Math 128A, Mon Sep 14

- 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. 4. Reading for Wed Sep 16: Ch. 5.
- Outline for PS04 (not written yet) due Wed Sep 23.
- Next problem session Fri Sep 18, 10:00–noon on Zoom: Exam review
- Zoom proctoring rehearsal **TODAY**.
- **Exam 1 moved to Mon Sep 21**, to cover Chs. 1–4 and PS01–03.

Exam rehearsal at 10:05am

2 pieces blank paper

1. Please have a clear workspace ready where you can write.
2. Please have some kind of camera ready. First position the camera so I can see your face, and later so I can see your workspace.
3. Please have the Gradescope assignment page "Exam rehearsal" open and ready to go.

Questions?

Exam format

$\boxed{\text{One page notes}}$

Types of questions:

- Computations
- Proofs
- True/false with justification

For last type, if true, write "True" for full credit; if false, e.g.:

> *(True/False) If G is a group, with its operation written multiplicatively, and $a, b \in G$, then $(ab)^{-1} = b^{-1}$.*

Need to write "False" and give justification.

False If $G = \mathbb{R}^*$, $a = 2$, $b = 3$, then $(ab)^{-1} = \frac{1}{6}$, $b^{-1} = \frac{1}{3}$.

Or False since $(ab)^{-1} = b^{-1}a^{-1}$, $b^{-1} \neq b^{-1}a^{-1}$ unless $e = a^{-1}$, i.e., if $a = e$.

Ch. 4: Understand cyclic groups completely

Defn of cyclic subgroup: $\langle a \rangle =$

$$\{a^n \mid n \in \mathbb{Z}\}$$

Defn of cyclic group: G cyclic

$\iff G = \langle a \rangle$ for some $a \in G$

So every element of a cyclic group looks like: a^n for some $n \in \mathbb{Z}$

$\langle a \rangle$

When is $a^i = a^j$? (and consequences)

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

Theorem

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

Corollary 1

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

Corollary 2

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

Both Cors

~~Second Corollary~~ show~~s~~ 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"....) Ch. 6

Example

Suppose $a \in G$, $\mathrm{ord}(a) = 12$.

$a^3 = a$^3

List all elements of $\langle a \rangle$.

$= \{a^1, a^2, \ldots, a^{11}, a^{12} = e\}$

$7 \equiv -5 \pmod{12}$

For which i is $a^i = a^{-5}$?

$31 \equiv -5 \pmod{12}$

$i = \{ \quad -17, -5, 7, 19,$

$\cdots = a^{-29} = a^{-17} = a^{-5} = a^7 = a^{19} = a^{31} = \cdots$

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

(as subgp of $\langle a \rangle$)

$\boxed{\langle a^k \rangle \leq \langle a \rangle}$

Theorem

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

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

Example: For $k<n$, $\gcd>1$, k not divisor

Given

$n = 27$ $\qquad$ $k = 18$

$\gcd(n,k)=9$

we have

$$\langle a^{18} \rangle = \left\langle a^k \right\rangle = \langle a^9 \rangle$$

$$\mathrm{ord}(a^k) = \frac{n}{\gcd(n,k)} = \frac{27}{9} = 3$$

$\boxed{\text{ord}(a)=27}$

Check

Thm 2

$(a^{18})^1 = a^{18} \neq e$ b/c 27 doesn't divide 18

$(a^{18})^2 = a^{36} \neq e$ b/c 27 doesn't divide 36

$= a^9$

$(a^{18})^3 = a^{54} = e$ b/c 27*2 = 54

✓

order 3

Thm

$|\langle a \rangle| = 27$ (given) and $\langle a \rangle = \{a^1, a^2, \ldots, a^{26}, e\}$

"Proof" by examples

$15 \equiv 3 \pmod{12}$

If $\operatorname{ord}(a) = 12$, what are all elements of $\langle a^5 \rangle$?

$\gcd(5,12)=1$

$= \{a^5, a^{10}, \underset{a^{15}}{\overset{\parallel}{a^3}}, a^8, \underset{a^{13}}{\overset{\parallel}{a}}, a^6, a^{11}, \underset{a^{16}}{\overset{\parallel}{a^4}}, a^9, a^2, a^7, a^{12} = e\}$

$\parallel$

$\langle a \rangle$, in diff order

If $\operatorname{ord}(a) = 12$, what are all elements of $\langle a^9 \rangle$?

$\gcd = 3$

$= \{a^9, a^6, a^3, e\}$

If $\operatorname{ord}(a) = 4$, what are all elements of $\langle a^3 \rangle$?

$\boxed{\bmod 4}$

$\div 3$

$= \{a^3, a^2, a^1, e\}$

Useful exercise: Pick n, k, k<n, gcd(n,k)=1 and compute powers of a^k until you get e (like a^5 for ord(a)=12).

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

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

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* $\gcd(n, k) = 1$.

Example: Suppose $\text{ord}(a) =$

What are all of the generators of $\langle a \rangle$?

Fundamental Theorem of Cyclic Groups

Theorem

Every subgroup of a cyclic group is cyclic. Also, if $\operatorname{ord}(a) = n$*, then the subgroups of* $\langle a \rangle$ *are precisely the subgroups* $\langle a^d \rangle$*, where* d *is some divisor of* n*.*

Sketch of proof: If $H \leq G = \langle a \rangle$ and H is nontrivial (contains some element $\neq e$), let d be the smallest positive integer such that $a^d \in H$.

Key point: Using division by d with remainder, we can show that $H = \langle a^d \rangle$ and also that d divides n.

Example

Let $\text{ord}(a) = n =$
Subgroups of $\langle a \rangle$:

Elements of order d in a cyclic group

Definition

$\varphi(d) =$ number of elements of $\{1, \ldots, d\}$ that are relatively prime to d.

Suppose $G = \langle a \rangle$, $n = \text{ord}(a)$, d divides n.

- Every element of order d in G generates a subgroup of order d.
- By Fund Thm, G has exactly one subgroup H of order d.
- H has $\varphi(d)$ generators.

So

Theorem

If $G = \langle a \rangle$, $n = \text{ord}(a)$, d divides n, then G has exactly $\varphi(d)$ elements of order d.

Number of elements of order d in **any** finite group G

No longer assuming G is cyclic, just that G is finite.

- Every element of order d in G generates a cyclic subgroup of order d.
- Each cyclic subgroup of G of order d has $\varphi(d)$ generators.

So

$$\text{elts of order } d \Rightarrow \text{cyclic subgps of } G \text{ of order } d$$

is a $\varphi(d)$-to-1 correspondence. Therefore:

Theorem

G a finite group. The number of elements of G of order d is a multiple of $\varphi(d)$.