Lecture 01: Historical note

Saturday, January 12, 2019 9:49 AM

Historically algebra was developed to study zeros of polynomials. The word algebra comes from the name of a book written by a persian mathematician Kharazmi (خوارزمی). In this book, he essentially told us how to find zeros of deg. 1 and deg. 2 polynomials. Finding zeros of deg. 3 polynomials has a fascinating history. Khayaam had a geometric method to solve certain such polynomials, but the general case had been solved by Tartaglia. Zeros of deg. 4 poly. were found by Ferrari. In 1824, Abel showed that one cannot express zeros of a general deg. 5 polynomial using $+, -, \times, /$, and radicals. In 1832, Galois taught us how to study zeros of polynomials.

Another problem that had a lot of influence in developement of algebra was Fermat's Last Conjecture: $x^n+y^n=z^n$ has no non-trivial integral solutions. As you can see, it is again about zeros of a polynomial; but this time there are more than 1

Lecture 01: Definition

Saturday, January 12, 2019 9:52 AM

variable and we are asking for zeros in $\mathbb{Z}$.

In both of these problems, we add a zero to $\mathbb{Q}$ or $\mathbb{Z}$, create a new "system of numbers", and study it. And this is how we get to ring theory.

In this course, we will study basics of ring theory and properties of polynomials with coefficients in $\mathbb{Z}$ (or any other ring). We will see the beginning of field theory as well.

Math 103a was about symmetries of objects (group theory); abstract group theory came after ring theory and its study was partially motivated by the mentioned work of Galois.

Def. A ring $(R, +, \cdot)$ is a set R with two binary operations: $+$ (addition) and $\cdot$ (multiplication) such that the following holds:

① $(R, +)$ is an abelian group.

② (associativity) $\forall a, b, c \in R$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Lecture 01: Example; units; fields

Saturday, January 12, 2019 10:08 AM

3 (distribution) $\forall a, b, c \in R$,

$$a \cdot (b+c) = a \cdot b + a \cdot c \quad \text{and} \quad (b+c) \cdot a = b \cdot a + c \cdot a.$$

- We say R is <u>unital</u> if, $\exists\, 1_R \in R$, $\forall\, r \in R$,

$$1_R \cdot r = r = r \cdot 1_R$$

Such an element is called a <u>unity</u> or <u>identity</u> of R. We will show that, if R has an identity, then it is unique; and so it is O.K. to denote it by 1_R.

- We say R is <u>commutative</u> if $\forall\, a, b \in R$, $a \cdot b = b \cdot a$.

<u>Example</u>. $\mathbb{Q}$: rational numbers;

This is a unital commutative ring with an additional property: any non-zero element has a multiplicative inverse.

<u>Def</u>. (a) An element a of a unital ring A is called a <u>unit</u> if it has a multiplicative inverse; that means $\exists\, a' \in A$ s.t. $aa' = a'a = 1$. The set of all the units of A is denoted by $A^{\times}$.

(b) A unital commutative ring F is called a field if

Lecture 01: Examples

Saturday, January 12, 2019 10:22 AM

$0 \neq 1$ (has at least two elements) and $F^{\times} = F \setminus \{0\}$; that means any element except 0 is a unit.

<u>Ex</u>. $\mathbb{R}$: ring of real numbers is a field.

- $\mathbb{C}$: ring of complex numbers is a field.
- $\mathbb{Z}$ integers form a unital commutative ring; but it is not a field; in fact $\mathbb{Z}^{\times} = \{1, -1\}$;

. $a \in \mathbb{Z}^{\times} \Rightarrow \exists\, a' \in \mathbb{Z},\ aa' = 1 \Rightarrow \left\{\begin{array}{l} |a|\,|a'| = 1 \\ a \neq 0,\ a' \neq 0 \end{array}\right.$

$$\left.\begin{array}{l} a, a' \in \mathbb{Z} \\ a, a' \neq 0 \end{array}\right\} \Rightarrow \left.\begin{array}{l} |a| \geq 1,\ |a'| \geq 1 \\ |a|\,|a'| = 1 \end{array}\right\} \Rightarrow |a| = 1 \Rightarrow a = \pm 1.$$

. $1 \times 1 = 1$ and $(-1) \times (-1) = 1$.

- $\mathbb{Z}^{\geq 0}$ the set of non-negative integers is not a ring since $(\mathbb{Z}^{\geq 0}, +)$ is not an abelian group; for instance $\nexists\, x \in \mathbb{Z}^{\geq 0},\ x + 1 = 0$.

- $M_2(\mathbb{R})$ is a non-commutative unital ring: the identity matrix is the unity of this ring; $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and

Lecture 01: Examples

Sunday, January 13, 2019 2:05 AM

$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ and so it is not commutative.

One can consider $n \times n$ matrices with entries in any given ring; and one can see that $M_n(R)$ is a ring.

$\boxed{Q}$ Is there a commutative ring with no identity?

Yes, for instance $2\mathbb{Z}$; subtracting and multiplying two even numbers we get another even number; associativity, distribution and commutativity are inherited from $\mathbb{Z}$.

Def. Suppose $(R, +, \cdot)$ is a ring. $S \subseteq R$ is called a subring if $(S, +, \cdot)$ is a ring.

In group theory, you learned that, if $(G, \cdot)$ is a group, $H \subseteq G$ is a subgroup if and only if $\forall\, h_1, h_2 \in H$, $h_1^{-1} h_2 \in H$. We called it subgroup criterion. Similarly we have a subring criterion.

Lemma (Subring Criterion) Suppose $(R, +, \cdot)$ is a ring and $S \subseteq R$ is a non-empty subset. S is a subring if and only if $\forall\, x, y \in S$, $x - y \in S$, $x \cdot y \in S$.

Lecture 01: Subring criterion; congruences

Sunday, January 13, 2019 2:17 AM

Pf. ($\Rightarrow$) is clear.

($\Leftarrow$) Using subgroup criterion, $(S,+)$ is a subgroup; and since S is closed under multiplication, $\cdot$ defines a binary operat. on S. Associativity and distribution is inherited from R. ∎

- $\mathbb{Z}_n := \{0,1,2,\dots,n-1\}$; in Math 103 a you have seen that $(\mathbb{Z}_n, \oplus)$ is a cyclic group where

$\forall a,b \in \mathbb{Z}_n$, $a \oplus b$ is the remainder of $a+b$ divided by n.

Similarly we can define a multiplication on $\mathbb{Z}_n$:

$\forall a,b \in \mathbb{Z}_n$, $a \odot b$ is the remainder of ab divided by n.

One can check that $(\mathbb{Z}_n, \oplus, \odot)$ is a unital commutative ring.

This can be observed using $a \oplus b \equiv a+b \pmod{n}$ and $a \odot b \equiv ab \pmod{n}$. For instance here is why get the distribution property:

$$a \odot (b \oplus c) \overset{n}{\equiv} a(b \oplus c) \overset{n}{\equiv} a(b+c) = ab+ac \overset{n}{\equiv} a\odot b + a \odot c$$

$$\overset{n}{\equiv} (a\odot b) \oplus (a \odot c)$$ Uniquess of remainder implies

$$a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$$

Lecture 01: Basic properties of rings

Sunday, January 13, 2019 2:32 AM

Basic properties of rings.

① If R is a unital ring, then it has a unique identity.

Pf. Suppose 1 and $1'$ are two identities. Then

$$1 = 1 \cdot 1' \quad (\text{since } 1' \text{ is an identity})$$
$$= 1' \quad (\text{since } 1 \text{ is an identity}).$$

② $0 \cdot a = a \cdot 0 = 0$

Pf. $0+0=0 \Rightarrow (0+0)\cdot a = 0\cdot a \Rightarrow 0 \cdot a + 0 \cdot a = 0 \cdot a$ (distribution)

$$\Rightarrow 0 \cdot a = 0 \quad ((R,+) \text{ is a group}).$$

Similarly $a\cdot(0+0) = a \cdot 0 \Rightarrow a\cdot 0 + a \cdot 0 = a \cdot 0 \Rightarrow a \cdot 0 = 0$.

③ $(-a)\cdot b = -a\cdot b = a \cdot (-b)$

Pf. . $a + (-a) = 0 \Rightarrow (a+(-a))\cdot b = 0 \cdot b = 0$

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

$$\Rightarrow (-a)\cdot b = -a \cdot b$$

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

$$\Rightarrow a \cdot (-b) = -a \cdot b.$$

Lecture 01: Examples

Sunday, January 13, 2019 2:41 AM

④ $(-a)\cdot(-b) = a\cdot b$

Pf. $(-a)\cdot(-b) = -(-a)\cdot b = -(-a\cdot b) = a\cdot b.$ $\blacksquare$

Ex. Write the multiplication table of $\mathbb{Z}_4$.

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$a\cdot 0 = 0\cdot a = 0$

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

Notice that $2 \neq 0$ in $\mathbb{Z}_4$, but

$$2\times 2 = 0 \text{ in } \mathbb{Z}_4.$$

Def. Suppose R is a ring, and $a\in R$. We say a is a zero-divisor if $a\neq 0$ and $aa'=0$ for some $a'\in R\setminus\{0\}$.

So 2 is a zero-divisor in $\mathbb{Z}_4$.

An element is a unit precisely when there is a 1 in its row in the multiplication table. So $\mathbb{Z}_4^{\times} = \{1, 3\}$.

Similar to group theory, for us structure of ring is important and not its elements; for instance it does not matter if one uses $0, 1, 2, 3, \dots$; $\mathrm{O}, \mathrm{I}, \mathrm{II}, \mathrm{III}, \dots$; ٠, ١, ٢, ٣, …; or $a, b, c, \dots$ to denote elements of $\mathbb{Z}_n$ as long as one uses the right

Lecture 01: Examples

Sunday, January 13, 2019 2:52 AM

multiplication and addition table, which essentially if there is an isomorphism between these rings.

Def. • Suppose R and R' are two rings. A function $f: R \to R'$ is called a ring homomorphism if

$$\forall a,b \in R, \quad f(\underbrace{a+b}_{\text{in } R}) = \underbrace{f(a)+f(b)}_{\text{in } R'}$$

$$f(\underbrace{a \cdot b}_{\text{in } R}) = \underbrace{f(a) \cdot f(b)}_{\text{in } R'}$$

• A ring hom. $f: R \to R'$ is called an isomorphism if f is a bijection.

$\boxed{Q}$ Is $\mathbb{Z}_n$ a subring of $\mathbb{Z}$?

$\boxed{A}$ No. $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ is a subset of $\mathbb{Z}$ and $(\mathbb{Z}_n, \oplus, \odot)$ is a ring; but $\mathbb{Z}_n$ is not a ring with $+, \cdot$ in $\mathbb{Z}$. In fact $\mathbb{Z}_n$ is not closed under addition in $\mathbb{Z}$; for instance $\underbrace{1 + (n-1) = n}_{(\text{in } \mathbb{Z})}$ which is not in $\mathbb{Z}_n$.

Warning. Starting from the 3rd lecture the binary operations of $\mathbb{Z}_n$ will be denoted by $+, \cdot$.