Math 128A, Wed Aug 26

- 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. 2. Reading for Mon: Ch. 3.
- PS01 due tonight, 11pm; PS02 outline due Mon Aug 31.
- Next problem session Fri Aug 28, 10:00–noon on Zoom.

but I am usually flexible with deadlines if you need a little time. (Exception: Please get outlines in on time.)
After Labor Day, outlines due on Wed, complete on Mon.

Last: D_n, the symmetries of a regular n-gon

let bi-gons be bi-gons

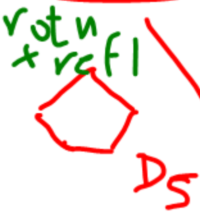
See completed table for D_6....

Go google "Escher patterns"

Q: What is the "right" abstract framework for understanding things like D_n?

D_n = dihedral group of order 2n

A: **Groups**.



Group of symmetries of the n-armed "pinwheel" is called C_n, the cyclic group of order n. Contains exactly the rotations of (360/n) degrees.

For Ch. 1 #24, ans to each is C_n or D_n for some appropriate value of n.

Problem looks like this

Ans: $C_3 D_4$ . . .

Ans looks like this

Definition of group

Not part of defn of a group to have ab=ba always. If ab=ba for all a,b in G, we say G is Abelian; but if ab is not equal to ba for some a,b in G, then we say G is nonabelian.

A **group** is:

- A set G, the **elements** of the group; and
- A **binary operation** on G, i.e., a way of defining a times b, or just ab, for any $a, b \in G$;

(or sometimes a+b, depending on context)

Such that:

- Associativity

$\forall a, b, c \in G \quad (ab)c = a(bc)$

- Identity

(Think of e as being like 1; German ein.)

$\exists e \in G$ s.t. $\forall a \in G \quad ea = a = ae$.

- Inverses

(Write this b as $b = a^{-1}$)

$\forall a \in G, \exists b \in G$ s.t. $ab = e = ba$

Formal definition of binary operation:

A binary operation on G is a function * : G x G -> G.

Instead of writing *(a,b), write a*b.

Or: If * is multiplication-like, write ab.

Or: If * is addition-like, write a+b.

Can rewrite axioms of a group in any of these notations:

Eg., assoc becomes (a+b)+c = a+(b+c)

Examples coming from numbers

$0+a=a=a+0$

- Integers $\mathbf{Z}$ under $+$

Assoc: (a+b)+c = a+(b+c); Identity: 0; Inverse of a is -a.

- Nonzero rationals $\mathbf{Q}^*$ under multiplication

Assoc, identity, inverses look like mult versions. $\left(-\frac{5}{3}\right)^{-1}=-\frac{3}{5}$

- Integers mod n: $\mathbf{Z}_n = \{0, \ldots, n-1\}$ under addition (mod n)

Notation looks like (Z,+)

- Integers relatively prime to n under multiplication (mod n)

Notn is usual multiplicative notn. Called $U(n)$

$U(8) = \{1, 3, 5, 7\}$

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5				
7				

etc.

$3 \cdot 3 = 9 = 1 \pmod 8$

$3 \cdot 5 = 15 = 7 \pmod 8$

$3 \cdot 7 = 21 = \quad \pmod 8$

Non-examples coming from numbers

G
$\shortparallel$

- Odd integers under $+$

I.e., binary operations must be closed.

$3+5=8 \notin G$, so $+$ not bin. op.

- Integers $\mathbf{Z}$ under $-$

$(1-5)-7=-4-7=-11$

$1-(5-7)=1-(-2)=3$

- Associative operation but no identity:

Set = pos ints, op = $+$

This set has no identity element.

- Associative, identity, not inverses:

Set = Z, operation = multiplication: This does not have inverses for all elements, so is not a group. (Note: Some elements, namely, +/- 1, have inverses, but not all do, so inverse axiom fails.)

An important example from linear algebra, and variations

Recall: A square matrix has an inverse iff det not 0.

$\exists$ id:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

The group $GL(2, \mathbf{R})$:

- Set is 2×2 matrices A with $\det A \neq 0$
- Operation is matrix multiplication

Can change $\mathbf{R}$ to $\mathbf{Q}$, $\mathbf{C}$, $\boxed{\mathbf{Z}_p \text{ (p prime)}}$.

Opn is matrix mult, arith (mod p)

Add extra condition $\det A = 1$, get $SL(2, \mathbf{R})$.

From linear algebra, you know that $AB \neq BA$ in general: These are **non-Abelian** groups.

Dihedral groups D_n

Look at Cayley table for D_6. Where can you see:

- Identity?
- Inverse?
- What other patterns do you notice?

Uniqueness of the identity

Theorem

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

Cancellation (Sudoku) property

Theorem

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.)

Uniqueness of inverses

Theorem

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