Math 128A, Wed Sep 09

- 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 Mon: Ch. 4.
- Outline for PS03 due 11pm, complete PS03 due Mon Sep 14.
- Next problem session Fri Sep 11, 10:00–noon on Zoom.
- Zoom proctoring rehearsal Mon Sep 14. Details over the weekend, but have blank paper ready and be ready to turn on your camera on Mon.
- **Exam 1 moved to Mon Sep 21**, to cover Chs. 1–4 and PS01–03.

Error in PS03

missing

In Problem 5, definition of $N(a)$ should be:

$$N(a) = \left\{ g \in G \,\middle|\, gag^{-1} = a^n \boxed{\text{and } g^{-1}ag = a^k} \text{ for some } n, k \in \mathbf{Z} \right\}.$$

Corrected version now up on website

soon.

Other questions?

Method for proving that $H \subseteq G$ is a sub**group** of G

Suppose H has a definition of the form $\{\text{foo} \mid \text{bar}\}$. To apply the Two-Step Subgroup Test:

- Write out steps 0, 1, 2 as if-then statements and set up **A**ssumptions and **C**onclusions.
- Rewrite **A** and **C** using $\{\text{foo} \mid \text{bar}\}$ definition of H.
- Fill in the middle.

The cyclic subgroup generated by $a \in G$

Theorem

G a group, $a \in G$. Then

Elts of H have form a^n

$$H = \langle a \rangle = \{a^n \mid n \in \mathbf{Z}\}$$

Where n is some integer

is a subgroup of G.

Step 0

(Often, to show that H is nonempty, easiest thing to check is that e is in H. Here, we would show that by starting with observation n=0 is an integer.)

$n=1$ is an integer

So $a^1 \in H$

$\checkmark$ There's something in H

Step1

Assume: $a^c, a^d \in H \mid c, d \in \mathbb{Z}$

$$(a^c)(a^d) = a^{c+d}$$

B/c $c+d \in \mathbb{Z}$

Conclusion: $a^c a^d \in H$

Step 2: A: $x \in H$ So $x = a^m$ $H = \{1\}$

$x^{-1} = a^{-m}$

So, b/c $-m \in \mathbb{Z}$

C: $x^{-1} \in H$

The centralizer of $a \in G$

Theorem

G a group, $a \in G$. Then (centralizer = everything that commutes with a)

$$C(a) = \{g \in G \mid ga = ag\}$$

is a subgroup of G.

$\boxed{\text{Pf}}$ 0. Consider $e \in G$.

$ea = ae$ (identity)

So $e \in C(a)$

C $C(a) \neq \emptyset$.

$$C(a) = \{g \in G \mid ga = ag\}$$

1. (A) $x, y \in C(a)$

So $x \in G$, $xa = ax$ $\star$

$y \in G$, $ya = ay$ $\star$

So $\star \Rightarrow xay = axy$ mult by y on right

$xya = axy$ by $\star$

So $xy \in G$, $(xy)a = a(xy)$

(C) $xy \in C(a)$

2. (A) $x \in C(a)$

$C(a) = \{g \in G \mid ga = ag\}$

So $x \in G$, $xa = ax$

mult by x^{-1} on left

$x^{-1}xa = x^{-1}ax$

$a = x^{-1}ax$

mult by x^{-1} on right

$ax^{-1} = x^{-1}axx^{-1} = x^{-1}a$

So $x^{-1} \in G$, $x^{-1}a = ax^{-1}$

(C) $x^{-1} \in C(a)$

How can we understand a class of groups completely?

To understand a class of groups completely, we must be able to:

- List all elements of that class of groups.
- For G in that class, write down elements of G, compute the product of two elements, and understand the order of a given element of G.
- For G in that class, list all subgroups of G.

Goal of Ch. 4 is to understand cyclic groups completely.

$a^i a^j = a^{i+j}$

Review: Defn of cyclic groups

G gp, $a \in G$

Defn of cyclic subgroup $\langle a \rangle$? Defn of cyclic group?

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

G cyclic means:

(v1) $\exists a \in G$ s.t. every $p \in G$ is equal to a^n for some $n \in \mathbb{Z}$.

(v2) $G = \langle a \rangle$ for some $a \in G$.

So every element of a cyclic group looks like: a^n, $n \in \mathbb{Z}$. (a fixed)

When is $a^i = a^j$?

WLOG (w/o loss of generality)

$i \geq j$

Theorem 4.1

G a group, $a \in G$.

$|a|$

- *If* $\text{ord}(a) = n < \infty$, *then* $a^i = a^j$ *exactly when* $i = j \pmod{n}$.
- *If* $\text{ord}(a) = \infty$, *then* $a^i = a^j$ *exactly when* $i = j$.

Proof. Suppose $\text{ord}(a) = n < \infty$ and $a^i = a^j$.

mult by a^{-j} on L

$a^{i-j} = a^j a^{-j} = e$

Let $k = i - j$, so $a^k = e$.

Division by n $\Rightarrow$ $k = qn + r$ $\quad 0 \leq r < n$

$\neq$

~~So $i = j \pmod{n}$.~~

But!

$$e = a^k = a^{qn} a^r$$
$$= (a^n)^q a^r$$
$$= a^r$$

$\boxed{a^n = e}$

So $a^r = e$, and $0 \leq r < n$.

n is smallest pos int s.t. $a^n = e$,

so r can't be > 0. So $r = 0$.

So $k = qn \Rightarrow k \equiv 0 \pmod{n}$

$\Rightarrow i - j \equiv 0 \pmod{n}$

Corollaries to $a^i = a^j$ theorem

$\Rightarrow i \equiv j \pmod{n}$

G a group, $a, b \in G$, $n = \operatorname{ord}(a)$.

Corollary

$a^k = e$ if and only if n divides k.

Corollary

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

Second Corollary shows that $\langle a \rangle$ is "the same as" the cyclic group $\mathbf{Z}_n$, i.e., all cyclic groups of a given order are "the same". (But we first have to define what it means to be "the same"....)

What is $\langle a^k \rangle$ like?

Theorem

G a group, $a \in G$, $\mathrm{ord}(a) = n < \infty$. Then

$$\left\langle a^k \right\rangle = \left\langle a^{\gcd(n,k)} \right\rangle, \qquad \mathrm{ord}(a^k) = \frac{n}{\gcd(n,k)}.$$

Proof. Suppose $\mathrm{ord}(a) = n < \infty$, $k > 0$, $d = \gcd(n,k)$, $n = qd$.

So $\langle a^k \rangle \subseteq \langle a^d \rangle$.

So $\langle a^d \rangle \subseteq \langle a^k \rangle$.

Corollaries to $\langle a^k \rangle$ theorem

G a group, $a, b \in G$, $\operatorname{ord}(a) = n < \infty$.

Corollary

$\langle a^k \rangle = \langle a^j \rangle$ if and only if $\gcd(n, k) = \gcd(n, j)$.

Corollary

a^k generates $\langle a \rangle$ if and only if $\gcd(n, k) = 1$.