Math 128A, Wed Oct 07

- 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. 7. Mon: Ch. 8.
- PS05 due tonight; outline for PS06 due Fri.
- Problem session Fri Oct 09, 10:00–noon on Zoom.

Cosets

Compare: $\phi_a(x) = axa^{-1}$

H conjugated on the left by a

Definition

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

$$aH = \{ah \mid h \in H\}$$
$$Ha = \{ha \mid h \in H\}$$
$$aHa^{-1} = \{aha^{-1} \mid h \in H\}$$

We call aH the **left coset of H in G containing** a, and we call Ha the **right coset of H in G containing** a.

Cosets via equivalence relations

$H \leq G$, $a, b, c \in G$.

Definition

Define $\boxed{a \sim b \text{ to mean that } a^{-1}b \in H.}$ ☆

Theorem

$\sim$ is an equivalence relation on G.

R A $a \in G$

Observe $a^{-1}a = e \in H$ b/c $H \leq$ subgp

So $a^{-1}a \in H$. defn ☆

C $a \sim a$ ☺

S A $a, b \in G$, $a \sim b$. defn ☆

So $a^{-1}b \in H$.

B/c H closed inv, $(a^{-1}b)^{-1} \in H$.

S&S $\Rightarrow (a^{-1}b)^{-1} = b^{-1}a$

So $b^{-1}a \in H$.

C $b \sim a$

T

A $a, b, c \in G$. $a \sim b$, $b \sim c$

So $a^{-1}b \in H$, $b^{-1}c \in H$

B/c H closed op, $(a^{-1}b)(b^{-1}c) \in H$

$(a^{-1}\cancel{b})(\cancel{b}^{-1}c) = a^{-1}c$.

So $a^{-1}c \in H$

C $a \sim c$.

Cosets are equivalence classes

What are equivalence classes of $\sim$? The class of $a \in G$ is:

$$
\begin{aligned}
[a] = \{b \in G \mid a \sim b\} &= \{b \in G \mid a^{-1}b \in H\} \\
&= \{b \in G \mid b \in aH\} \\
&= aH.
\end{aligned}
$$

mult on L by a

So left cosets of H are equivalence classes of an equivalence relation, which means that left cosets of H **partition** G:

Cosets all have the same size

Theorem

Suppose H is a finite subgroup of G, $a, b \in G$. Then $|aH| = |bH|$.

Proof: Consider $f : aH \to bH$ given by

$$f(ah) = bh. \quad \text{for all } h \in H.$$

We prove that f is a bijection: (sketch)

Consider: $g : bH \to aH$ by

$$g(bh) = ah.$$

Can check $f \circ g = \mathrm{id}$, $g \circ f = \mathrm{id}$.

So $g = f^{-1} \Rightarrow f$ inv'ble $\Rightarrow f$ bij.

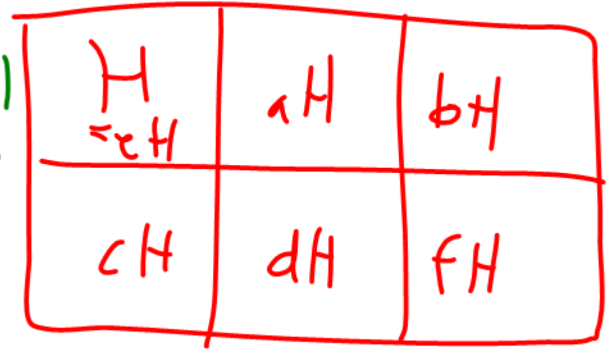
Lagrange's Theorem

Theorem

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

Proof: Combine previous two slides into one picture:

$|G:H| = 6$



So if there are n pieces, each of size |H|, then the order of G is n|H|.

Define $|G : H|$ to be the number of cosets of H in G.

|G:H| is called the index of H in G.

Corollary

$|G : H| = |G| \,/\, |H|$.

Two consequences of Lagrange's Theorem

Corollary

G finite, $a \in G$. Then $\mathrm{ord}(a)$ divides $|G|$.

order of an element divides the order of the group

Pf $\mathrm{ord}(a) = |\langle a \rangle|$.

$\Rightarrow$ If $|G| = 8675309$, then $G \cong \mathbb{Z}_{8675309}$

Corollary

If $|G| = p$ prime, then G is cyclic.

Pf Choose any $a \in G$, $a \neq e$.

By, $\mathrm{ord}(a)$ div p, so $\mathrm{ord}(a) = 1$ or p.

$a \neq e$, so $\mathrm{ord}(a) \neq 1 \Rightarrow |\langle a \rangle| = p$, so $\langle a \rangle = G$

$U(12) = \{1, 5, 7, 11\}$

$|U(12)| = 4$

(Can check $U(12)$ not cyclic.)

The only groups of prime order that we have seen are all cyclic.
That's not an accident -- all groups of prime order are cyclic.

A counting fact

Suppose $H, K \leq G$. Define

$$HK = \{hk \mid h \in H, k \in K\}.$$

Note that HK may not be a sub**group** of G, though it is always a sub**set** of G. (See PS03.)

Theorem

We have that

$$|HK| = \frac{|H|\,|K|}{|H \cap K|}.$$

Proof: PS07.

Groups of order $2p$

Suppose $p > 2$ is prime.

Theorem 6, 10, 14, 22, ...

If $|G| = 2p$, then either G is isomorphic to $\mathbf{Z}_{2p}$ (cyclic) or G is isomorphic to D_p (dihedral). Cor $S_3 \simeq D_3$

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

1 ▶ Show that G must contain an element a of order p.

2 ▶ Show that any $b \notin \langle a \rangle$ must have order 2.

3 ▶ Because b, ab have order 2, G must be isomorphic to D_p.

① $\boxed{\text{ABC}}$ All $a \neq e$ in G have ord 2.

Take a, b, $a \neq b$, $ab \neq e$.

Note $a = a^{-1}$, $b = b^{-1}$ b/c ord 2.

If $ab = e$, then $a = b^{-1} = b$; contra.

So ab has order 2, $(ab)^2 = e$.

$\Rightarrow abab = e \Rightarrow (\cancel{b}\cancel{a})\cancel{a}\cancel{b}ab = (ba)e$

$\Rightarrow ab = ba$. Then we can check

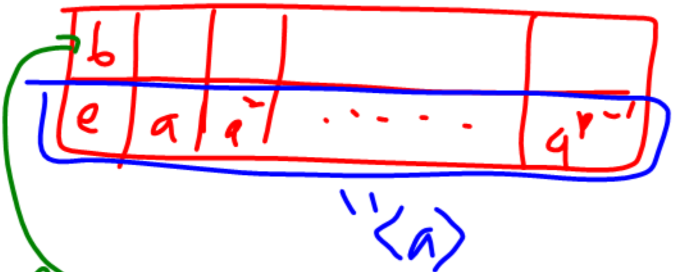
$\{e, a, b, ab\}$ is subgp of G, ord 4.

But 4 doesn't divide $|G| = 2p$; contra.

So can't have all elts have ord. 2 $\Rightarrow \exists$ elt a of order p.

Picture:

Technique for analyzing finite groups: Filling the box, i.e., figure out the orders of all of the elements of a group.



$|G| = 2p$

Q: For $b \notin \langle a \rangle$, what's ord(b)?

By counting fact $\boxed{\#}$, can't be p, ABC $\neq 2p$, so must be ord$(b) = 2$

Fact that $\operatorname{ord}(a)=p$, $\operatorname{ord}(b)=2$, $G \neq \mathbb{Z}_{2p} \Rightarrow$ mult table of G.

See text for details.

Orbits and stabilizers

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

$$\begin{aligned} \mathrm{stab}_G(i) &= \{\alpha \in G \mid \alpha(i) = i\}, \\ \mathrm{orb}_G(i) &= \{\alpha(i) \mid \alpha \in G\}. \end{aligned}$$

The Orbit-Stabilizer Theorem says:

Theorem

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

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

Examples of Orbit-Stabilizer

G a finite group of permutations of a set S.

Theorem

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

Example: $G =$ group of rotational symmetries of icosahedron.

$\#$ vertices $=$ $|\mathrm{stab}_G(v)| =$

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

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

External direct products

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:

Inverse of (g, h) is:

Examples

$\mathbf{Z}_3 \oplus \mathbf{Z}_4 =$

Sum of two random elements:

$D_5 \oplus S_4$ has order:

Product of two random elements: