Math 128A, Mon Aug 31

- 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 Wed: Ch. 3.
- Outline for PS02 now due **Wed Sep 02**. Completed due Wed Sep 09, after Labor Day
- Next problem session Fri Sep 04, 10:00–noon on Zoom.

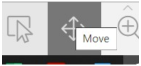
How to use Limnu

Limnu is the online whiteboard software we'll use to collaborate during problem sessions, office hours, and class.

- Each day we'll start with a new board, sometimes preloaded with materials. The board will have an address of the form:

  `http://go.limnu.com/random-words`

  The board will usually be shared as a clickable link, either in chat or in an email before problem sessions.
- Click on the link or type the address into a browser on a machine where you have a touchscreen (e.g., smartphone or tablet). If this is your first time using limnu, you may have to set up an account first.
- Draw and write! And by default, stay in "Move" mode:



Uniqueness of the identity

Theorem

G a group. If e, e' are both identity elements for G, then $e = e'$.

Proof. ~~Consider ee'.~~

A e, e' id in G

Consider

$e' = ee' = e$ b/c e' is id

b/c e is id

C $e = e'$.

Cancellation (Sudoku) property

LEFT

Theorem $a, b, c \in G$ a' an inv of a

G a group. If $ab = ac$, then $b = c$.

(I.e., same entry can't appear twice in the row of Cayley table corresponding to a.)

Proof. (A) Suppose $ab = ac$.

mult ~~div by~~ by a' ~~a~~ on left

$a'ab = a'ac$

id

$eb = ec$ inv

(C) $b = c$

Solve

$7x = 7(33)$

mult ~~div~~ by $1/7$ ~~by 7~~

$\cancel{\frac{7x}{7}} = \cancel{\frac{7(33)}{7}}$

$x = 33$

Uniqueness of inverses

Theorem Point: We are then OK in saying THE inverse of a, writing a^{-1}.

G a group, $a \in G$. If b and b' are both inverses of a, then $b = b'$.

Proof. Suppose $ab = e$ and $ab' = e$.

$ab = ab'$ mult on left by b

$bab = bab'$ $ba = e$

$eb = eb'$ identity

$b = b'$

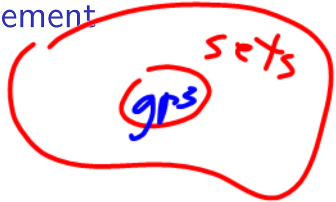
cancel

Corollary (Socks-Shoes) Remember: ab is do b first, so a = shoes, b= socks.

G a group, $a, b \in G$. $(ab)^{-1} = b^{-1}a^{-1}$ shoes off first.

Proof. Consider $(ab)(b^{-1}a^{-1})$. try this yourself!

Order of a group vs. order of an element



Suppose G is a group.
Defn: The **order** of G is:

# of elts of G
(aka cardinality of G)

Defn: Suppose $a \in G$. The **order** of a is:

SMALLEST $n > 0$ such that $a^n = e$

Brute force method to find the order of a: Look at a^1, a^2, a^3, ... until you get a^n=e. First n that produces a^n=e is the order of a.

(If no such n exists, we say that the order of a is infinite.)

Examples of the order of an element

$U(10) = \{1, 3, 7, 9\}$, op'n: mult (mod 10)

Note: 1 is identity of U(10) b/c 1(a) = a in the integers, so 1(a) = a (mod 10).

Compute orders by brute force

Order of 1 in U(10): $1^1 = 1$ ✓ order(1) = 1

Note: $1^2 = 1, 1^3 = 1, 1^4 = 1, \ldots$ ← why smallest $n > 0$

so $a^n = e \not\Rightarrow n$ is order of a.

Order of 3 in U(10):

$3^1 = 3 \neq 1, 3^2 = 9 \neq 1, 3^3 = 3(3^2) = 3 \cdot 9 = 7 \neq 1$ (mod 10)

$3^4 = 3(3^3) = 3(7) = 1$ ✓ order(3) = 4

$$3 = 3$$

$$3^2 = 9$$

$$3^3 = 3(3^2) = 3(9) = 27 = 7 \pmod{10}$$

$$3^4 = 3(3^3) = 3(7) = 21 = 1 \pmod{10}$$

Two numbers are equal (mod 10) when they differ by a multiple of 10.
So 21 = 1 (mod 10) because 21 - 1 = 20 = 2(10).
Arithmetic "mod 10" means: Set 10 = 0. So 21 = 2(10) + 1 = 2(0) + 1 = 1.

Subgroups

G a group.

Definition

If $H \subseteq G$ is itself a group under operation of G, we say H is a **subgroup** of G. Write $H \leq G$ (as opposed to just $H \subseteq G$).

Theorem (Enhanced Two-Step Subgroup Test)

Suppose $H \subseteq G$. TFAE:

- *H is a sub***group** *of G.*
- *The following all hold:*
  0. *H is nonempty:* H has an elt in it, e.g. $e \in H$
  1. *H is closed under operation:* If $a, b \in H$, then $ab \in H$.
  2. *H is closed under inverses:*

If $a \in H$, then $a^{-1} \in H$.

__Nonex__ $H = \{1, 3\}$ in $U(10)$.

$H \not\leq U(10)$ b/c

$3 \cdot 3 = 9 \notin H$ so H not closed.

Inv of 3 in $U(10)$ is 7, so H not closed under ${}^{-1}$.

Example of a subgroup

Theorem

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

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

is a subgroup of G.