MAT401 Dror Bar-Natan

homepage: google "drorbn" → classes → 401

Polynomials, Equations and Fields Jan 09

(Following Galois to the top of math's first mounta

linear equation $ax+b=0 \Rightarrow x=-b/a$

quadratic equation $ax^2+bx+c=0$

$$\Rightarrow x_{1,2} = \frac{-b\pm\sqrt{b^2-4ac}}{2a}$$ "the monster"

cubic equation $ax^3+bx^2+cx+d=0$

$\Rightarrow X_{1,2,3} = - - - -$

$ax^4+bx^3+cx^2+dx+e=0$

$X_{1,2,3,4} = - - - -$

"truly horrible monster" !!

$ax^5+bx^4+ \cdots +f=0$

Belwegian mathematician proved that you cannot solve (find a solution)

(Abel)

Galois proved it better, and improved it from Abel.

Ring: set of real numbers

★ not ℝ

ℝ: real number

Def'n A "ring" is a non-empty set, R, along with two binary operations

"plus" $+ : R\times R \to R \quad a,b \mapsto a+b$

"times" $\cdot : R\times R \to R \quad a,b \mapsto a\cdot b$

s.t. for all $a,b,c \in R$:

① $a+b=b+a$ commutative law for additio

② $(a+b)+c = a+(b+c)$

③ ∃ distinguished element $0 \in R$

s.t. $0+a = a+0 = a$

④ $\forall\ a\in R \ \exists\ \underset{(-a)}{b}\in R$ s.t. $a+b=0$

★ negative is NOT operation applied to a. $a+(-a)=0$

⑤ $a(bc) = (ab)c$
⑥ $(a+b)c =$ ~~ab + bc~~ $ac+bc$
[illegible] $a(b+c) = ab + ac$

R is Commutative or "Abelian" if
⑦ $ab = ba$

~~A~~multiplication isn't neccessarly commutative

"R has a unity" if $\exists\ \overset{\text{"the unity"}}{1} \in R$
s.t. $1 \cdot a = a \cdot 1 = a$

Examples

1. $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$
a) commutative
b) has unity 1.

2. Let n be an integer (positive)
$R = \{0, 1, 2, \dots n-1\} = \mathbb{Z}_n = \mathbb{Z}/n$
is a ring using
$a +_R b := a +_{\mathbb{Z}} b \mod n$

if $n = 7$ $\quad 3 +_R 6 = 9 \mod 7 = 2$

$a \times_R b := a \times_{\mathbb{Z}} b \mod n$
$2 \times_R 4 = 8 \mod 7 = 1$

commutative, unity: 1
This ring is finite
order of the ring = n = # of elements

Jan 9

3. $\mathbb{Z}[x] := \{ \sum_{i=0}^{\infty} a_i x^i$: all but finitely many a_i's are 0, $a_i \in \mathbb{Z} \}$

$\{ 22x^3 - 7x^2 + 3x - 2$, $22x + 7$, $2 \}$

add & multiply the way you add & multiply polynomi

$(2x+3)(x-7)$
$= (x-7)(2x+3)$

unity? $1 = \underline{1x^0}$ (polynomial)

4. Even integers ($2\mathbb{Z}$) $\ldots -4, -2, 0, 2, 4, \ldots$
a) commutative b) no unity

4. $n\mathbb{Z} = \{ \ldots, -2n, -n, 0, n, 2n, 3n \ldots \}$
a) commutative b) no unity unless $n = 1$

5. $M_{2\times2}(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z} \right\}$

matrix addition, matrix multiplication
a) not commutative b) unity : $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

6. $M_2(n\mathbb{Z}) = \begin{pmatrix} na & nb \\ nc & nd \end{pmatrix}$: it is a ring
But $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is not in.
Exercise: prove that there is no unity

7. $\mathbb{Z}/6 = \{ 0, 1, 2, 3. 4, 5 \}$
commutative, unity $= 1$
Subset $R = \{0, 2, 4\}$
with same addition & multiplication
$2+2 = 4$ $4+4 = 2$
commutative? Yes
Unity? Yes Unity $= 4$ $4 \cdot 0 = 0$
$4 \cdot 2 = 8 \to 2$
$4 \cdot 4 = 16 \to 4$

⑧ Definition: If R_1, R_2 are rings, ~~make~~ let $R = R_1 \oplus R_2$ be the ring whose elements are $\{(r_1, r_2) : r_1 \in R_1, r_2 \in R_2\}$

under: $(a_1, b_1) +_R (a_2, b_2) := (a_1 +_{R_1} a_2, b_1 +_{R_2} b_2)$

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

Exercise: this is indeed a ring
if R_1 and R_2 are commutative, then $R_1 \oplus R_2$ is commutative
if R_1 and R_2 have unity, $R_1 \oplus R_2$ has unity

0. If $a+b=a$ then $b=0$

Theorem 1: If R is a ring & $a, b \in R$,
Then
1. $a \cdot 0 = 0 \cdot a = 0$
2. $a \cdot (-b) = (-a) \cdot b = -(ab)$
3. $(-a) \cdot (-b) = a \cdot b$
4. negatives are unique
$a+b=0$ & $a+c=0 \Rightarrow b=c$
($a \to -a$ is single valued)
($a-b := a+(-b)$)
5. $c(a-b) = ca-cb$

If R has a unity 1
6. $(-1) a = -a$
7. $(-1)(-1) = 1$

must use the distributive law
Exercise: find ring that doesn't have a distributive law
$\Rightarrow$ Let a rung be a not-necessaily distributive "ring"
Find a rung in which $0 \cdot a \neq 0$ for some a

Jan 9

Proof of 1 $0+0=0$

$a(0+0) = a\cdot 0$

'' using distributivity law

$a\cdot 0 + a\cdot 0 = a\cdot 0$ & add $(-a\cdot 0)$ to both sides

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

$a\cdot 0 + (a\cdot 0 + (-a\cdot 0)) = \underbrace{a\cdot 0 + (-a\cdot 0)}_{\overset{''}{0}}$ by def'n of $-a\cdot 0$

$a\cdot 0 + 0 = 0$

$a\cdot 0 = 0$. □

★ on the step

$\underline{a\cdot 0} + a\cdot 0 = \underline{a\cdot 0}$

these are same.

∴ must be 0

BUT, hasn't shown $a\cdot 0 = 0$

∴ must carry on...

★ If $a+b=a$ then $b=0$

must be included in Theorem 1 as Prop

then above can be shortened.

⇒ "Cancellation law for addition"

Theorem: If $a+c=b+c$, then $a=b$

in particular, if $a+c=0+c=c$

then $a=0$.

proof: add $(-c)$ to both sides.

Corollary: There is unique 0.

Proof of Prop 2: → prove $a\cdot(-b) = -(ab)$

$a\cdot(-b) = (-a)\cdot b = -(ab)$ will follow

Consider $b+(-b)=0$

$a(b+(-b)) = a\cdot 0$

by prop ①, $a \cdot 0 = 0$

$\Rightarrow a(b+(-b)) = 0$

by distributivity

$\rightarrow ab + a(-b) = 0$

add $-(ab)$

$a(-b) = -(ab)$

8. If R has a unity, it is unique.

$\Rightarrow (a \cdot c) = a \quad \forall a$

$\Rightarrow \quad c = 1$

9. If a has an inverse, it is unique

$\begin{matrix} ab = 1 \\ ac = 1 \end{matrix} \Rightarrow b = c$

Pf of 8

$\forall a \quad a \cdot c = a \Rightarrow 1 \cdot c = 1$

$\Rightarrow c = 1$

Def'n If R is commutative, an element $a \in R$ is a "Zero-divisor" if

1. $a \neq 0$
2. $\exists \, b \neq 0$ s.t. $ab = 0$

Example: in $\mathbb{Z}/6$, 2 is a zero divisor

$2 \neq 0, \quad 2 \cdot 3 = 0$

$3 \neq 0$

Def'n A commutative ring with unity R is called an integral domain, (a domain) if it has no zero divisors.

Jan 9

<u>Example</u>: $\mathbb{Z}_6$ isn't
$\mathbb{Z}_n$ isn't if n is not a prime.

<u>Example</u>: $\mathbb{Z}$ is a domain

$(\Rightarrow a \cdot b = 0 \Leftrightarrow a = 0$ or $b = 0)$

<u>Example</u>: $\overset{=R}{\mathbb{Z}/p}$ is an integral domain
if p is prime

<u>proof</u>: assume $a, b \in \mathbb{Z}/p$ and
$a \cdot_R b = 0 \Rightarrow a \cdot_{\mathbb{Z}} b$ is a multiple of p.

$\Rightarrow p$ divides $a \cdot b$
$\Rightarrow p$ divides a or p divides b
$\Rightarrow a = 0$ $\qquad \Rightarrow b = 0$.

<u>Def'n</u>: A commutative ring with unity R is a "Field" if every non-zero element has an inverse.

<u>Examples</u>: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$
~~$\mathbb{Z}$~~
<u>claim</u>: $\mathbb{Z}/p$ is a field.