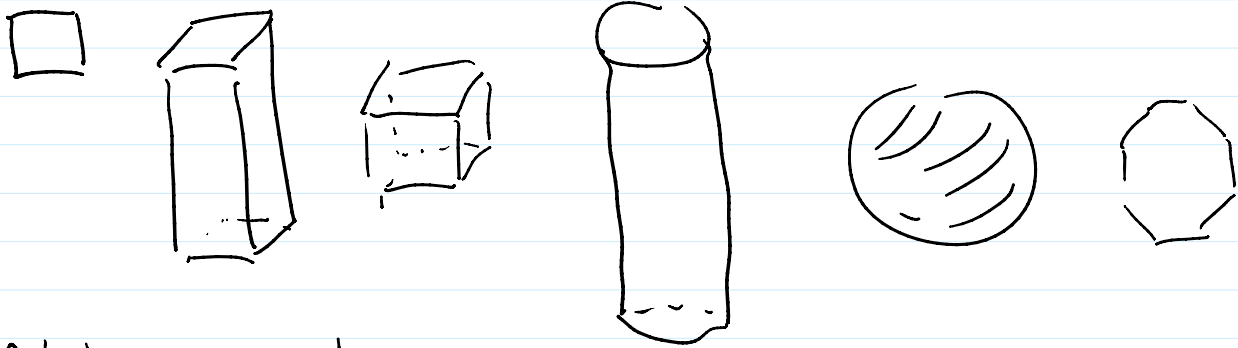
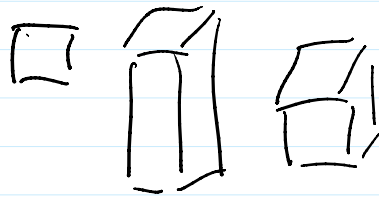


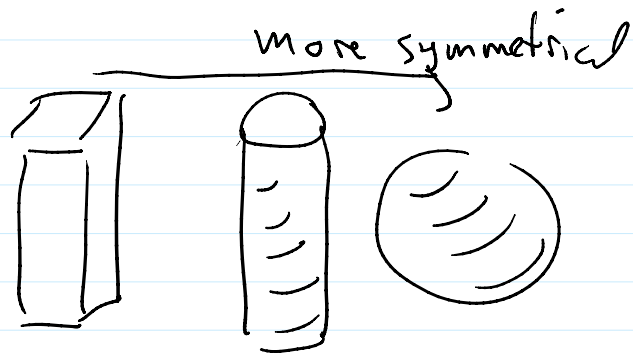
Consider the following shapes



All have symmetry



more symmetrical



The purpose of this course: to define and study groups

Groups: measure symmetry the way numbers measure size

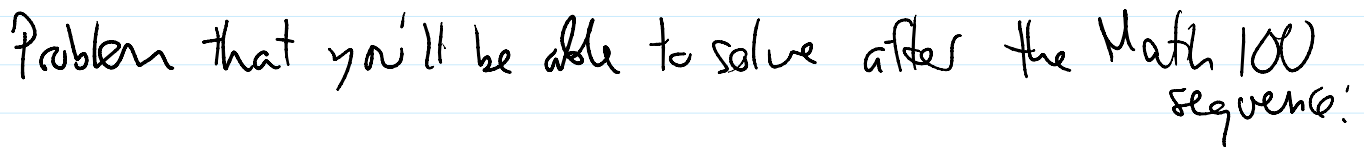
Given a straightedge (ruler w/o markings)

and a compass (tool to make circles)

what sort of objects can you construct?

Ex Can always bisect an angle





- ① You cannot trisect any angle w/ straightedge + compass
- ② Completely classify objects that you can construct

- A law of composition on a set S is a way of combining two elements of S to get a third elt of S .

$$\underbrace{S \times S} \rightarrow S$$

Examples

- addition of real numbers: $a, b \mapsto a+b$
- multiplication of real numbers: $a, b \mapsto a \cdot b$

$\left. \begin{array}{l} \text{addition of real numbers: } a, b \mapsto a+b \\ \text{multiplication of real numbers: } a, b \mapsto a \cdot b \end{array} \right\} \begin{array}{l} S = \mathbb{R} \\ \text{the} \\ \text{real \#s} \end{array}$

- $m_1, m_2 \mapsto m_1 \cdot m_2$, matrix multiplication
note! order matters

- composition of fns on a set M : $S = \{f: M \rightarrow M\}$

Problem $S = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$

1. $\frac{1}{2} \times 100 = 50$ 50

problem $\Rightarrow \{ (b \ a) : a, b \in \mathbb{R} \}$

Does matrix multiplication define a L.O.C. on S ?

Answer: Yes.

$$\underbrace{\begin{pmatrix} a_1 & b_1 \\ b_1 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ b_2 & a_2 \end{pmatrix}}_{\text{matrix multiplication}} = \begin{pmatrix} a_3 & b_3 \\ b_3 & a_3 \end{pmatrix} \quad \text{for some } a_3, b_3 \in \mathbb{R}$$

$$\begin{pmatrix} a_1 a_2 + b_1 b_2 & a_1 b_2 + b_1 a_2 \\ b_1 a_2 + a_1 b_1 & b_1 b_2 + a_1 a_2 \end{pmatrix} \quad \begin{aligned} a_3 &= a_1 a_2 + b_1 b_2 \\ b_3 &= a_1 b_2 + b_1 a_2 \end{aligned}$$

non example $S = \left\{ \begin{pmatrix} 1 & 2 \\ a & b \end{pmatrix} : a, b \in \mathbb{R} \right\}$

Q: Does addition define a L.O.C. on S ?

Ans: NO

$$\begin{pmatrix} 1 & 2 \\ a & b \end{pmatrix} + \begin{pmatrix} 1 & 2 \\ a' & b' \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ a+a' & b+b' \end{pmatrix} \leftarrow \text{not in } S$$

non-example $S = \mathbb{R}, a, b \mapsto \frac{a}{b}$.

not a L.O.C.: if $b = 0$ then $\frac{a}{0}$ is not defined

Q: How can I rectify this?

$S = \mathbb{R} \setminus \{0\}$, the nonzero real #'s

Now $a, b \mapsto \frac{a}{b}$ is a L.O.C.

Notation L.O.C. on set S . Usually denote the composition as $\cdot$, i.e. we'll write $a \cdot b$ or ab for the way of composing (a, b) .

Defⁿ A LOC is

- commutative if $a \cdot b = b \cdot a$ for all $a, b \in S$
- associative if $\underbrace{a(b \cdot c)}_{\substack{\text{first combine } b, c, \\ \text{then combine that with } a}} = \underbrace{(a \cdot b) \cdot c}_{\substack{\text{first combine } a \text{ w/ } b, \\ \text{then combine the result w/ } c}}$ for all $a, b, c \in S$

- Examples
- matrix multiplication is associative but not comm. i.e. $ab \neq ba$ in general if $a, b \in M_n(\mathbb{R})$
 - addition & multiplication of real #'s is both associative & commutative
 - composition of fns is assoc. but not comm.

Q: $a, b \in \mathbb{R} \setminus \{0\}$. Consider LOC $a, b \mapsto \frac{a}{b}$.
Is this associative?

Ans: $\frac{a}{\frac{b}{c}} \stackrel{?}{=} \frac{\frac{a}{b}}{c}$

() NO, division is not assoc.

LHS: $\frac{ac}{b}$

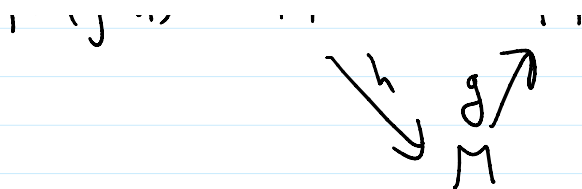
RHS: $\frac{a}{bc}$

only equal when $c = 1$ or -1

Composition of fns $f, g, h: M \rightsquigarrow M$

$$f \circ (g \circ h): M \xrightarrow{g \circ h} M \xrightarrow{f} M$$

$\searrow \quad \nearrow$
 $h \quad g$



$$(f \circ g) \circ h: M \xrightarrow{h} M \xrightarrow{f \circ g} M$$

$$\begin{array}{ccc} & & \\ & \searrow g & \nearrow f \\ & M & \end{array}$$

In both cases, $(f \circ (g \circ h))(m) = f(g(h(m)))$
 $= ((f \circ g) \circ h)(m).$

- comp of fns is associative.

S , set w/ loc

Suppose $a_1, a_2, a_3, a_4 \in S$

$$(a_1 a_2) a_3) a_4 ; \quad (a_1 (a_2 a_3)) a_4$$

$$(a_1 a_2) \cdot (a_3 a_4)$$

different ways of combining the elts a_1, a_2, a_3, a_4 .

If LOC on S is associative, then different ways above result in the same final elt of S

Ex Prove that if LOC on S is assoc, then

$$(a_1 a_2) a_3) a_4 = a_1 (a_2 a_3) a_4.$$

Pf: $(a_1 a_2) a_3) a_4 = (a_1 (a_2 a_3)) a_4$

↑ assoc. ↓

$$= a_1 ((a_2 a_3) \cdot a_4)$$

} assoc. again ✓

$$= a_1 ((a_2 a_3) \cdot a_4) \quad \checkmark$$

Propⁿ S set, w/ assoc. LOC. Then given any n elts w/ $n \geq 1$ then there is a unique way of combining the elts, $[a_1, a_2, \dots, a_n]$, w/ the following properties

- $[a_1] = a_1$
- $[a_1, a_2] = a_1 \cdot a_2$ the LOC
- $[a_1, \dots, a_n] = [a_1, \dots, a_i] \cdot [a_{i+1}, a_{i+2}, \dots, a_n]$
 $n \geq 2 \qquad 1 \leq i \leq n-1$

$$\forall a_1, a_2, \dots, a_n \in S$$

In other words, ^{with an} assoc LOC, the order of grouping elts does not matter. //

Pf: Induction on n . Clear 'if $n=1, 2$

$$\underline{n \geq 2} \quad \text{Define } [a_1, \dots, a_n] = [a_1, \dots, a_{n-1}] [a_n].$$

$$\underline{\text{Claim:}} \quad [a_1, a_2, \dots, a_n] = [a_1, \dots, a_i] \cdot [a_{i+1}, \dots, a_n]$$

To see this,

$$[a_1, \dots, a_n] = [a_1, \dots, a_{n-1}] [a_n]$$

$$= ([a_1, \dots, a_i] [a_{i+1}, \dots, a_{n-1}]) [a_n] \quad \text{by induction}$$

$$= [a_1, \dots, a_i] ([a_{i+1}, \dots, a_{n-1}] [a_n]) \quad \text{by assoc.}$$

$$= [a_1, \dots, a_i] \cdot [a_{i+1}, \dots, a_{n-1}, a_n] \quad \text{by defⁿ } \quad \square$$

Next tmr: Define a gp