Math 3340
Spring 2021
Lecture #6

Groups! Yay!

19 Feb 2021
Lecture #6

Def A group $(G, *)$ is a set G, together with a binary operation $*$ on G satisfying:

0. closure: if $a, b \in G$, then $a * b \in G$
   (note: follows since $* : G \times G \to G$).

1. $*$ is associative: $\forall a, b, c \in G$
   $$a * (b * c) = (a * b) * c$$

2. $*$ has an identity $e \in G$: $\exists e \in G$ s.t. $\forall a \in G$
   $$a * e = e * a = a$$

3. every element has an inverse: $\forall a \in G$, $\exists a' \in G$ s.t.
   $$a * a' = a' * a = e$$

Def A group $(G, *)$ is called Abelian if $\forall a, b \in G$, $a * b = b * a$
(ie: commutative)

a' in ③ is usually written a^{-1}

ie: $a^{-1} \in G$, $a * a^{-1} = a^{-1} * a = e$.

Def ① $(G, *)$ is a finite group if $|G|$ (= # elem's of G) has $|G| < \infty$

② $|G|$ is called the order of $(G, *)$.

$|G|$ can be some non-negative number, or $|G| = \infty$, G is an infinite group.

Example Zoo land

① $(\mathbb{Z}, +)$

- closure ✓
- associativity ✓
- $e = 0$ $\quad 0 + a = a + 0 = a \quad \forall a$.
- if $a \in \mathbb{Z}$, its inverse is $-a$

$|\mathbb{Z}| = \infty$

$\mathbb{Z}$ is Abelian (since $a + b = b + a \quad \forall a, b \in \mathbb{Z}$)

② $(\mathbb{R}, +)$ is also an Abelian group

$(\mathbb{R}_{>0}, \cdot)$ is an Abelian group

$a \cdot b \in \mathbb{R}_{>0}$ if $a, b \in \mathbb{R}_{>0}$

associativity,

$e = 1$ $(a \cdot 1 = 1 \cdot a = a)$

inverse of a : $a^{-1} = \frac{1}{a} \in \mathbb{R}_{>0}$.

3 Let S = set, $\mathrm{Sym}(S) = \{h : S \to S : h \text{ is bijective}\}$

$S = [n]$

$S_n = \mathrm{Sym}([n])$.

$(\mathrm{Sym}(S), \text{composition})$ is a group :

- closure ✓
- associativity if $a, b, c \in \mathrm{Sym}(S)$

  $a \circ (b \circ c) \stackrel{?}{=} (a \circ b) \circ c$,

  YES! (for all functions)
- $e = \mathrm{id}_S : S \to S$.
- inverses : if $a : S \to S$ is a bijection, then a has an inverse $a^{-1} : S \to S$

$\therefore$ $\mathrm{Sym}(S)$, S_n are groups.

$|S_n| = n!$

$|\mathrm{Sym}(S)| = (|S|)!$ (or ∞ if $|S| = \infty$).

is S_n Abelian? Good question.

$|S_1| = 1$ (only the identity)

think about this: S_2, S_3, S_4 ?

$\{id, (1\,2)\}$ Abelian

not Abelian

not Abelian

4 matrices

notation $\mathbb{R}^{n \times n}$ = set of all $n \times n$ matrices with entries in $\mathbb{R}$.

(also $\mathbb{Q}^{n \times n}$, $\mathbb{C}^{n \times n}$)

review:
- if $A, B \in \mathbb{R}^{n \times n}$, then $A + B \in \mathbb{R}^{n \times n}$ and $AB \in \mathbb{R}^{n \times n}$

we will assume

- also have determinant.

$$\det : \mathbb{R}^{n \times n} \longrightarrow \mathbb{R}$$
$$A \longmapsto \det A$$

$\det A \neq 0 \iff A$ has an inverse A^{-1}

$\det(AB) = \det(A)\det(B)$.

What groups?

$(\mathbb{R}^{n\times n}, +)$ is an Abelian group.

What about multiplication?

<u>Def</u> $GL_n(\mathbb{R}) = \{ A \in \mathbb{R}^{n\times n} : A \text{ is invertible} \}$
"general linear" (ie: $\det A \neq 0$)

Similarly: $GL_n(\mathbb{Q})$, $GL_n(\mathbb{C})$

<u>theorem</u> $(GL_n(\mathbb{R}), \cdot)$ is a group.
(similarly for $GL_n(\mathbb{Q})$, $GL_n(\mathbb{C})$)

is $GL_n(\mathbb{R})$ Abelian?
$n=1$: Abelian
$n\geq 2$: not Abelian.

Basic properties of groups

Suppose $(G, *)$ is a group.

Prop

① The cancellation law holds: $\forall a,b,c \in G$
- if $a*b = a*c$ then $b=c$.
- if $b*a = c*a$ then $b=c$

2. $e \in G$ is the unique elem st. $a * e = e * a = a \quad \forall a \in G$

ie: if you have $e' \in G$ s.t. $a * e' = e' * a = a$ then $e = e'$.

Proof of 1: $\exists\ a' \in G$ s.t. $a * a' = a' * a = e$

then

$$a' * (a * b) = a' * (a * c)$$

$$\therefore \quad (a' * a) * b = (a' * a) * c$$

$$e * b = e * c$$

$$b = c \quad \checkmark$$

other part is similar

Proof of 2: have $a * e' = a * e$

cancellation $\Rightarrow$ $e' = e$ $\checkmark$

3. Given $a \in G$, $\exists !\ a' \in G$ s.t. $a * b = b * a = e$ (inverse is unique).

$\therefore$ we write this inverse as a^{-1} (unique).

4. $(a^{-1})^{-1} = a \quad \forall a \in G$.

proof of 3, 4 : do it!

Next time: $(\mathbb{Z}_n, +)$, subgroups