D6

Problem set 2 is on the web,
due Monday, January 23

---

Previously in Math 203a:

Equivalence relation on a set $S$

$a, b \in S$ write $a \sim b$ if $a$ is equiv. to $b$

i.e. $(a,b) \in R$

$$[a] = \{x \in S : x \sim a\}$$

equivalence class of $a$

Ex: $S = \mathbb{Z}$, fix $n > 1$

put $a \sim b \iff a \bmod n = b \bmod n$

set of equiv. classes =

$$\{[0], [1], \ldots, [n-1]\}$$

A peek ahead to groups.

Put $\boxed{\mathbb{Z}_n} = \{ [0], [1], \ldots, [n-1] \}$ & define

"addition" by $\underline{[j] + [k] := [j+k]}$

Need to check this is well-defined

i.e. if $[j] = [j']$ & $[k] = [k']$

then $[j+k] = [j'+k']$

Otherwise, this makes no sense!

We know

$$(j \bmod n + k \bmod n) \bmod n = (j+k) \bmod n$$

$$\& \; (j' \overset{\shortparallel}{\bmod} n + k' \overset{\shortparallel}{\bmod} n) \bmod n = (j'+k') \bmod n$$

$$\therefore (j+k) \bmod n = (j'+k') \bmod n$$

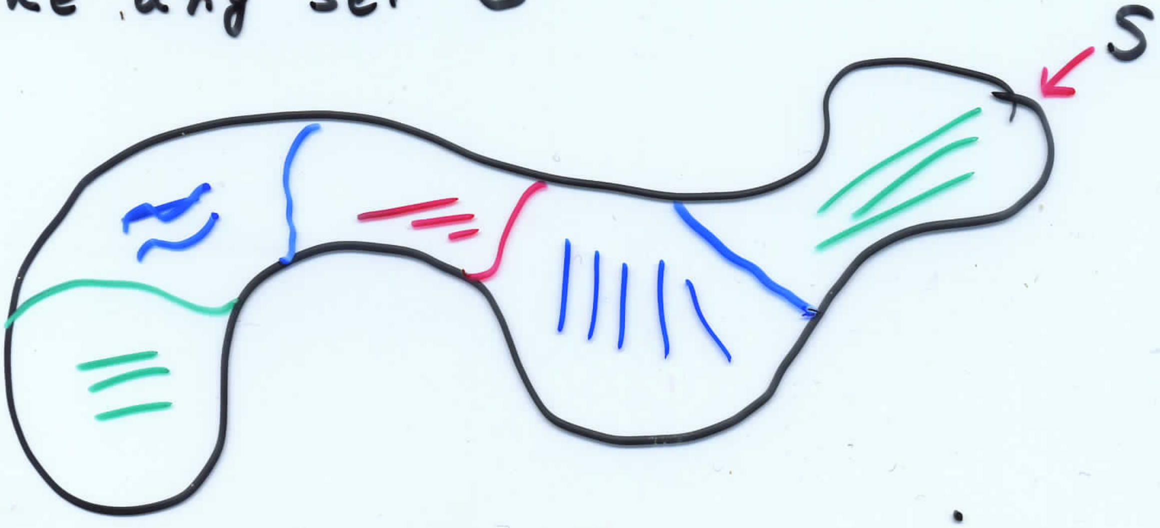
i.e. $\boxed{[j+k] = [j'+k'] \text{ if } [j] = [j'] \; \& \; [k] = [k'].}$

$\mathbb{Z}_n$ is a set with "addition" & is an example of a group (not yet defined)

We need to review a bit more before continuing with groups.

# Another way to think about equiv. classes

Take any set $S$



Divide it into disjoint pieces,
called a partition of $S$

(Could be finitely many or $\infty$ many pieces)

$$S = \bigcup_{\alpha} S_\alpha, \quad S_\alpha \cap S_\beta = \phi, \quad \alpha \neq \beta$$

Then for $x, y \in S$, put $x \sim y$ if $x \in S_\alpha \Leftrightarrow y \in S_\alpha$

i.e. $x$ and $y$ are in same piece of $S$

1 to 1 correspondence

Partitions of $S$ $\longleftrightarrow$ Equivalence relations on $S$

$$\xrightarrow{\checkmark}$$

$$\longleftarrow$$

$$S = \bigcup [a]$$

all equivalence classes.

# Review of stuff about functions

A, B sets. a function (or map or mapping) from A to B is an assignment $\varphi$

$$\boxed{A \ni a \longmapsto \varphi(a) \in B}$$

$\varphi$ is 1-1 if $\varphi(a) = \varphi(a') \Longrightarrow a = a'$

$\varphi$ is onto B if $\forall\, b \in B \ \exists\ a_b \in A$ s.t. $\varphi(a_b) = b$

a bijection from A to B is a map $\varphi : A \longrightarrow B$ that is 1-1 and onto.

These notions depend on A & B. Ex: $\mathbb{R}$ = reals. Put $\varphi(x) = x^2$ $\quad \varphi : \mathbb{R} \longrightarrow \mathbb{R}$ is neither 1-1 nor onto

but $\quad \varphi : [0, \infty) \longrightarrow [0, \infty)$ is 1-1 & onto.

---

## Groups!

Def. A group is a set equipped with a binary operation i.e. a map

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

(written like multiplication)

satisfying

(i) (indentity) $\exists\ e \in G$ s.t. $\boxed{ea = ae = a}$ $\forall\, a \in G$.

(ii) (inverse) $\forall\, a \in G \ \exists\ a^{-1} \in G$ s.t. $\boxed{aa^{-1} = a^{-1}a = e}$.

(iii) (associativity) $\forall\, a, b, c \in G$,

$$\boxed{(ab)c = a(bc)}$$

**Ex.** $\mathbb{Z}_n$ Define $\mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$

If $a=[j]$ & $b=[k]$, put $ab=[j+k]$

Identity $= [0]$ since $[0+k]=[k]$

Inverse: For $a=[j]$, $a^{-1}=[n-j]$, $0 \le j < n$

Then $aa^{-1}=[j+n-j]=[0]=e$

Associativity: let $c=[\ell]$

Then $(ab)c = [(j+k)+\ell] = [j+(h+\ell)]$.

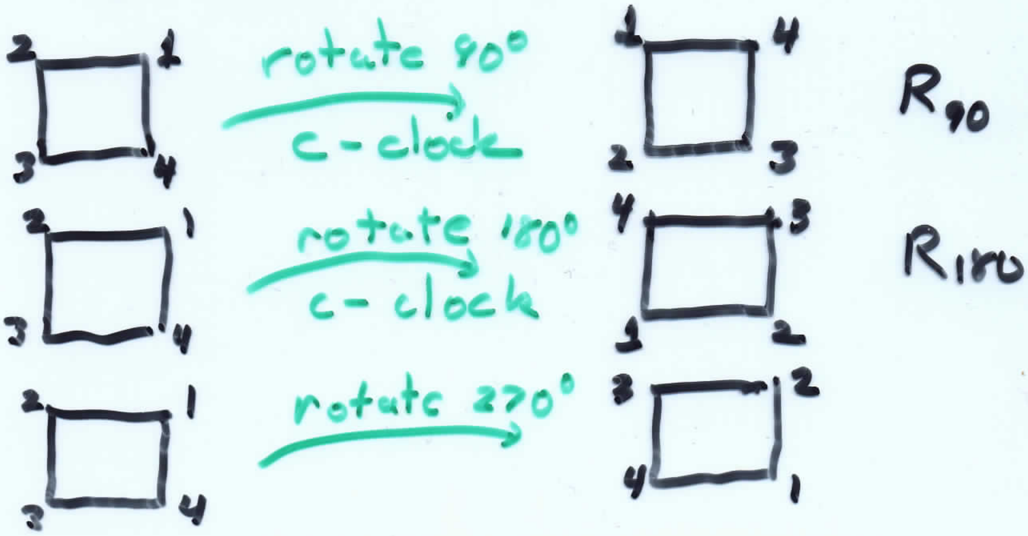
$\mathbb{Z}_n$ has a further property: $ab=ba$ $\forall\, a,b \in \mathbb{Z}_n$ (since $[j+k]=[h+j]$)

Def. If $ab=ba$ $\forall\, a,b \in G$, then $G$ is abelian.

---

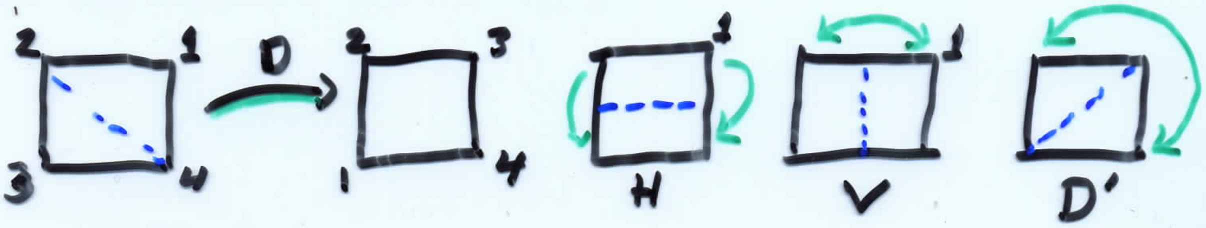
Some "natural" nonabelian groups are obtained as flips & rotations of a regular $n$-gon.

Take $n=4$; regular 4-gon = a square.



Identity = $R_0 = R_{360}$

Other symmetries are flips!

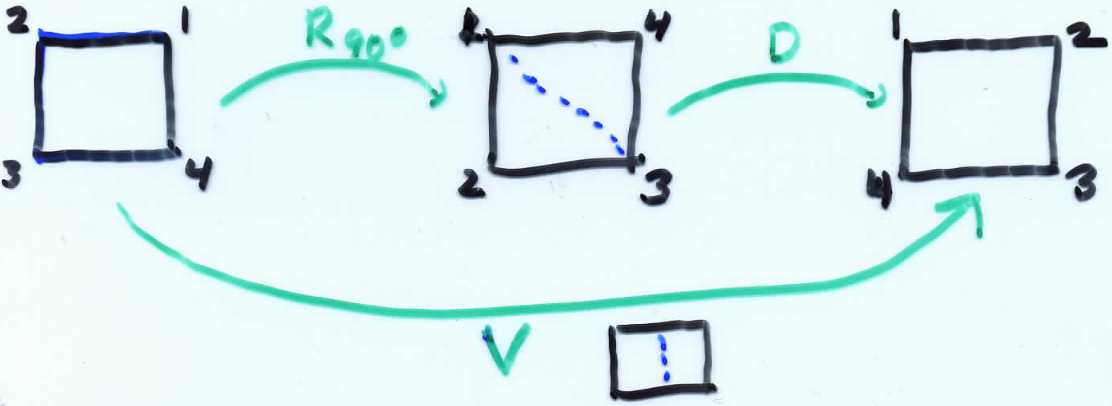


**Rotations**: numbers go c-clockwise

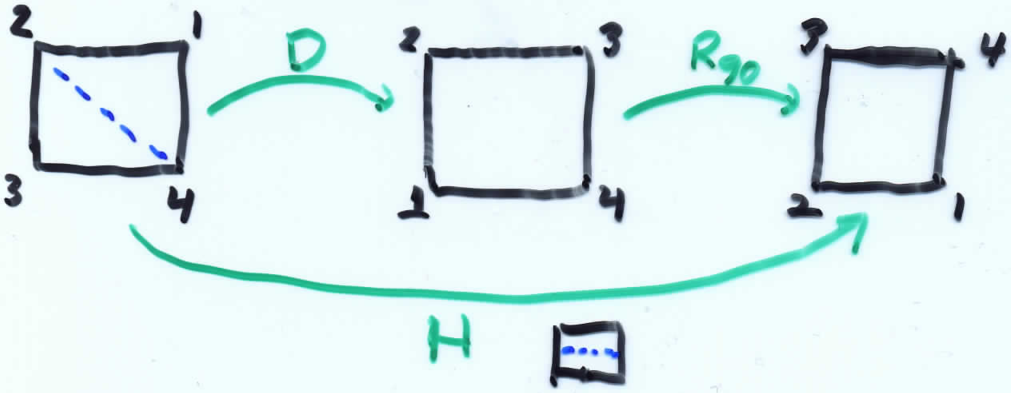
**Flips**: numbers go clockwise

4 Flips + 4 rotations = 8 symmetries

Interesting observation:



$\therefore D \cdot R_{90} = V$



so $DR_{90} \neq R_{90}D = H$

Observations: (Check them)

The composition of any 2 symmetries is again a symmetry.

① Composition of 2 rotations is a rotation.

② Composition of 2 flips is a rotation.

③ Composition of a flip & a rotation is a flip.

The set of flips & rotations of a square form a group with 8 elements, operation is composition of operators (which is associative)

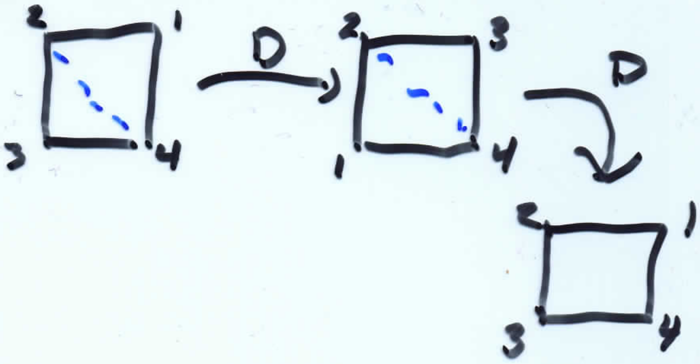
Check: Identity = $\boxed{R_0}$

Inverses: $\boxed{R_\alpha^{-1} = R_{360-\alpha}}$

($\alpha = 90, 180, 270,$ or $360$)

Any flip is its own inverse

e.g. $D \circ D = R_0$



This group is called $D_4$ non abelian