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

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

- 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 blankpaper

- 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

Types of questions:

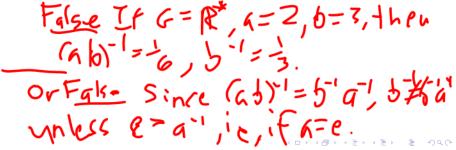
- Computations
- Proofs

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.



Ch. 4: Understand cyclic groups completely

Defn of cyclic subgroup: $\langle a \rangle =$ fa' nEZY

Defn of cyclic group: G Cyclic G=>G=<a>fir some a EG

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

$$G$$
 a group, $a, b \in G$, $n = ord(a)$.
Theorem

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

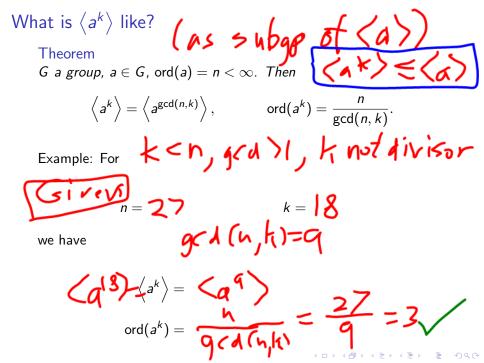
Corollary **7**

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

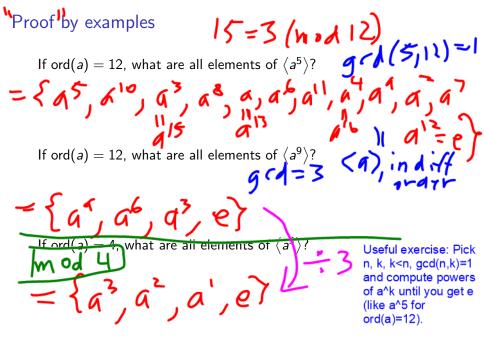
Second Corollary shows that $\langle a \rangle$ is "the same as" the cyclic group \mathbf{Z}_n , i.e., all cyclic groups of a given order are "the same". (But we first have to define what it means to be "the same"....)

Example

8=83 Suppose $a \in G$, ord(a) = 12. List all elements of $\langle a \rangle$. $= \{a', a', \dots, a'', a'' = e\}$ 7=-5(m112) 31=-5(mid 12) For which *i* is $a^i = a^{-5}$? $I = \{ -17, -5, 7, 19, \\ \cdots = a^{29} = a^{19} = a^{-5} = a^{7} = a^{19} = a^{11} = \cdots$



[ord(a)=27] $\frac{Check}{a^{b}} = a^{18} \neq e^{b/c 27 \operatorname{doesn't divide 18}}$ $(q^{18})^{2} = q^{36} \neq e^{b/c 27 \operatorname{doesn't} \operatorname{divide} 36}$ $(q^{(S)}) = q^{S+} = e^{b/c 27^{*}2} = 54$ (Given) and (Given) (Given)



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 $\operatorname{gcd}(n, k) = \operatorname{gcd}(n, j)$.

Corollary

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

Example: Suppose 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 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 $\operatorname{ord}(a) = n =$ 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 $G = \langle a \rangle$, $n = \operatorname{ord}(a)$, 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 $G = \langle a \rangle$, $n = \operatorname{ord}(a)$, 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 φ(d) generators.
 So

```
elts of order d \Rightarrow cyclic subgps of G 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 $\varphi(d)$.