# Lecture 01: Introduction

Sunday, April 1, 2018 10:25 PM

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: Introduction; definition of ring

Sunday, April 1, 2018 11:27 PM

variable and we 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.

<u>Def.</u> A ring $A$ is a set with two operations $+, \cdot$ with the following properties:

(1) $(A,+)$ is an abelian group.

(2) (associativity) $a\cdot(b\cdot c) = (a\cdot b)\cdot c$

(3) (distribution) $a\cdot(b+c) = a\cdot b + a\cdot c$

$$(b+c)\cdot a = b\cdot a + c\cdot a$$

- We say $A$ is <u>commutative</u> if $a\cdot b = b\cdot a$ for any $a,b\in A$.
- We say $A$ is <u>unital</u> if it has a <u>unity</u> or <u>identity</u>; that means $\exists\, e\in A$ s.t. $\forall a\in A$, $a\cdot e = e\cdot a = a$.

<u>Basic Properties</u>. (1) If $A$ is unital, its unity is unique.

<u>Pf</u>. Suppose $e_1$ and $e_2$ are two unities; then

# Lecture 01: Basic properties of rings

Monday, April 2, 2018 10:15 AM

$$e_1 = \underbrace{e_1 \cdot e_2}_{\boxed{e_2 \text{ is a unity}}} \underbrace{=}_{\boxed{e_1 \text{ is a unity}}} e_2 .$$

(2) $0 \cdot a = a \cdot 0 = 0$

**Pf.** $\underbrace{(0+0)}_{0} \cdot a = 0 \cdot a + 0 \cdot a$ (distribution)

$\Rightarrow \quad 0 \cdot a = 0 \cdot a + 0 \cdot a \quad \Rightarrow \quad 0 \cdot a = 0$

(adding $-0 \cdot a$ to both sides)

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

**Pf.** $a \cdot (-b) + a \cdot b = a \cdot ((-b) + b)$ (distribution)

$= a \cdot 0$

$= 0$ (as we proved above)

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

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

(4) $(-a) \cdot (-b) = ab$

**Pf.** $(-a) \cdot (-b) \underset{\boxed{\text{part}(3)}}{=} -(a \cdot (-b)) \underset{\boxed{\text{part}(3)}}{=} -(-a \cdot b) \underset{\boxed{\text{group theory}}}{=} a \cdot b$ .

(5) If $1$ is the unity of $A$, then $(-1) \cdot a = a \cdot (-1) = -a$ .

**Pf.** $(-1) \cdot a = -(1 \cdot a) = -a$ and $a \cdot (-1) = -(a \cdot 1) = -a$ .

# Lecture 01: Examples of rings

Monday, April 2, 2018 10:24 AM

Ex. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are unital commutative rings.

Ex. $\mathbb{Z}^{\geq 0}$ is NOT a ring as $(\mathbb{Z}^{\geq 0}, +)$ is not a group.

Remark. In a unital ring non-zero element might not have a multi. inverse. For instance $U(\mathbb{Z}) := \{n \in \mathbb{Z} \mid n \text{ has multipl. inverse}\}$

$= \{n \in \mathbb{Z} \mid \exists m \in \mathbb{Z},\ n.m = m.n = 1\} = \{1, -1\}$.

Ex. The set $2\mathbb{Z}$ of integer multiples of $2$ is a ring.

It is commutative, but it is not unital.

Since $2\mathbb{Z} \subseteq \mathbb{Z}$, to check whether it is a ring or not it is enough to check (1) $(2\mathbb{Z}, +)$ is a group (2) $(2\mathbb{Z}, \cdot)$ is closed under multiplication.

. Recall . $H$ is a subgroup of $(\mathbb{Z}, +)$ if and only if $H = n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

. Remark . Suppose $(R, +, \cdot)$ is a ring. Then $S \subseteq R$ is a subring if and only if (1) $(S, +)$ is a subgroup (2) $S$ is closed under multiplication.