Math 128A, Mon Oct 26

- 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. 9. Reading for Wed: Ch. 10.
- PS07 outline due today, full version due Wed.
- Problem session, Fri Oct 30, 10:00–noon on Zoom.

Normal subgroups, normal subgroup test

left and right cosets are the same

Definition
To say that $H \leq G$ is **normal** in G means that $aH = Ha$ for all $a \in G$, in which case we write $H \lhd G$.

Theorem (NST)
Suppose $H \leq G$. TFAE:

1. $H \lhd G$.
2. *For all $x \in G$, $x^{-1}Hx \subseteq H$.*

Cond 2 =
"For all x in G and all h in H, "$x^{-1}hx \in H$"
= "$x^{-1}hx = h'$ for some $h' \in H$"

$=$ "$hx = xh'$ for some $h' \in H$"

In other words, H is normal exactly when we can move any x in G past any h in H, at the cost of possibly changing h to some other element h' of H.

Factor groups

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

a is called a representative of the coset aH, and b reps bH.

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

Note that this is the multiplication of cosets that you get when you multiply individual elements — assuming that coset times coset is coset.

I.e., defn of the operation looks like it might depend on which representative we choose for each coset; we need to show that it doesn't.

Theorem

G/H really is a group.

Proof: Hard part is showing that operation is well-defined; i.e., if $aH = a'H$ and $bH = b'H$, is $(a'b')H = (ab)H$?

Recall that TFAE: (Ch. 7)

- $xH = yH$
- $y \in xH$
- $y = xh$ for some $h \in H$.

This step takes more work, see Ch. 7.

So if $aH = a'H$

$bH = b'H$

then $a' = ah_1$ $(h_1, h_2 \in H)$

$b' = bh_2$

So $a'b' = a\underbrace{h_1 b}h_2$ b/c $H \lhd G$

$= abh_3h_2$ for some $h_3 \in H$

Let $h = h_3h_2$

So $a'b' = ab\underbrace{h}$ for some $h \in H$

b/c H closed.

$a'b'H = abH$

Remains to check associativity, identity, inverse:

Id: is $eH = H$

Inv $(aH)^{-1} = a^{-1}H$

Check

$$(aH)(a^{-1}H) \overset{\text{by defn}}{=} (aa^{-1})H = eH = H, \text{ the id in } G/H$$

$(a^{-1}H)(aH)$ similar.

Example

G/H = "G mod H"

$\{e, R_{60}, R_{120}, \ldots, R_{300}\}$

1. $G = D_6$, $H = \langle R_{60} \rangle$. Then

$$G/H \approx \mathbb{Z}_2$$

+	0	1
0	0	1
1	1	0

$|G| = 12$

$= \{e, R_{180}\}$

2. $G = D_6$, $H = \langle R_{180} \rangle$. Then

$$G/H \approx D_3$$

$|G/H| = 6$

$\mathbb{Z}_6$ or D_3?

H F, H

	e	R_{60}	R_{120}	R_{180}	R_{240}	R_{300}	F_1	F_2	F_3	F_{12}	F_{23}	F_{34}
e	e	R_{60}	R_{120}	R_{180}	R_{240}	R_{300}	F_1	F_2	F_3	F_{12}	F_{23}	F_{34}
R_{60}	R_{60}	R_{120}	R_{180}	R_{240}	R_{300}	e	F_{12}	F_{23}	F_{34}	F_2	F_3	F_1
H R_{120}	R_{120}	R_{180}	R_{240}	R_{300}	e	R_{60}	F_2	[illegible]	F_1	F_{23}	F_{34}	F_{12}
R_{180}	R_{180}	R_{240}	R_{300}	e	R_{60}	R_{120}	F_{23}	F_{34}	F_{12}	F_3	F_1	F_2
R_{240}	R_{240}	R_{300}	e	R_{60}	R_{120}	R_{180}	F_3	F_1	F_2	F_{34}	F_{12}	F_{23}
R_{300}	R_{300}	e	R_{60}	R_{120}	R_{180}	R_{240}	F_{34}	F_{12}	F_{23}	F_1	F_2	F_3
F_1	F_1	F_{34}	F_3	F_{23}	F_2	F_{12}	e	R_{240}	R_{120}	R_{300}	R_{180}	R_{60}
F_2	F_2	F_{12}	F_1	F_{34}	F_3	F_{23}	R_{120}	e	R_{240}	R_{60}	R_{300}	R_{180}
F_3	F_3	F_{23}	F_2	F_{12}	F_1	F_{34}	R_{240}	R_{120}	e	R_{180}	R_{60}	R_{300}
F.H F_{12}	F_{12}	F_1	F_{34}	F_3	F_{23}	F_2	R_{60}	R_{300}	R_{180}	e	R_{240}	R_{120}
F_{23}	F_{23}	F_2	F_{12}	F_1	F_{34}	F_3	R_{180}	R_{60}	R_{300}	R_{120}	e	R_{240}
F_{34}	F_{34}	F_3	F_{23}	F_2	F_{12}	F_1	R_{300}	R_{180}	R_{60}	R_{240}	R_{120}	e

		e	R_{180}	F_2	F_{34}	R_{60}	R_{240}	F_1	F_{23}	R_{120}	R_{300}	F_3	F_{12}
		e		a		b		c		d		f	
e	e	e	R_{180}	F_2	F_{34}	R_{60}	R_{240}	F_1	F_{23}	R_{120}	R_{300}	F_3	F_{12}
	R_{180}	R_{180}	e	F_{34}	F_2	R_{240}	R_{60}	F_{23}	F_1	R_{300}	R_{120}	F_{12}	F_3
a	F_2	F_2	F_{34}	e	R_{180}	F_{12}	F_3	R_{120}	R_{300}	F_1	F_{23}	R_{240}	R_{60}
	F_{34}	F_{34}	F_2	R_{180}	e	F_3	F_{12}	R_{300}	R_{120}	F_{23}	F_1	R_{60}	R_{240}
b	R_{60}	R_{60}	R_{240}	F_{23}	F_1	R_{120}	R_{300}	F_{12}	F_3	R_{180}	e	F_{34}	F_2
	R_{240}	R_{240}	R_{60}	F_1	F_{23}	R_{300}	R_{120}	F_3	F_{12}	e	R_{180}	F_2	F_{34}
c	F_1	F_1	F_{23}	R_{240}	R_{60}	F_{34}	F_2	e	R_{180}	F_3	F_{12}	R_{120}	R_{300}
	F_{23}	F_{23}	F_1	R_{60}	R_{240}	F_2	F_{34}	R_{180}	e	F_{12}	F_3	R_{300}	R_{120}
d	R_{120}	R_{120}	R_{300}	F_3	F_{12}	R_{180}	e	F_2	F_{34}	R_{240}	R_{60}	F_1	F_{23}
	R_{300}	R_{300}	R_{120}	F_{12}	F_3	e	R_{180}	F_{34}	F_2	R_{60}	R_{240}	F_{23}	F_1
f	F_3	F_3	F_{12}	R_{120}	R_{300}	F_{23}	F_1	R_{240}	R_{60}	F_2	F_{34}	e	R_{180}
	F_{12}	F_{12}	F_3	R_{300}	R_{120}	F_1	F_{23}	R_{60}	R_{240}	F_{34}	F_2	R_{180}	e

Center of G

Consequences!!!!

Z(G) is the set of elements in G that commute with everything in G.

Recall $Z(G) = \{z \in G \mid zx = xz \text{ for all } x \in G\}$.

Note that $Z(G) \lhd G$:

(A) $x \in G,\ h \in Z(G)$

$x^{-1}hx = \underbrace{x^{-1}x}h$ b/c $h \in Z(G)$

$= h \in Z(G)$.

(C) $x^{-1}hx \in Z(G)$

NST

G/Z theorem

know $Z \lhd G$

Theorem

G a group, $Z = Z(G)$ center of G. If G/Z is cyclic, then G is abelian.

Proof: Suppose G/Z is cyclic. Then G/Z is generated by some coset aZ, i.e.:

$$G/Z = \{Z, aZ, a^2Z, \ldots\}$$

$$= \{a^nZ \mid n \in \mathbb{Z}\} = \langle aZ \rangle$$

$$(aZ)^n = a^nZ$$

B/c cosets partition G, for any x, y in G, each of x and y is contained in some coset a^n Z. So:

$$x = a^n z_1 \quad y = a^k z_2 \quad z_1, z_2 \in Z$$

Then

$$\begin{aligned} xy &= a^n z_1 a^k z_2 \\ &= a^n a^k z_1 z_2 \\ &= a^k a^n z_2 z_1 \\ &= a^k z_2 a^n z_1 \\ &= yx \end{aligned}$$

$z_i \leftarrow$ center of G

Since x and y are arbitrary elements of G, G must be abelian.

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: Induction (strong) on $n = |G|$. If $|G| = p$, G cyclic, done. Now suppose theorem holds whenver $|G| < n$. Take a nontrivial element of G; by taking a suitable power of that nontrivial element, get some $x \in G$ such that $\mathrm{ord}(x) = q$ is prime. If $q = p$, done; otherwise, let $N = \langle x \rangle$ and consider G/N. Note that $|G/N| = |G| / |N| = n/q$ is still divisible by p, in that case. $q \neq p$

By ind, $\exists\ aN \in G/N$ s.t. $\mathrm{ord}(aN) = p$.

So $(aN)^p = N$.

$\Rightarrow a^p N = N$

$\Rightarrow a^p \in N$.

START HERE NEXT

But $a^1N, a^2N, \ldots, a^{p-1}N \neq N$, so $\mathrm{ord}(a)$ can't be r.p. to p. so p divs $\mathrm{ord}(a)$, i.e. $\mathrm{ord}(a) = pk$ for some k. Then $\mathrm{ord}(a^k) = p$.

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

Groups of order p^2

Theorem

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

Proof: Suppose G not cyclic. Then every $a \neq e$ in G has order

Claim: Every cyclic subgroup $\langle a \rangle$ of G is normal.
ABC: $b \in G$ such that $bab^{-1} \notin \langle a \rangle$. Then if $H = \left\langle bab^{-1} \right\rangle$, b must be in one of the cosets

$$H,\ aH,\ a^2H, \ldots, a^{p-1}H.$$

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.