Math 128A, Mon Oct 05

- 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. Reading for Wed: Ch. 8.
- **New deadlines:** PS05 due Wed; outline for PS06 due Fri.
- Problem session Fri Oct 09, 10:00–noon on Zoom.

Outlines for PS05 still accepted by tonight.

Reminder: Exam 2 in 2 weeks.

In what way are isomorphic groups the same?

Things preserved by isomorphisms:

Theorem

$\varphi : G \to \overline{G}$ an isomorphism, $a, b \in G$. Then

1. $\varphi(e) = \overline{e}$. identity
2. $\varphi(a^n) = \varphi(a)^n$. powers
3. *a and b commute $\Leftrightarrow$ $\varphi(a)$ and $\varphi(b)$ commute.* commuting
4. $G = \langle a \rangle \Leftrightarrow \overline{G} = \langle \varphi(a) \rangle$. generators
5. $\operatorname{ord}(a) = \operatorname{ord}(\varphi(a))$. orders
6. *$x^k = b$ and $\overline{x}^k = \varphi(b)$ have the same number of solutions.* kth roots
7. *$\varphi^{-1} : \overline{G} \to G$ is also an isomorphism.*
8. *G and $\overline{G}$ have same number of elements of each order.* # elements of a given order
9. *G abelian $\Leftrightarrow$ $\overline{G}$ abelian.* abelian
10. *φ sends subgroups of G to subgroups of $\overline{G}$, and vice versa.* subgroup lattice
11. *φ sends the center of G to the center of $\overline{G}$.* center

Proof of one of those preserved properties

6. x^k = b and y^k = \phi(b) have the same number of solutions.

Pf S'pose $x^k = b$. Then $\varphi(x^k) = \varphi(b)$

$\Rightarrow (\varphi(x))^k = \varphi(b)$

So because phi is a bijection (one-to-one and onto) every solution to x^k = b produces a different solution to y^k = phi(b). Therefore, there are at least as many solutions to y^k = phi(b) as there are to x^k = b.

However, because phi^{-1} is also isomorphism, by symmetry, there are at least as many solutions to x^k = b as there are to y^k = phi(b). So the # of solutions must be equal.

---

7. φ^{-1} is an isom. $(\varphi: G \to \bar{G})$

FACT: (Math 108) A function f is a bijection if and only if it has an inverse f^{-1}, and in that case, f^{-1} is also a bijection. See Thm 0.8, pp. 22-23.

So φ^{-1} is a bijection. ✓

$\boxed{\text{WTS: For } \bar{a}, \bar{b} \in \bar{G}, \quad \varphi^{-1}(\bar{a}\bar{b}) = \varphi^{-1}(\bar{a})\varphi^{-1}(\bar{b})}$

A $\bar{a}, \bar{b} \in \bar{G}$

b/c φ onto, $\exists\, a, b \in G$ s.t. $\varphi(a) = \bar{a}$, $\varphi(b) = \bar{b}$

We know $\varphi(ab) = \varphi(a)\varphi(b) = \bar{a}\bar{b}$

$\boxed{\varphi^{-1} \text{ both sides}}$ $\quad ab = \varphi^{-1}(\bar{a}\bar{b})$

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

So $\varphi^{-1}(\bar{a})\varphi^{-1}(\bar{b}) = \varphi^{-1}(\bar{a}\bar{b})$

$\boxed{C}$ $\varphi^{-1}(\bar{a}\bar{b}) = \varphi^{-1}(\bar{a})\varphi^{-1}(\bar{b})$

Isoms/homoms: φ, ρ, ψ

rho

psi

Φ

Phi

Proving that groups are **not** isomorphic

Not enough to pick some $\varphi : G \to \overline{G}$ and show φ isn't an isomorphism — maybe there's a different map that is!

But just as two people with different eye colors can't be genetic twins, two groups with different characteristics can't be isomorphic.

Example: Two groups of order 10 that aren't isomorphic?

$\mathbb{Z}_{10}$ - cyclic, abelian

D_5 - nonab $\Rightarrow$ not cyclic

Example: Prove that D_6 and A_4 aren't isomorphic.

$|D_6| = 2 \cdot 6$, nonab, D_6 has elt order 6

$|A_4| = \frac{4!}{2}$, nonab. A_4 has only elts of order 1, 2, 3

$|U(12)| = |\{1,5,7,11\}| = 4$

$|\mathbb{Z}_{12}| = 12$ $\quad \mathbb{Z}_{12}$ abelian

So no two of $D_6, A_4, \mathbb{Z}_{12}$ are isom

(Turns out that there are exactly 5 groups of order 12, up to isomorphism.)

Automorphisms

Definition

An **automorphism** of G is an isomorphism from G to itself.

An automorphism of G isn't used to show that G is the same as itself; it shows a certain symmetry in the structure of G.

Definition

G a group, $a \in G$. Define $\varphi_a : G \to G$ by

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

for all $x \in G$. We call φ_a an **inner automorphism of** G.

Try at home: Prove that φ_a is an automorphism of G.
Can show that the following are groups:

$$\left.\begin{aligned} \mathrm{Aut}(G) &= \{\text{all automorphisms of } G\} \\ \mathrm{Inn}(G) &= \{\text{all inner automorphphms of } G\} \\ &= \{\varphi_a \mid a \in G\}. \end{aligned}\right\}$$

See ch. 9

In general, Aut(G) is strictly bigger than Inn(G).

Example: Take G cyclic of order 3. G abelian, so Inn(G) = {id}.

But if $G = \langle a \rangle = \{e, a, a^2\}$

Then $\varphi(e) = e$

$\varphi(a) = a^2$

$\varphi(a^2) = a$

is in Aut(G).

What are the main problems in group theory?

Example: Classify all groups of a given order **up to isomorphism**. That is, prove a theorem of the form:

Theorem

If G is a group with $|G| = n$, then G is isomorphic to exactly one of the following groups:

- *(blah)*
- *(blah)*
- *etc.*

This kind of list quickly becomes way too long to be interesting. However, we can still make notable progress using the idea of **coset**.

After Ch. 7: Can answer above for all $n<12$ except $n=8$.

Cosets

Definition

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

$$aH = \{ah \mid h \in H\} \quad \text{L coset}$$
$$Ha = \{ha \mid h \in H\} \quad \text{R coset}$$
$$aHa^{-1} = \{aha^{-1} \mid h \in H\}$$

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

$aH =$ L coset

$Ha =$ R coset

Examples

integers mod 24 that are rel prime to 24, op'n mult.

$G = U(24)$, $H = \{1, 5, 7, 11\}$. $a = 13$, $b = 5$

$aH = 13\{1,5,7,11\}$

$= \{13\cdot 1, 13\cdot 5, 13\cdot 7, 13\cdot 11\}$

$= \{13, 17, 19, 23\} = Ha$ b/c G abelian

~~$G = S_4$, $H = \langle(1\ 2\ 3)\rangle = \{\epsilon, (1\ 2\ 3), (1\ 3\ 2)\}$.~~

$bH = 5\{1,5,7,11\}$

$= \{5\cdot 1, 5\cdot 5, 5\cdot 7, 5\cdot 11\}$

$= \{5, 1, 11, 7\} = H$

In general, if a in H, then aH = H.

$G = S_4$, $H = \langle (123) \rangle$
$= \{\varepsilon, (123), (132)\}$

$a = (14)$

$\leftarrow$ coset aH

$aH = (14) \cdot \{\varepsilon, (123), (132)\}$
$= \{(14)\varepsilon, (14)(123), (14)(132)\}$
$= \{(14), (1234), (1324)\}$

$Ha = \{\varepsilon, (123), (132)\} \cdot (14)$
Rcoset Ha

$= \{\epsilon\cdot(14), (123)(14), (132)(14)\}$

$= \{(14), (1423), (1432)\} \boxed{\neq aH}$

$b = (12)$

$bH = (12)\cdot\{\epsilon, (123), (132)\}$

$= \{(12), (12)(123), (12)(132)\}$

$= \{(12), (23), (13)\}$

$Hb = \{\epsilon(12), (123)(12), (132)(12)\}$

$= \{(12), (13), (23)\} = bH$

In a nonabelian group, sometimes aH=Ha, sometimes not.

Cosets via equivalence relations

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

Definition

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

Theorem

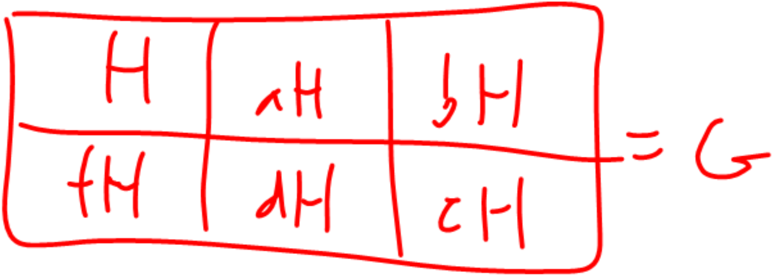
$\sim$ is an equivalence relation on G.

Cosets are equivalence classes

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

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

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

$$f(ah) = bh.$$

We prove that f is a bijection:

Lagrange's Theorem

Theorem

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

Proof: Combine previous two slides into one picture:

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

Corollary

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

Two consequences of Lagrange's Theorem

Corollary

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

Corollary

If $|G|$ is prime, then G is 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

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