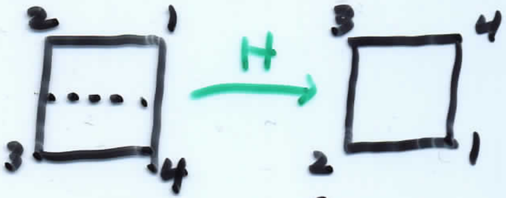
ED

Previously in Math 103a

Symmetries of squares / Groups

Rotation 90°



Reflection across a bisector

These symmetries form a group

i.e. a set G w/ binary operation

$$G \times G \longrightarrow G \qquad (a,b) \longmapsto ab$$

satisfying existence of identity, inverses, and associativity.

Group of symmetries is non abelian

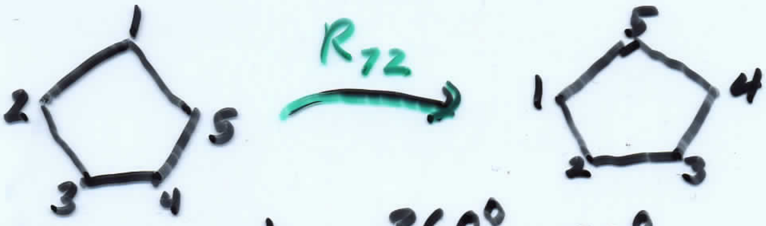
i.e. $\exists\ a, b \in G$ for which $\boxed{ab \neq ba}$.

In today's episode: more groups!

More symmetries

For regular n-gon, the set of rotations & reflections (flips) forms a group with $2n$ elements: n rotations, n flips, written $\boxed{D_n}$

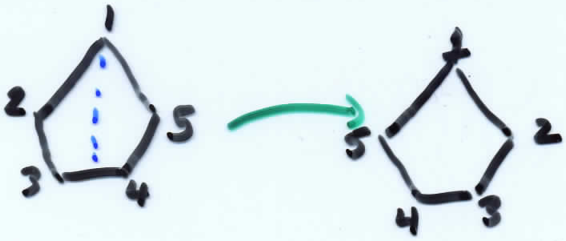
Ex: $n=5$



Rotation by $\frac{360^\circ}{5} = 72^\circ$

Other rotation by $2\times 72^\circ$, $3\times 72^\circ$, $4\times 72^\circ$

Flips



Every vertex corresponds to 1 flip e.g. vertex 4

1-1 correspondence between flips & vertices

5 flips, 5 rotations

Ex: $n=6$

Rotation by $\frac{360^\circ}{60} = 60^\circ$, $2\times 60^\circ$, $3\times 60^\circ$, $4\times 60^\circ$, $5\times 60^\circ$

flips similar to square e.g.

Examples of groups & "nongroups"

1. $\mathbb{Z}$, $\mathbb{Q}$ = rationals, $\mathbb{R}$ = all reals, $\mathbb{C}$ = complex
   with addition as operation, Group!
   0 = identity, $-a$ = inverse of a.

2. $\mathbb{Z}$, operation = multiplication
   Identity = 1, but no numbers
   except ± 1 have inverses.
   Not a group!

3. $\mathbb{Q}^*$ = nonzero rationals (also written $\mathbb{Q}\setminus\{0\}$)
   operation = mult., 1 = identity
   $$\left(\frac{p}{q}\right)^{-1} = \frac{q}{p}$$ Group!

   Also $\mathbb{Q}^+$ = positive rationals is a group
   (product of 2 positive is positive,
   inverse is positive)

   $\mathbb{Q}^-$ = negative rationals not a
   group
   Many reasons!

4. All nonzero irrational numbers. Not a
   group! Not closed under multiplication.
   (other reasons, too)
   for multiplication

5. $\mathbb{R}^n$ or all $j \times k$ matrices with entries in $\mathbb{R}$, operation = addition of corresponding entries. Group! Matrices may be identified with $\mathbb{R}^{j \times k}$. Identity = $(0, \ldots, 0)$.

6. $\mathbb{R}^*$ or $\mathbb{Q}^*$ or $\mathbb{C}^*$ (* means 0 is removed) group with operation = mult.

These groups are all abelian.

Groups of matrices with matrix multiplication are often nonabelian

Recall: a square matrix A is invertible $\Longleftrightarrow$ $\det A \neq 0$

7. $GL(2, \mathbb{R})$ = all 2×2 matrices with real entries & $\det \neq 0$. Identity = $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Inverse of A is

$$A^{-1} = \frac{1}{\det A}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}, \text{ where } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$\det A = ad - bc$. Group! Nonabelian, since

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

8. $M(2,\mathbb{R})$ all 2×2 real matrices
$\boxed{\text{not a group}}$ under mult.
A has inverse $\Longleftrightarrow$ $\det A \neq 0$

Important example.

$\mathbb{Z}_n$ is not a group under mult since $[0]$ has no inverse. How about $\mathbb{Z}_n^*$?

Check it out $\boxed{\mathbb{Z}_3^*} = \{[1],[2]\}$

$[2][2] = [4] = [1]$ $\qquad$ $[2]^{-1} = [2]$.

$[1][2] = [2]$ $\qquad$ $[1] =$ identity

group!

Try $\boxed{\mathbb{Z}_4^*} = \{[1],[2],[3]\}$

$[2][2] = [4] = [0]$ no good!

not closed under mult

& $[2]$ has no inverse.

not a group!

Try $\boxed{\mathbb{Z}_6^*} = \{[1],[2],[3],[4],[5]\}$

$[2][3] = [6] = [0]$ no good

not a group.

ES

Def. For $n>1$, let $\boxed{U(n)=\{[m] : \gcd(m,n)=1\}}$

For simplicity, use the notation

1 for $[1]$
2 for $[2]$
$\vdots$
$n-1$ for $[n-1]$

Thm. $U(n)$ is a group under multiplication.

will prove later.

Ex: $n=9$, $U(9)=\{1,2,4,5,7,8\}$

Write Cayley table for mult.

	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8				
5	5	1				
7	7	5				
8	8	7				

	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

Pf of Thm.

show $U(n)$ is closed under mult.

$$\left.\begin{array}{l} \gcd(a,n)=1 \\ \gcd(b,n)=1 \end{array}\right. \Longrightarrow \gcd(ab,n)=1$$

by prime factoriz

Inverses? Recall linear comb.

$\exists$ s, t such that

$$as + nt = \gcd(a,n) = 1$$

$\therefore$ $as \bmod n = 1$

check that $\gcd(s,n)=1$

do it!

Cor If p is prime, then $\mathbb{Z}_p^*$ is a group under multiplication.

$$|\mathbb{Z}_p^*| = p-1 \quad - \quad 1, 2, 3, 4, \ldots, p-1$$

More groups!

Ex. $SL(2,F)$, $F=\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{Z}_p$, p prime

$$= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in F,\ \det = 1 \right\}$$

Special linear group

closed under mult since

$$\det(AB) = (\det A)(\det B)$$

even $SL(2,\mathbb{Z})$ is a group.