Week 5

Last Friday, we started Chapter 4.

Def A group is a set G with an operation $*$ on G satisfying the following conditions.

(G0) If $a, b \in G$,

$$a * b \in G.$$

(G1) If $a, b, c \in G$

$$a * (\underbrace{b * c}_{\in G}) = (\underbrace{a * b}_{\in G}) * c$$

by (G0)

(G2) There is an element e in G (called the identity element)

s.t. $a * e = e * a = a \quad \forall a$

(G3) For every element a of G,
there exists b in G
s.t. $a * b = b * a = e$
This b is called the inverse of a.

It involves specify
a set G
& $*$ .....

If $(G, *)$ is a group
& furthermore satisfies

the condition

(G4) $a, b \in G$,

$$a * b = b * a ,$$

then we call it

an abelian group.

$(\mathbb{Q}, +)$ is a abelian group

$(\mathbb{Q} - \{0\}, \times)$ is a abelian group

$(\mathbb{Q}, \times)$ is <u>NOT</u> a abelian group.

abelian

$(\mathbb{Z}, +)$ is a group.

abelian

- identity element 0

(because $a+0=0+a$
$=a$)

- the inverse of a in $\mathbb{Z}$

is $(-a)$

$a+(-a)=(-a)+a=0$

$(\mathbb{Z}, \times)$ is not a group

identity element 1

$$a \cdot 1 = 1 \cdot a = a$$

$\times$

For example, there is no $b \in \mathbb{Z}$

s.t. $2 \cdot b = b \cdot 2 = 1$.

$(\{\text{the roots of } x^n - 1 \text{ in } \mathbb{C}\}, \times)$

We know every root of $x^n - 1$ in $\mathbb{C}$

is of the form $e^{2\pi i a/n}$

for some $a \in \mathbb{Z}$

Using Proposition 1,

$$a = n \cdot q + r$$

$$0 \leq r < n.$$

So $e^{2\pi i a/n} = e^{2\pi i r/n}$

$$= e^{2\pi i (nq+r)/n}$$

$$= (e^{2\pi i})^q \cdot e^{2\pi i r/n}$$

$$= 1 \cdot e^{2\pi i r/n}$$

$\{$ the roots of $x^n - 1$ in $\mathbb{C}^n \}$

$$= \{ e^{2\pi i 1/n}, e^{2\pi i 2/n}, \ldots, e^{2\pi i (n-1)/n} \}$$

$$e^{2\pi i r/n} \cdot e^{2\pi i s/n} = e^{2\pi i (r+s)/n}$$

OTOH,

$$\left(\left\{ \begin{array}{c} \text{the roots of} \\ x^n - 1 \text{ in } \mathbb{C} \end{array} \right\}, + \right)$$

is NOT a group!

In fact, (G0) does NOT hold!!

For example, if $n=2$,

$$(\{\pm 1\}, +)$$

$(-1)+(-1)$ is -2

but this is NOT a root

of $x^2 - 1$!

$\left(\{ \text{the } 2\times 2 \text{ matrices with entries in } \mathbb{R} \text{ with determinant} \neq 0 \}, \times \right)$

is a group but not abelian

(i.e. $AB \neq BA$)

the identity element : $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

the inverse of $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$a, b, c, d \in \mathbb{R}$

$\det A = ad - bc \neq 0$

is $\dfrac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

$$\parallel$$

$$A^{-1}$$

$(\mathbb{Z}_n, +)$ is a abelian group

$\parallel$

the set of equiv classes on $\mathbb{Z}$

w.r.t. $\equiv$ mod n

- the identity element $= [0]$

  because

$$[a] + [0] = [0] + [a]$$

$\parallel$ by definition $\qquad\qquad \parallel$

$$[a+0] \qquad\qquad [a]$$

$\parallel$

$$[a]$$

- the inverse of $[a]$

  is $[-a]$.

because

$$[a]+[-a] = [-a]+[a]$$

$$= [0]$$

by definition.

$(\mathbb{Z}_n, \times)$

- the identity element $[1]$

because $[a][1] = [1][a] = [a]$

- Can $[a]$ always have

$[b] \in \mathbb{Z}_n$ s.t.

$$[a][b] = [b][a] = [1]$$??

G3

Recall Theorem 12 which says

that $[a]$ has (multiplicative) inverse

$$\iff$$

$$\gcd(a,n) = 1.$$

In other words, of all the elements in $\mathbb{Z}_n$,

only $[a]$'s s.t. $\gcd(a, n) = 1$

pass (G3)

So $(\mathbb{Z}_n, \times)$ is NOT a group

$(\{[a] \text{ in } \mathbb{Z}_n \mid \gcd(a,n)=1\}, \times)$

is a group.

How about

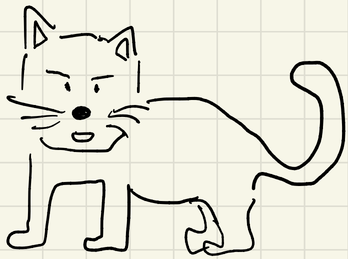
$(\mathbb{R}, *)$

where $*$ is defined as

$a, b \in \mathbb{R}$.

$a * b = a^2 b$. ?

Is this a group?



G1 does NOT hold.

$$a*(b*c) = a*(b^2c)$$

$$= a^2b^2c$$

$$(a*b)*c = (a^2b)*c$$

$$= a^4b^2c$$

G2 does not hold either!!

Look at typed up notes for why.

$$(\mathbb{Z}_{\geq 0}, *)$$

|

the set of positive integers

$$\forall\, a, b \in \mathbb{Z}_{\geq 1}$$

$$a * b = |a - b|.$$

Is this a group?

(G1) does <u>NOT</u> hold!

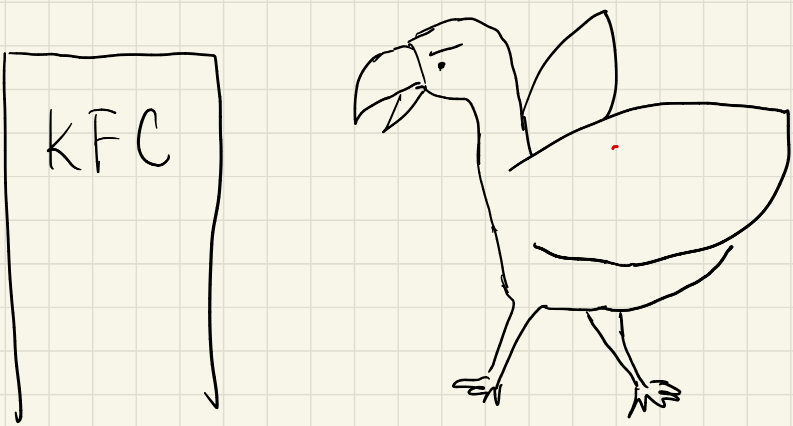
$$\underline{1} * (2 * 5) = 1 * 3$$

$$= 2$$

$$(1 * 2) * 5 = 1 * 5$$

$$= 4$$

So this fails (G1).



Let S be a non-empty set

$\mathrm{Sym}(S)$ be the set of

G "

bijective functions

$a : S \to S$

(bijective = injective

$s, t \in S$ $a(s) = a(t)$

& $\Rightarrow s = t$

Surjective

if $s \in S$, there exists

$t \in S$

s.t. $f(t) = s$)

$*$ is composition :

$$a, b \in \mathrm{Sym}(S)$$

$$a \circ b : S \to S$$

sending $s \in S$ to $\underline{\underline{a(b(t))}}$

In other words, it is the composition.

$$\begin{array}{ccccc} S & \xrightarrow{b} & S & \xrightarrow{a} & S \\ \downarrow & & \downarrow & & \downarrow \\ t & \longmapsto & b(t) & \longmapsto & a(b(t)) \end{array}$$

<u>Claim</u> $(G, *)$

$$=$$

$(\mathrm{Sym}(S), \circ)$

is a group.

(not abelian).

(G0) If $a, b \in \mathrm{Sym}(S)$,

then $a \circ b \in \mathrm{Sym}(S)$,

i.e. if a & b are bijective

then so is $a \circ b$.

Is $a \circ b$ injective?

To do this, suppose we have

$$(a \circ b)(s) = (a \circ b)(t)$$

(& aim at $s = t$)

By definition, we have

$$a(b(s)) = a(b(t))$$

Since a is injective,

$$b(s) = b(t).$$

Since b is injective,

$$s = t.$$

Is $a \circ b$ surjective?

To do this, let s' be an element in S'.

(I aim at showing that there is $s'' \in S$ s.t.

$$s' = (a \circ b)(s'')$$

$= a(b(s''))$

Since $\underline{\underline{a}}$ is surjective,

there exists $s' \in S'$ s.t. $\underline{\underline{a}}(s')$
$= s$.

Since $\underline{\underline{b}}$ is surjective,

there exists $s'' \in S''$ s.t.
$\underline{\underline{b}}(s'') = s'$

This s'' is what we are looking for.

Indeed

$$(a \circ b)(s'') = a(b(s'')) = a(s') = s'. \quad \square.$$

G2 $a, b, c \in Sym(S),$

$$a \circ (b \circ c) = (a \circ b) \circ c$$

$$[a \circ \underbrace{(b \circ c)}_{d}](s)$$

$$= [a \circ d](s)$$

$$= a(d(s))$$

$$= a((b \circ c)(s))$$

$$= a(b(c(s)))$$

$$= (a \circ b)(c(s))$$

$= \overline{[}(a \circ b) \circ c](s)$.

(G2) The identity element in $Sym(S)$ is the identity function $id : S \to S$ sending $s \in S$ to s itself.

I need to check

$$a \circ id = id \circ a = a$$

For example

$$(a \circ \mathrm{id})(s)$$

$$= a(\mathrm{id}(s))$$

$$= a(s)$$

Similarly $(\mathrm{id} \circ a)(s)$

$$= \mathrm{id}(a(s))$$

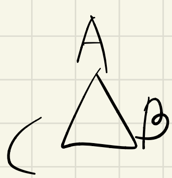
$$= a(s).$$

(G3) Look at notes.

This example formalises what we previously discussed as "symmetries of an equilateral triangle"

In the sense that

$S = \{$ the vertices $A, B, C \}$



& $Sym(S)$ was described completely in terms of reflections & rotations.

It's possible to look at

$S :=$ vertices of a tetrahedron etc.

Prop 14 (Elementary properties of a group).

Let $(G, *)$ be a group

- The identity element in G is unique. ($\leadsto$ (G2))

- Each element of G has a unique inverse. ($\leadsto$ (G3))

- If $a * b = a * c$, then $b = c$

- The inverse of $(a*b)$

is $b^{-1} * a^{-1}$.

the inverse of b

the inverse of a.

Let's prove the first statement.

Suppose we have

e & e'

satisfying

(G2) $e * a = a * e = a \quad \forall a$

$e' * a = a * e' = a \quad \forall a$

GOAL $e = e'$

Letting $a = e'$ in the first,

$$e * e' = e'$$

Letting $a = e$ in the second,

$$e * e' = e$$

Combining these two, we get

$$e = e'.$$