Group: A set G with binary operation satisfying

(a) Associativity $(ab)c = a(bc)$ a, b, c in G

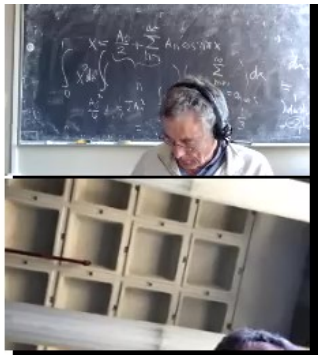
(b) Identity element: $ae = a = ea$ for all a in G

(c) Inverse: for all $a \in G$ there exists a b in G such that $ab = e = ba$

Associativity often follows from associativity for composition of functions:

Lemma: Let maps α, β, γ be given as $\alpha: A \to B$, $\beta: B \to C$, $\gamma: C \to D$ where A, B, C, D are sets

Then composition of functions is associativity i.e $\gamma(\beta\alpha) = (\gamma\beta)\alpha$



Proof Let $a \in A$

$$(\gamma\beta)\alpha\,(a) = (\gamma\beta)(\alpha(a)) = \gamma(\beta(\alpha(a)))$$

$$\gamma(\beta\alpha)\,(a) = \gamma((\beta\alpha)(a)) = \gamma(\beta(\alpha(a)))$$

✓

Some general properties of groups:

Question: group axioms $\Rightarrow$ existence of at least one identity element

↳ can there be more than one identity element?

Theorem Uniqueness of Identity

There is only one identity element in a group

proof. Assume e and e' are identity elements in a group G

$\Rightarrow$ $ae = a = ea$ for all a in G

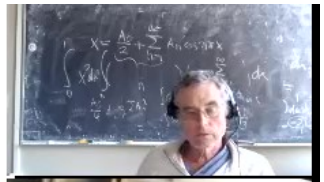
and $ae' = a = e'a$ " " " "

$a = e'$ $\quad$ $a = e$

$e'e = e'$ $\quad$ $e = e'e$

$e = e'e = e'$

$\Rightarrow e = e'$ ✓



Theorem Cancellation.

(i) $ba = ca \Rightarrow b = c$

(ii) $ab = ac \Rightarrow b = c$

Proof Let a' be the inverse of a

i.e. $a'a = e = aa'$

for (i): $ba = ca$ | multiply by a' from the right

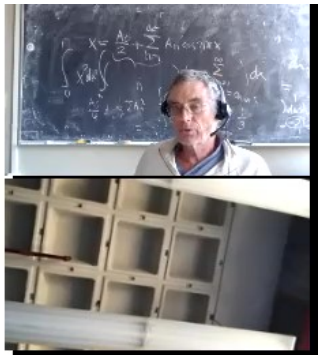
$baa' = caa'$

$\underbrace{baa'}_{=e} = \underbrace{caa'}_{=e}$

$be = ce$

$\Rightarrow b = c$

for (ii) do it yourself !



Theorem (Uniqueness of Inverse)

For each $a \in G$ there is exactly one inverse element.

Proof. Assume b and b' both are inverses of a

$$\Rightarrow \quad ba = e = ab$$

$$b'a = e = ab'$$

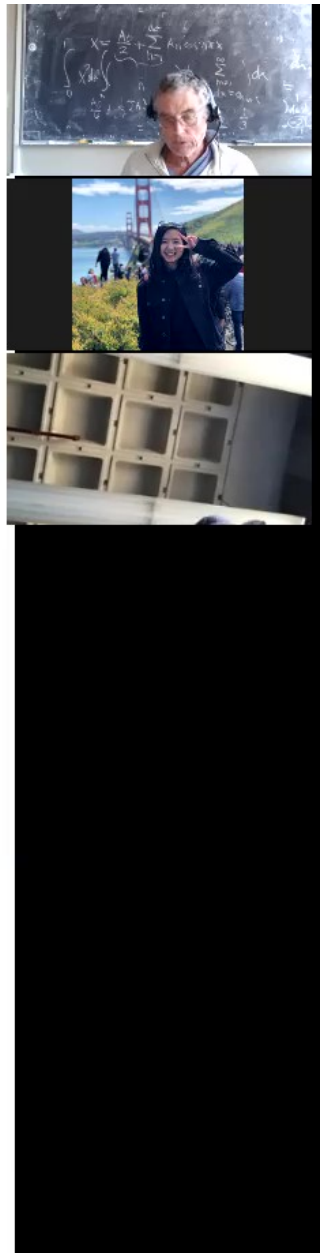
$$\Rightarrow \quad b = be = b(ab') = (ba)b' = eb' = b'$$

(associativity)

$$\Rightarrow \quad b = b'$$

✓

Remark: For given a we can talk about **the** inverse of a, usual notation a^{-1}.



More examples!

Chapter 1 Symmetries

Symmetry of a square

Question: given a square

how many ways are there to cut out the square and put it back?

corner P: ⟶ have four possibilities to place corner P | 4

corner W: ⟶ " two " " " " W | 2

(it needs to be adjacent to new position of P)

corner G ⟶ other adjacent corner | 1

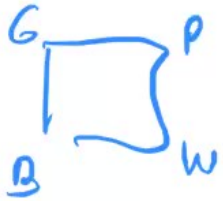
corner B ⟶ remaining corner | 1

⟶ have at most $4 \cdot 2$ possibilities

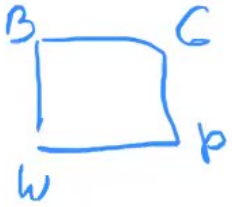
indeed there are 8 such possibilities

4 rotations

R_0 

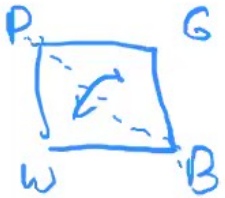
R_{90} 

↘ 90°

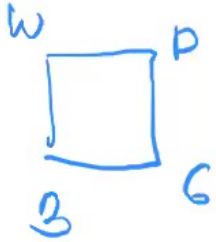
R_{180} 

R_{270} 

4 flips

S 

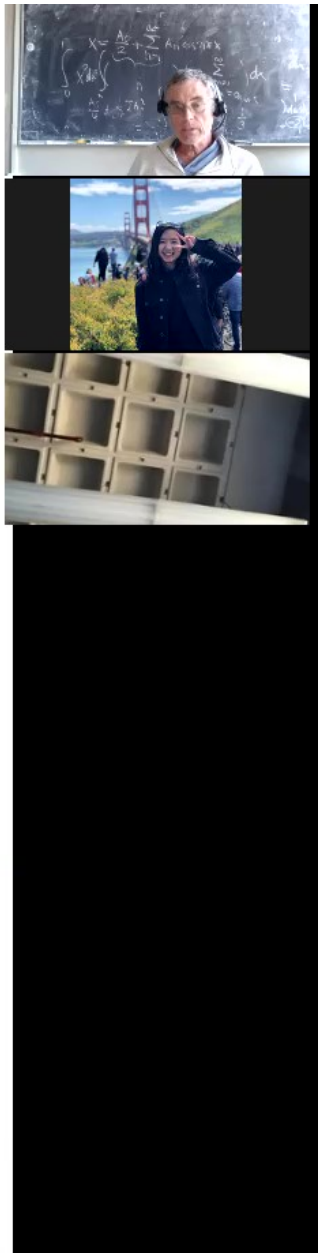
reflection at diagonal

R_{90} S 

reflect + rotate.

R_{180} S 

R_{270} S 



want to get a group

need an operation:

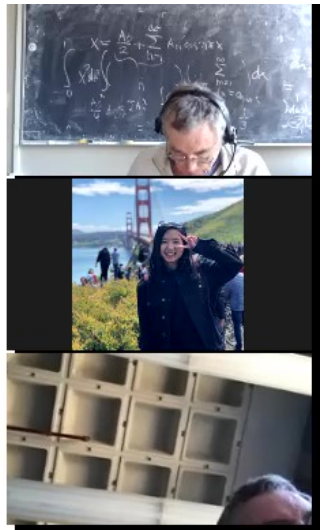
here: concatenation

applying one symmetry after another one

→ get new symmetry

- get associativity from our Lemma by viewing symmetries as maps from square to itself
- identity element: R_0
- inverse: of symmetry T = symmetry which puts $T(\square)$ back to its old position

e.g. $(R_{90})^{-1} = R_{270}$, ...



Recall: The symmetries of a square form a group with eight elements (operation: concatenation of maps)

This group is usually called the dihedral group D_4

Remark: D_4 is not Abelian!