(x) = 2x$. Then φ is a homomorphism because: $\forall x, y \in \mathbb{Z}_{20}$

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

op in $\mathbb{Z}_{20}$

Check:

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

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

Kernel is:

x s.t.

$\varphi(x) = 2x = 0$

$\ker\varphi = \{0, 10\}$

$\varphi(0) = 0$
$\varphi(10) = 0$

not 1-to-1

Homomorphisms preserve or reduce a lot of element structure

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

1. $\varphi(e) = \overline{e}$.
2. $\varphi(g^n) = \varphi(g)^n$.

you check

3. $\mathrm{ord}(\varphi(g))$ divides $\mathrm{ord}(g) < \infty$
4. K is a subgroup of G.

later

5. $\varphi(a) = \varphi(b)$ if and only if $aK = bK$.

next time -- shows up in lots of parts of math.

Pf If $\mathrm{ord}(g) = n$, $g^n = e$.
Then $(\varphi(g))^n = \varphi(g^n) = \varphi(e) = \overline{e}$
$\Rightarrow \mathrm{ord}(\varphi(g))$ divides n.

Pullbacks

Definition

If $f : X \to Y$ is a map, $T \subseteq Y$, then

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

I.e., $\varphi^{-1}(T)$ is the set of all inputs x such that $\varphi(x) \in T$.

Homomorphisms preserve, reduce, pull back subgp structure

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.
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.)

6. $\varphi^{-1}(\overline{H})$ is a subgroup of G.

etc.

Kernels are normal subgroups

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

Example

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

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

- Kernel

The First Isomorphism Theorem