Lecture 1

Monday, January 26, 2015 7:45 AM

MATH 332

Algebra: set, w/ some collection of operations

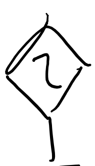
Oftentimes encode symmetry of some sort.

Binary operations

Set G, $\cdot : G \times G \longrightarrow G$

Write $a \cdot b$ for $\cdot(a,b)$.

- $\cdot$ is associative if $a\cdot(b\cdot c) = (a\cdot b)\cdot c$ for every $a, b, c \in G$
- $\cdot$ is commutative if $a\cdot b = b\cdot a$ for all $a, b \in G$.



Oftentimes $\cdot$ will be non commutative!

e.g. $+$ on $\mathbb{R}$ is assoc & comm

$-$ on $\mathbb{R}$: $a-(b-c) = a-b+c$
neither $\neq (a-b)-c$

Matrix mult is assoc but not comm.

<u>Defn</u> A <u>group</u> is an ordered pair $(G, \cdot)$ where G is a set & $\cdot$ is an <u>associative</u> binary operation such that

① $\exists e \in G$ s.t. $e \cdot a = a \cdot e = a$ for all $a \in G$.

e is the identity elt

② $\forall a \in G$ $\exists a^{-1} \in G$ s.t. $a \cdot a^{-1} = e$. $= a^{-1} \cdot a$

the inverse of a

If $(G, \cdot)$ is a group & $\cdot$ is commutative, then $(G, \cdot)$ is an <u>abelian group</u>

<u>e.g.</u> ① $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are gps under $+$ w/ $e = 0$ & $a^{-1} = -a$

② $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^\times$, $\mathbb{C}^\times$ are gps under mult. w/ $e = 1$, $a^{-1} = \frac{1}{a}$

③ $\mathbb{Z} \setminus \{0\}$ under mult is not a gp b/c it lacks inverses

④ $\{\pm 1\}$ w/ mult is a gp.

(5) Vector space under + form a gp

(6) $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$,

$a \boxplus b =$ remainder of $a+b$ divided by n

w/ $e = 0$, $a^{-1} = n - a$.

(7) Let $\mathbb{Z}_n^{\times} = \{ i \in \{0, 1, \dots, n-1\} \mid \exists j \in \{0, 1, \dots, n-1\}$ s.t. $\underbrace{ij \equiv 1 \pmod{n}}_{n \text{ divides } ij-1} \}$,

then $\mathbb{Z}_n^{\times}$ is a gp under mult mod n
w/ $e = 1$

(8) If $(A, \cdot)$ & $(B, \odot)$ are groups, then $A \times B$ has a gp structure via

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \odot b_2)$$

w/ $e = (e_A, e_B)$, $(a, b)^{-1} = (a^{-1}, b^{-1})$

Properties which follow from axioms:

If $(G, \cdot)$ is a gp, then

1. If $e' \in G$, and $e' \cdot a = a \cdot e' = a \ \forall a \in G$, then $e' = e$.
2. If $ab = e$, then $a = b^{-1}$ & $b = a^{-1}$.
3. $(a^{-1})^{-1} = a \ \forall a \in G$
4. $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$
5. $a_1 \cdot a_2 \cdots a_n$ is well-defined regardless of parenthetisization.

Pf
1. $e' \cdot e = e$ & $e' \cdot e = e' \implies e = e'$.
2. $$\begin{aligned} a^{-1} &= a^{-1} \cdot e && [id] \\ &= a^{-1} \cdot (a \cdot b) && [hypothesis] \\ &= (a^{-1} \cdot a) \cdot b && [assoc] \\ &= e \cdot b && [inverses] \\ &= b && [id] \end{aligned}$$
3. $(a^{-1})^{-1} = a$ ✓

(4) Claim $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$

Know $(a \cdot b)(a \cdot b)^{-1} = e$

By assoc, $a \cdot (b \cdot (a \cdot b)^{-1}) = e$

Mult on left by a^{-1}: $a^{-1} \cdot (a \cdot (b \cdot (a \cdot b)^{-1})) = a^{-1} \cdot e$

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

Mult on left by b^{-1}: $b^{-1} \cdot (b \cdot (a \cdot b)^{-1}) = b^{-1} \cdot a^{-1}$

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