Jan27

Tuesday, January 25, 2022 11:18 AM

Announcements

Thursday 1/27 : No office hours

Tuesday 2/1 : Remote Class

Wednesday 2/2 : No office hours.

Thursday 2/3 : Back to normal.

---

§ Groups

History

① Number Theory

Observe

- p prime & $p \nmid a$ then a^{p-1} is one more than a multiple of p. } Fermat's little theorem.
- $2, 5 \nmid a$. a^{40} ends in 01 } Euler's theorem.

Deduce this from understanding the structure of the groups

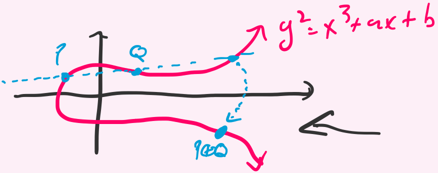
- $(\mathbb{Z}/p\mathbb{Z})^{\times}$
- $(\mathbb{Z}/100\mathbb{Z})^{\times}$

Recall → $(\mathbb{Z}/n\mathbb{Z})^{\times} = \{ \bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a,n) = 1 \}$

w/ multiplication.

② Geometry

Solutions to cubic equation



behaves like addition.

- Related to + in $\mathbb{C}$
- Related to a funny multiplication law of types of integrals.

③ Algebra

Quadratic Formula

zeros of $ax^2 + bx + c$

are $x = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

2 solutions are symmetric, swap + & −

Cubic Formulas
Quartic Formulas

More complicated but give roots in terms of (+, −, ×, ÷, $\sqrt{\ }$ (*)) & get symmetries.

Observation: Galois

- * Symmetries "of things related by (*)" are simple.
- * Roots of degree 5 polynomial can be more complicated. ←

(group theory showed difference btwn complicated & simple)

Result: No quintic formula.

Point

- 3 different fields, notion of taking 2 things & combining to get a third, was highly structured & lucrative.

(mult #s
adding points
composing symmetries

- Pin down these abstract axioms that extend all 3 examples above & view them in same universe.

Impt Definition(s)

Def^{n} Let G be a set. A binary operation on G is a function

$$* : G \times G \longrightarrow G$$

Notation
we will write $a * b$ instead of $*(a,b)$

Fundamental Definition

A group is a set G w/ a binary operation $*$ satisfying:

(Associative) ① $(a*b)*c = a*(b*c)$
$\forall\ a,b,c \in G$

(Identity) ② $\exists\ e \in G$ s.t. $\forall\ a \in G$

$$e*a = a = a*e$$

(Inverse) ③ Given $a \in G$, $\exists\ b \in G$
s.t.
$$a*b = e = b*a$$

Observations

① We did *not* assert that

$a*b = b*a$. (Not always true).

② We did not assert that inverses and identities are unique.

(Will be true!!)

③ We often write G as the group rather than $(G, *)$.

Theorem

Let G be a group.

① The identity $e \in G$ is unique.

② If $a \in G$, the inverse of a is unique. Call it a^{-1}!

③ Let $a \in G$. If $\boxed{\underline{a*b=e}}$, then $a = b^{-1}$ and $b = a^{-1}$.

Proof

① Suppose e_1 & e_2 both identities.

$$e_1 \underset{\substack{\uparrow \\ e_2 \text{ an} \\ \text{identity.}}}{=} e_1 * e_2 \underset{\substack{\uparrow \\ e_1 \text{ an identity.}}}{=} e_2$$

② $a \in G$. Suppose $b, c \in G$ both inverse to a.

$$\begin{aligned}
b &= b * e && (e \text{ identity}) \\
&= b * (a * c) && (c \text{ an inverse}) \\
&= (b * a) * c && (\text{associative law}) \\
&= e * c && (b \text{ an inverse}) \\
&= c && (e \text{ identity}).
\end{aligned}$$

✓

③ Exercise.

Remarks:

① Never changed order.

② Only used group axioms

Corollary

G a group. $a, b \in G$.

① $(a^{-1})^{-1} = a$

② $(a*b)^{-1} = b^{-1} * a^{-1}$

Pf/ ① Use part ③ of Thm.

Compute inverse of a^{-1}, the thing (b) s.t. $(a^{-1})*b = e$

Try $b = a$.

$$(a^{-1})*a = e \quad \checkmark$$

② Similar. Exercise.

Notation

1) Sometimes write ab for $a*b$.

2) Write $a^n = \underbrace{a*a*a*\cdots*a}_{n\text{- times}}$

$$a^{-n} = \underbrace{a^{-1}*a^{-1}*\cdots*a^{-1}}_{n\text{- times.}}$$

3) Write 1 or 1_a for the identity instead of e.

Solving Equations & Cancellation Laws

Questions

- $ax = b$ solve for x. } Can we do this in a general group?

- $ab = ac$, does $b = c$?

  (true for x if $a \neq 0$).

Proposition (Cancellation)

Let G be a group. $a, b, u, v \in G$.

i) Left Cancellation: If $au = av$ then $u = v$.

ii) Right Cancellation: If $ub = vb$ then $u = v$.

Proof/ Assume $au = av$.

(i) Multiply on left by a^{-1}.

$$a^{-1}(au) = a^{-1}(av)$$

$$(a^{-1}a)u = (a^{-1}a)v \quad \text{(assoc)}$$

$$1 \cdot u = 1 \cdot v \quad \text{(inverse)}$$

$u = 2v$ (identity).

(ii) Identical. ∅

Corollary (Solving equations).

G a group. $a, b \in G$. x, z variables.

i) $ax = b$ has a unique solution
$x = a^{-1}b$

ii) $za = b$ has a unique solution
$z = ba^{-1}$

pf/ i) **Existence.**

$$a * (a^{-1}b) = (aa^{-1})b = 1b = b$$

so $a^{-1}b$ is a solution.

Uniqueness

Let u be another solution.

$$\cancel{a}u = b = \cancel{a}(a^{-1}b)$$

By cancellation

$$u = a^{-1}b$$ ∅

(ii) Exercise.

Examples

① Additive groups:

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$

$e = 0$ $\quad a + 0 = a = 0 + a$

Inverse of a is $-a$

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

② $(\mathbb{Q} \setminus \{0\}, \times)$ $\quad e = 1$ $\quad a \times 1 = a = 1 \times a$

$(\mathbb{R} \setminus \{0\}, \times)$ $\quad$ inverse of a is

$a^{-1} = \frac{1}{a}$ $\quad a \times \left(\frac{1}{a}\right) = 1$.

Question

Why did we need to remove 0?

Is $(\mathbb{Q}, \times)$ still a group??

③ $(\mathbb{Z} \setminus \{0\}, \times)$. Not a group.

$e = 1$ ok

What is 2^{-1} ? No inverse!

④ $(\mathbb{Q}_{>0}, \times)$ } positive #s.

$(\mathbb{R}_{>0}, \times)$

⑤ Linear Algebra

V a vector space.

Then $(V, \underset{\uparrow\text{ vector addition}}{+})$ is a group.

$e = \vec{0}$. Inverse of $\vec{v}$ is $-\vec{v}$.

In particular

$(\mathbb{R}^n, +)$ a group.

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n).$$

Rmk Vector spaces have even more structure given by scaling.
($\mathbb{R}$-action)

Often associativity is hard.

⑥ $(\mathbb{R}^3, \underset{\uparrow\text{ cross product}}{\times})$

Not a group bc not associative.

Example 5 motivates the following construction:

Def^n $(G, *)$ and $(H, \bullet)$ be 2 groups. The direct product of G & H is

$$G \times H = \{ (g,h) \mid g \in G,\ h \in H \}$$

Operation is

$$(g_1, h_1) \times (g_2, h_2) = (g_1 * g_2,\ h_1 \bullet h_2)$$

Exercise

This is a group.

Examples

⑦ $\mathbb{Z}/n\mathbb{Z} = \{ \overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1} \}$

w/ $\overline{a} + \overline{b} = \overline{a+b}$ is a group!

Identity: $e = \overline{0}$ $\quad \overline{a} + \overline{0} = \overline{a+0} = \overline{a}$

Inverse of $\overline{a}$ is $\overline{n-a}$ (or $\overline{-a}$)

$$\overline{a} + \overline{n-a} = \overline{a+n-a} = \overline{n} = \overline{0}$$

Associativity (follows from assoc in $\mathbb{Z}$)

Pf/ $(\overline{a} + \overline{b}) + \overline{c} = (\overline{a+b}) + \overline{c}$

$= \overline{(a+b)+c}$

$= \overline{a+(b+c)}$

$= \overline{a} + (\overline{b+c})$

$= \overline{a} + (\overline{b} + \overline{c})$

⑧ $(\mathbb{Z}/n\mathbb{Z}, \times)$ not a group.

(not inverses!).

⑨

$$(\mathbb{Z}/n\mathbb{Z})^{\times} = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a,n) = 1\}$$

$$= \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \bar{a} \text{ has a mult inverse}\}$$

Is a group under ×.

$e = \bar{1}$ $\quad \bar{a} \times \bar{1} = \overline{a \times 1} = \bar{a}$

Assoc (follows from $\mathbb{Z}$)

Inverse:

$\bar{a}^{-1} \leftarrow$ $\gcd(a,n) = 1$. $\exists\, u, v$ s.t.

$au + nv = 1$

so $au \equiv 1 \mod n$.

Therefore

$$\bar{a} \cdot \bar{u} = \overline{au} = \bar{1}$$

so $\bar{a}^{-1} = \bar{u}$ $\quad \emptyset$

⚠ Need to prove $(\mathbb{Z}/n\mathbb{Z})^\times$ is closed under ×.

i.e., if $\bar{a}, \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$

need $\bar{a} \cdot \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$

exercise

⑩

$$GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; ad - bc \neq 0 \right\}$$

Operation is matrix multiplication.

1) Closed under multiplication.

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

so if $\det A$ & $\det B \neq 0$ ✓

$$\det(AB) \neq 0$$

$$AB \in GL_2(\mathbb{R}).$$

2) Associative. (Later)

3) Identity

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$ ✓

4) Inverses.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Observation

$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in GL_2(\mathbb{R})$

$AB = \begin{pmatrix} a & d \\ 0 & d \end{pmatrix}$

$BA = \begin{pmatrix} a & a \\ 0 & d \end{pmatrix}$

$AB \neq BA$ in general

Def^n

A group $(G, *)$ is called an abelian group if $\forall\, a, b \in G$

$a * b = b * a$

(commutative group).

Notation

Some groups are more naturally written additively.

$(\mathbb{Z}, +)$. $\quad \cancel{2 * 3} \quad 2 + 3$

also $\underbrace{a + \cdots + a}_{n\text{-times}} \cancel{= a^n} = n \cdot a$

Observation

1) in $(\mathbb{Z}/8\mathbb{Z})$ $\quad |\bar{2}| = 4$

$\bar{2} + \bar{2} + \bar{2} + \bar{2} = \bar{8} = \bar{0}$

↑ do binary operation over over again I get to the identity.

$$\underbrace{\bar{1}+\bar{1}+\cdots+\bar{1}}_{8\text{-times}} \leftarrow |\bar{1}|=8$$

2) In $\mathbb{Z}$, this never happens.

$$1+1+1+\cdots+1 \neq 0.$$

↑ $|1|=\infty$.

3) In $(\mathbb{Z}/7\mathbb{Z})^{\times}$

$$\bar{2},\quad \underset{\bar{4}}{\underset{\shortparallel}{\bar{2}\times\bar{2}}},\quad \bar{2}\times\bar{2}\times\bar{2} = \underset{\bar{1}}{\underset{\shortparallel}{\bar{8}}}$$

$$\bar{2}^3=\bar{1} \qquad \nwarrow |\bar{2}|=3$$

Def$^{\underline{n}}$

Let G be a group & $g\in G$.
The order of g is

$$|g| = \min\{n\geq 0 \mid g^n = 1_G\}.$$
