$S = \{a, b\}$, operation (binary)

$\left.\begin{array}{l} x \in S \\ y \in S \end{array}\right\} \underbrace{x \circ y}$

$n = 2$

	O_1	O_2	. . .	O_{16}
$a \circ a$	a	a		b
$a \circ b$	a	a		b
$b \circ a$	a	a		b
$b \circ b$	a	b		b

$\left.\begin{array}{l} a \circ a \\ a \circ b \\ b \circ a \\ b \circ b \end{array}\right\}$ 4

$\circ$	a	b
a	$a \circ a = a$	a
b	a	b

For $n = 3$ elt sets

- no. rows $= n^2$

$n = 2$:

$n = 3 \quad S = \{a, b, c\}$

	O_1	O_2	O	$O_{19{,}000}$
$a \circ a$	a	b	$n = 3$	
$a \circ b$	.	a	$n = 3$	
$a \circ c$	.	.	3	
$b \circ a$	.	.	.	
$b \circ b$	.	.	.	
$b \circ c$	.	.	.	
$c \circ a$	.	.	.	
$c \circ b$	.	.	.	
$c \circ c$	a	a	.	

9

$x \circ y$

$3 \cdot 3 = 3^2 = 9$

n^2

$\underbrace{n \cdot n \cdots n}_{n^2} = n^{n^2}$

1 Group C_3

$n = 3: N = 3^{3^2} \sim 19{,}000$

$n = 4: N = 4 \times 10^9$

2 groups 4×10^9

Def^n: Group

A group is a set S with an operation $\circ$ such that these 4 criteria are satisfied.

$G = \langle S, \circ \rangle$

1. Closure : $a \circ b \in S \quad \forall\, a, b \in S$.
2. Associativity : $(a \circ b) \circ c = a \circ (b \circ c) \quad \forall\, a, b, c \in S$. (for all)
3. Identity : $\exists\, e \in S$ s.t. $a \circ e = e \circ a = a \quad \forall\, a \in S$.
4. Inverse : $\forall\, a \in S \ \exists\, a^{-1} \in S$ s.t. $a \circ a^{-1} = a^{-1} \circ a = e$.

$\in$: is an element of

$\forall$: for all

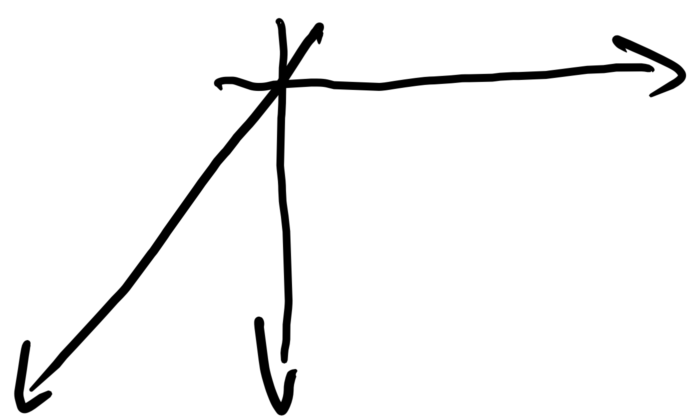
$\exists$: there exists.

s.t. such that.

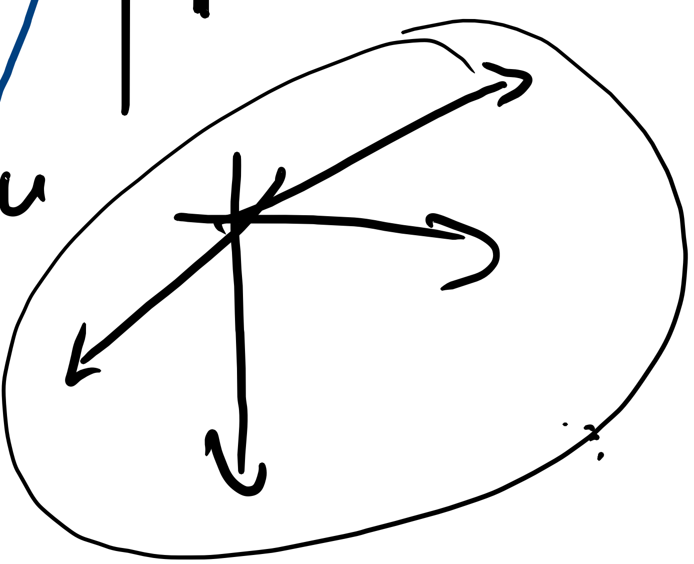
$\vdots$

$AA^{-1} = I \qquad 3 \cdot 3^{-1} = 3 \cdot \frac{1}{3} = 1$

·	a	b	c
a	a·a	a·b	a·c
b			
c			



$x \circ y \circ z = u$



Examples of Groups

1. Group of integers $\mathbb{Z}$ under $+$ $G = \langle \mathbb{Z}, + \rangle$.

closure: ✓   identity: ✓ 0

assoc. ✓   inverses: ✓ $n \in \mathbb{Z} \rightarrow$ inverse is $-n$ s.t. $n + (-n) = 0$.

1.a $\mathbb{Z}$ under $\times$ $\rightarrow$ group?

closure: ✓   identity: ✓

assoc.: ✓   inverses: $1 \cdot 1 = 1$ ✓ $\rightarrow$ $-1 \cdot -1 = 1$ ✓ $3 \rightarrow 3 \times \underset{\uparrow}{\_} = 1$ $\notin \mathbb{Z}$

• infinite

Cayley Table:

$+$	0	$+1$	-1	$+2$	-2	$\cdots$
0	0	$+1$	-1	$+2$	-2	
$+1$	$+1$	$+2$	0	3	-1	
-1	-1					
$+2$	$+2$					
-2	-2					
$\vdots$						

3. Define $Q^* = \{ q \in Q : q \neq 0 \}$

$G = \langle Q^*, \times \rangle$.

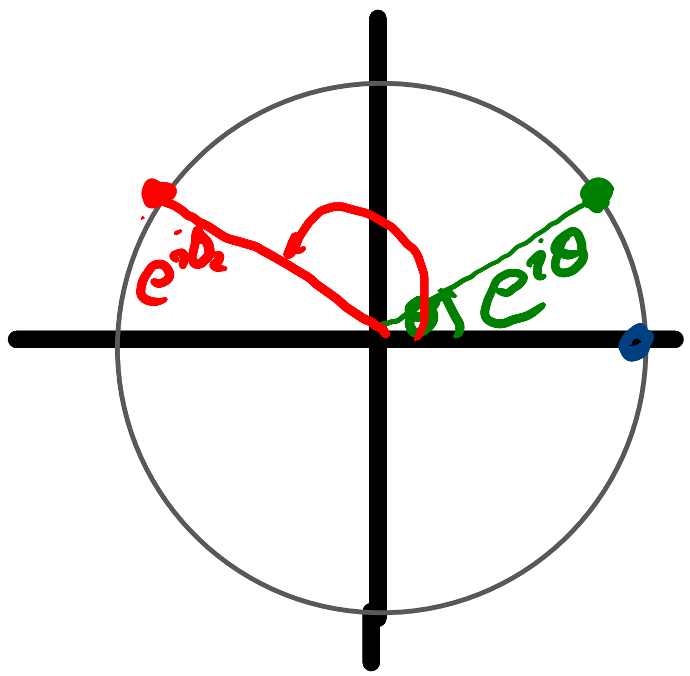
$3 \cdot \frac{1}{3} = 1$

• closure ✓   identity: 1

• assoc. ✓   inverses: ✓ $q \cdot \frac{1}{q} = 1$

$\frac{1}{q} = q^{-1}$

4.) Group of complex num's on the unit circle under $\times$.



Set $\{ e^{i\theta} : \theta \in \mathbb{R} \}$ mod 2π

- closure: $e^{i\theta_1} \cdot e^{i\theta_2} = e^{i(\theta_1 + \theta_2)} = e^{i\theta_3} \in G$
- assoc: ✓ $(e^{i\theta_1} \cdot e^{i\theta_2}) \cdot e^{i\theta_3} = e^{i((\theta_1 + \theta_2) + \theta_3)} = \cdot$
- identity: ✓ $e^{i\theta} \cdot \underline{1} = e^{i\theta}$
  $\underline{1} = \underline{e^{i0}}$: $e^{i\theta} \cdot e^{i0} = e^{i(\theta + 0)} = e^{i\theta}$.
- inverse: ✓ $e^{i\theta} \cdot \underline{e^{-i\theta}} = e^{i0} = e^{i(\theta + -\theta)} = e^{i0}$

- infinite set

5.) Finite group.

$S = \{2, 4, 6, 8\}$ $\quad$ $\circ$: mult^n mod 10.

$\circ$	2	4	6	8
2	4	8	2	6
4	8	6	4	2
6	2	4	6	8
8	6	2	8	4

abc mod 10

$=$ $((ab \bmod 10) \times c) \bmod 10$

Points:

1. closure ✓
2. assoc. ✓
3. identity: $a \times \_ = a$

   6
4. every row/col is a permutation of S.

   $S = \{2\ 4\ 6\ 8\}$ → rep'd 1

   → no elts missing.
5. inverse: ✓

   $2 \times \underline{8} = 6$: $2^{-1} = 8$, $4^{-1} = 4$, $6^{-1} = 6$, $8^{-1} = 2$
6. Commutativity ✓ ⟷ symmetric Cayley Table

$2 \times \underline{6} = 2$

$\_ \times a = a$

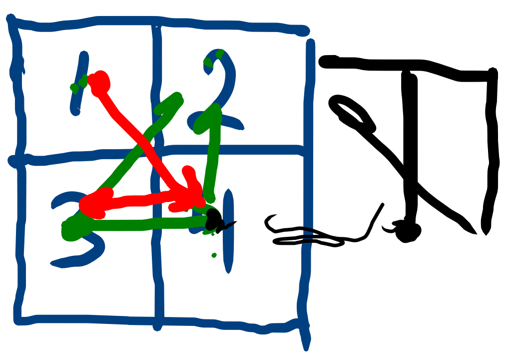
Commutative: $x \cdot y = y \cdot x$

$2 \cdot 4 = 8$ $\quad$ $8 \cdot 4 = 2$

$4 \cdot 2 = 8$ $\quad$ $4 \cdot 8 = 2$

4	8	2	6
8	6	4	2
2	4	6	8
6	2	8	4

D. Checkerboard Game.



- 4 moves I, V, H, D

$H \circ V = D$

$D \circ H = V$

$\circ$	I	V	H	D
I	I	V	H	D
V	V	I	D	H
H	H	D	I	V
D	D	H	V	I

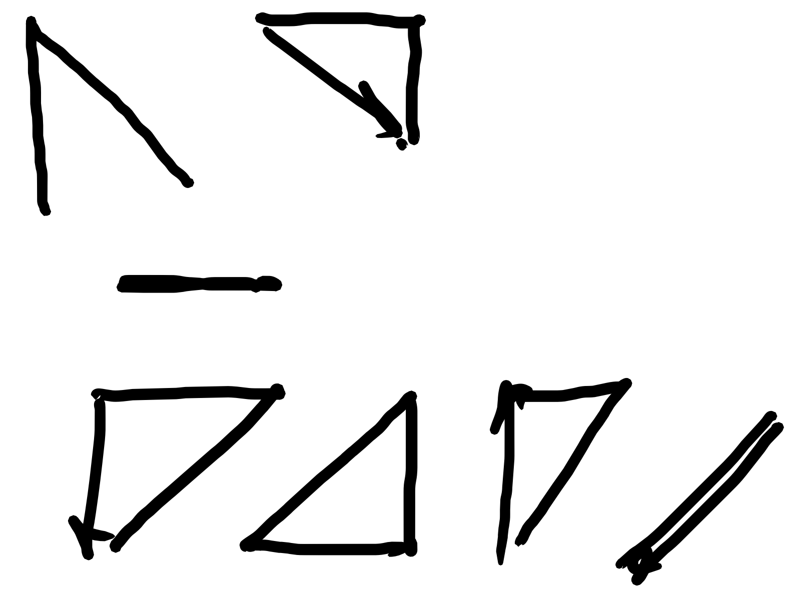
I = 6

V = 8

H = 4

2 = D

	6	8	4	2
6				
8				
4				
2				



4. Elementary Properties of Groups.

1. **Claim:** The identity elt in a group is unique → there's only one.

Proof: Assume there are two identities

e_1 & e_2.

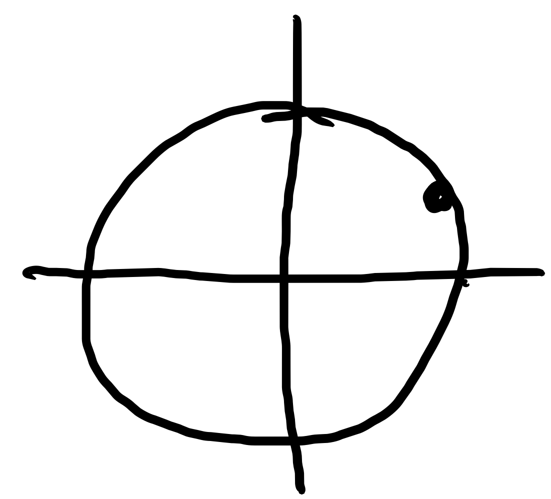
1. closure
2. assoc.
3. $\exists$ an identity
4. inverses exist.

Consider $e_1 \circ e_2$

Since e_1 is an identity → $\underline{e_1} \circ e_2 = e_2$

" e_2 " " " $e_1 \circ \underline{e_2} = e_1$

$$e_1 \circ e_2 = e_2$$
$$e_1 \circ e_2 = e_1$$
$$\boxed{e_1 = e_2} \checkmark$$



2. Uniqueness of Inverses.

Claim: inverses of elts are unique.

Proof: Pick $a \in S$.

Assume it has two inverses, a_1, a_2.

Consider: $a_1 a a_2$

$\rightarrow$ $(a_1 a) a_2 = (e) a_2 = a_2$ $\Rightarrow$ TS = BS

$a_1 (a a_2) = a_1 (e) = a_1$ $\Rightarrow$ $a_1 = a_2$

$\therefore$ the inverse is unique.

- closure
- $\rightarrow$ assoc'y
- identity.
- inverses.