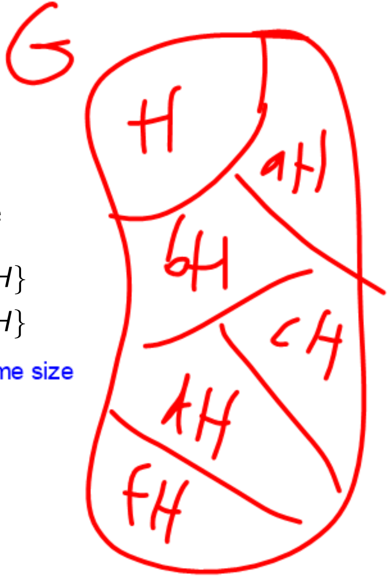
Math 128A, Mon Oct 12

- 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 Wed: Ch. 8.
- PS06 due Wed.
- **EXAM ~~1~~ 2 in one week.**
- Exam review Fri Oct 16, 10:00–noon on Zoom.

Cosets so far



Definition

G a group, H a subgroup, $a \in G$. Define

$$aH = \{ah \mid h \in H\}$$
$$Ha = \{ha \mid h \in H\}$$

and all cosets have same size

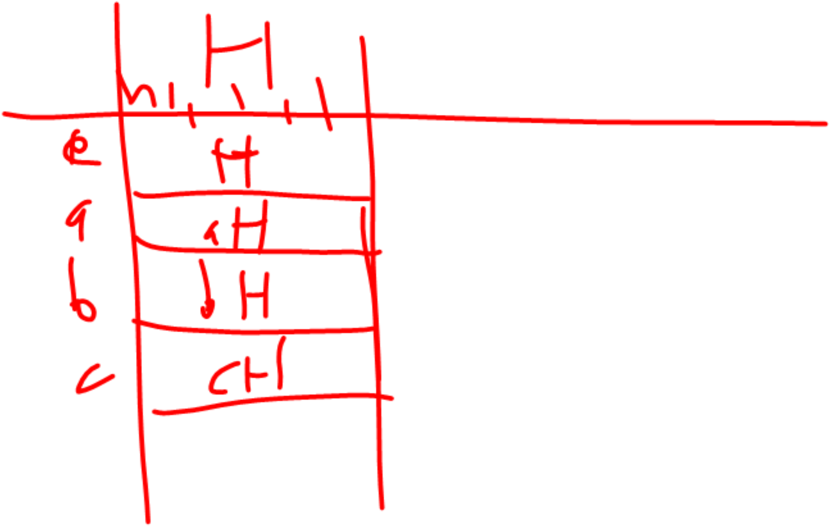
The left cosets of H partition G, so:

Theorem (Lagrange)

G finite, $H \leq G$. Then $|H|$ divides $|G|$.

Note that in general, left and right cosets might overlap. To get a partition, only use one type of coset at a time.

Cosets as pictured by Cayley table:



Groups of order $2p$

Suppose $p > 2$ is prime.

	b	ab
$\langle a \rangle =$	e	$a \quad a^2 \quad \cdots \quad a^{p-1}$

G

Theorem

If $|G| = 2p$, then either G is isomorphic to $\mathbf{Z}_{2p}$ (cyclic) or G is isomorphic to D_p (dihedral).

Proof: Assume G is not cyclic, so no elements of order $2p$. Then:

- Show that G must contain an element a of order p.
- Show that any $b \notin \langle a \rangle$ must have order 2. Uses |HK| formula
- Because b, ab have order 2, G must be isomorphic to D_p.

B/c $\mathrm{ord}(ab) = 2$:

$$abab = e$$

mult a^{-1} on L

$$\cancel{a^{-1}a}\,bab = a^{-1}e$$

$$\boxed{bab = a^{-1}}$$

So as we see from PS02, where we analyzed a group with
FRF = R^{-1}, F^2=e, every element of G can be written in the form a^n b^k, and multiplication in G (i.e., Cayley table of G) is determined by "move-past rules". So PS02 finishes this proof: If |G|=2p, and G not cyclic, then G must be isomorphic to D_p.

To what extent do we understand groups of small order now?

|G|=1: We know G = {e}.
|G|=2: prime order, so G = $\mathbb{Z}_2$

$|G|=3$: $G \cong \mathbb{Z}_3$

$|G|=5$: $G \cong \mathbb{Z}_5$

$|G|=6=2p$: $G \cong \mathbb{Z}_6, D_3 \cong S_3$

$|G|=7$: $G \cong \mathbb{Z}_7$

$|G|=10$: $G \cong \mathbb{Z}_{10}, D_5$

Gaps: $|G|=4,8,9$

$|S_3|=6$

$|G|=11$
$G \cong \mathbb{Z}_{11}$

$|G|=12$: $\mathbb{Z}_{12}, D_6, A_4$; others?

$|G|=p$: 13, 17, 19, 23, ...

$|G|=2p$: 14, 22, ...

$|G|=15, 18, 20, 21$: Math 128B

$|G|=16$ -- it's complicated!!!

$|G|=24$: See PS06....

See 128B...

Orbits and stabilizers

Suppose G is a finite group of permutations of a set S. For $i \in S$, define

stab = all permutations that fix i (leave i alone)

$$\text{stab}_G(i) = \{\alpha \in G \mid \alpha(i) = i\},$$

$$\text{orb}_G(i) = \{\alpha(i) \mid \alpha \in G\}.$$

orbit = all the places that elements of G can send i.

The Orbit-Stabilizer Theorem says:

Theorem

For $i \in S$, $|G| = |\text{orb}_G(i)|\,|\text{stab}_G(i)|$.

Why: Can show that elements of $\text{orb}_G(i)$ correspond bijectively with cosets of $\text{stab}_G(i)$.

Examples of Orbit-Stabilizer

G a finite group of permutations of a set S.

We can also think of G as a group of permutations of the vertices of icosahedron.

Theorem

For $i \in S$, $|G| = |\mathrm{orb}_G(i)|\,|\mathrm{stab}_G(i)|$.

Example: G = group of rotational symmetries of icosahedron. All vertices in same G-orbit; same holds for edges and faces.

Can move any v to any other vertex by rotataions, and so all vert in same orbit.

Same is true for edges and faces. So all edges in same orbit, and all faces.

$\#$ vertices $= 12$ $\quad |\mathrm{stab}_G(v)| =$ |# rotations fixing v| $=5$

$|G| = 12 \cdot 5 = 60$

$\#$ edges $= 30$ $\quad |\mathrm{stab}_G(e)| = 2$

$60 = 30 \cdot 2$

$\#$ faces $= 20$ $\quad |\mathrm{stab}_G(f)| = 3$

$60 = 20 \cdot 3$

Other applications of Orbit-Stabilizer: Find the orders of the rotational symmetry groups of cube, octahedron, dodecahedron, and tetrahedron....

External direct products

Making new groups from old....

Ch. 8

Definition

G, H groups. **External direct product** $G \oplus H$ is:

- Set: Cartesian product $G \times H = \{(g, h) \mid g \in G, \ h \in H\}$.
- Operation is componentwise:

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2).$$

Identity is: $(e_G, e_H) \in G \oplus H$

Inverse of (g, h) is: $(g^{-1}, h^{-1}) \in G \oplus H$

Why is (g^{-1}, h^{-1}) inv of (g,h)?

B/c $(g^{-1}, h^{-1})(g,h) = (g^{-1}g, h^{-1}h)$

$= (e,e)$

$(g,h)(g^{-1}, h^{-1}) = (gg^{-1}, hh^{-1})$

$= (e,e)$

So $(g^{-1}, h^{-1}) = (g,h)^{-1}$!

Examples

$\mathbf{Z}_3 \oplus \mathbf{Z}_4 = \{(0,0),(0,1),(0,2),(0,3),(1,0),(1,1),(1,2),(1,3),(2,0),(2,1),(2,2),(2,3)\}$

Sum of two random elements:

$$(0,1)+(1,3)=(\overset{\text{mod } 3}{1},\overset{\text{mod } 4}{4})=(1,0)$$

$D_5 \oplus S_4$ has order:

$|D_5 \oplus S_4| = 10 \cdot 24 = 240$

$|D_5| = 10, \; |S_4| = 24$

Product of two random elements:

$$(F_1,(123))(F_2,(14)) = (F_1F_2,(123)(14)) = (R_{216},(1423))$$

Why external direct products?

Among other applications, they provide a convenient way to describe non-cyclic abelian groups. For example:

Theorem

If $|G| = 4$*, then either* G *is cyclic, or* G *is isomorphic to* $\mathbf{Z}_2 \oplus \mathbf{Z}_2$*.*

Proof:

When is $G \oplus H$ cyclic?

We'll see that every finite abelian group is isomorphic to a group of the form $\mathbf{Z}_{n_1} \oplus \cdots \oplus \mathbf{Z}_{n_k}$, just like any positive integer is a product of primes.

Also, just as prime factorization is unique up rearrangement, the form $\mathbf{Z}_{n_1} \oplus \cdots \oplus \mathbf{Z}_{n_k}$ is unique up to rearrangement and a particular kind of ambiguity.

To start:

Theorem

For $(g, h) \in G \oplus H$, *if* $\operatorname{ord}(g)$ *and* $\operatorname{ord}(h)$ *are finite, then*

$$\operatorname{ord}((g, h)) = \operatorname{lcm}(\operatorname{ord}(g), \operatorname{ord}(h)).$$

Proof:

Counting orders of elements

Example: Let $G = \mathbf{Z}_9 \oplus \mathbf{Z}_{27}$.

- How many elements of order 9 are there in G?
- How many cyclic subgroups of order 9 does G have?

Back to “When is $G \oplus H$ cyclic?”

Theorem

$\mathbf{Z}_n \oplus \mathbf{Z}_k$ *is cyclic if and only if* $\gcd n, k = 1$.

Proof:

$U(n)$ as an external direct product

For k dividing n, let

$$U_k(n) = \{x \in U(n) \mid x \equiv 1 \pmod{k}\}.$$

Theorem

If $\gcd(s,t) = 1$, *then*

$$U(st) \approx U(s) \oplus U(t).$$

Also, $U_s(st) \approx U(t)$ *and* $U_t(st) \approx U(s)$.

Proof delayed until Ch. 10.

Facts: We also have that $U(2)$ is trivial, and

$$\begin{aligned} U(4) &\approx \mathbf{Z}_2 & \\ U(2^n) &\approx \mathbf{Z}_{2^{n-2}} \oplus \mathbf{Z}_2 & \text{for } n \geq 3 \\ U(p^n) &\approx \mathbf{Z}_{p^n - p^{n-1}} & \text{for } n \geq 3,\ p \text{ an odd prime.} \end{aligned}$$

Example of computing the isomorphism type of $U(n)$

Let $n =$.

Then $U(n)$ is: