Math 128A, Wed Sep 30

- 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 for Mon: Ch. 7.
- PS05 due Mon.
- Problem session Fri Oct 02, 10:00–noon on Zoom.

Finding cycle shapes of permutations in S_6 and A_6

In A_6?

6	$(abcdef)$ (-1)	no
5+1	$(abcde)(f)$ $+1$ $+1$	yes
4+2	$(abcd)(ef)$ -1 -1	yes
4+1+1	$(abcd)(e)(f)$	no
⋮		

Remember: Even length cycles are odd perms (-1)
Odd length cycles are even perms $(+1)$

# of these: $\left(\dfrac{6\,(\text{for } a)\cdot 5\cdot 4\cdot 3}{4}\right)\left(\dfrac{2\cdot 1}{2}\right)$

$\div 4$: $(1234)=(2341)=(3412)=(4123)$

Example of an isomorphism

opn in G

opn in $\overline{G}$

Definition

A **isomorphism** from G to $\overline{G}$ is $\varphi : G \to \overline{G}$ such that

1. For all $a, b \in G$,

$$\varphi(\underbrace{ab}) = \underbrace{\varphi(a)\varphi(b)}$$

and

2. φ is a bijection (one-to-one and onto).

Example: Suppose $\overline{G} = \langle a \rangle$ is a multiplicative cyclic group of order 60 (i.e., ord$(a) = 60$). Define $\varphi : \mathbf{Z}_{60} \to \overline{G}$ by

$$\varphi(i) = a^i.$$

Opns:

$\mathbb{Z}_{60}$: +

$\overline{G}$: ·

Thm: φ is an isomorphism.

Well-defined:

Ambiguity in formula for phi: If the number i is only specified (mod 60), is there only one possible meaning for a^i?

Yes: Thm from Ch.4 that says: If ord(a) = 60, then a^i = a^j if and only if i=j (mod 60). So in particular, if i=j (mod 60) , then a^i=a^j, which means that the RHS of the formula is unambiguous.

One-to-one: WTS: Different inputs give different outputs.
= Same output must come from same input.

(A) $i, j \in G$, $\varphi(i) = \varphi(j)$

$a^i = a^j$

Thm Ch4 $\Rightarrow$ $i \equiv j \pmod{60}$

(C) $i = j$ in $\mathbb{Z}_{60}$

any 1-to-1 pf.

Onto: WTS: Every element of codomain gets hit as an output.

Ⓐ $y \in \bar{G}$ So $y = a^n$ for $n \in \mathbb{Z}$

Pick $x = n \pmod{60}$

Then $\varphi(x) = a^n = y$

Ⓒ $\varphi(x) = y$

Ⓒ $\exists\, x \in G$ s.t. $\varphi(x) = y$

any onto pf.

Want $a^x = y = a^n$

Operation-preserving:

Ⓐ $i, j \in G$

$\varphi(i+j) = a^{i+j}$ ← equal!

$\varphi(i)\varphi(j) = a^i a^j$

Ⓒ $\varphi(\overbrace{i+j}^{\text{in } \mathbb{Z}_{60}}) = \overbrace{\varphi(i)\varphi(j)}^{\text{in } \bar{G}}$

Example

Let $\overline{G} = \{3n \mid n \in \mathbf{Z}\}$, operation $+$.
Define $\varphi : \mathbf{Z} \to \overline{G}$ by $\varphi(n) = 3n$.

1-to-1 (A) $n, k \in Z$, $\varphi(n) = \varphi(k)$

So $3n = 3k$

$k - 12$

(C) $n = k$

onto (A) $y \in \overline{G}$. By defn, $y = 3n$, $n \in Z$

Pick $x = n$

Then $\varphi(x) = 3n = y$

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

(C) $\exists x \in G$ s.t. $\varphi(x) = y$

op pres = homom prop

(a) $n, k \in \mathbb{Z}$

$\varphi(n+k) = 3(n+k)$

$\varphi(n)+\varphi(k) = 3n+3k$ yay!

Note: phi is a homomorphism b/c of distributive law.

(c) $\varphi(n+k) = \varphi(n)+\varphi(k)$ ☺

Example? (Non ex)

$\mathbf{R}^*$ is nonzero reals, operation $\times$.

Define $\varphi : \mathbf{R}^* \to \mathbf{R}^*$ by $\varphi(x) = 3x$. Is φ an isomorphism?

$$\varphi(xy) = 3xy$$

$$\varphi(x)\varphi(y) = (3x)(3y)$$

Not homom. (not op-preserving)

Cayley's Theorem

Really saying: Every group is a group of symmetries of itself as a geometric object.

Theorem

Every group G is isomorphic to a permutation group on the set G.

Sketch of proof: Define $T_g : G \to G$ by

(For $g \in G$)

$$T_g(x) = gx.$$

Let $\overline{G} = \{T_g \mid g \in G\}$, operation composition. Can show that each T_g is a permutation and that $\overline{G}$ is a group.
Now define $\varphi : G \to \overline{G}$ by

$$\varphi(g) = T_g.$$

To prove φ is an isomorphism, we need to:

1. φ 1-to-1
2. φ onto
3. $\varphi(gh) = \varphi(g)\varphi(h)$ i.e.

Ie, WTS: $T_{gh} = T_g \circ T_h$

In book: This is the interesting part.

How and why are isomorphic groups the same?

Theorem

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

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

~~Proof of one~~ of those preserved properties

List

φ preserves:

identity

powers

orders of elts

"kth roots"

subgps, subgp lattice

center

being cyclic

being abelian

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?

$\mathbb{Z}_{10}$ abelian

D_5 non-abelian

so not isom.

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

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:

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

Cosets

Definition

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

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

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

Examples

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

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

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: