Historically, algebra was developed to study zeros of polynomials. The word algebra comes from the name of a book written by a Persian mathematician Khwarazmi (خوارزمي). 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 +, -, x, /, and radicals. In 1832, Galois taught us how to study zeros of polynomials.

Another problem that had a lot of influence in development 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
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.

**Def.** A ring \( A \) is a set with two operations \( +, \cdot \) with the following properties:

1. \((A,+)\) is an abelian group.
2. (associativity) \( a.(b.c) = (a.b).c \)
3. (distribution) \( a.(b+c) = a.b + a.c \)
   \( (b+c).a = b.a + c.a \)

We say \( A \) is **commutative** if \( a.b = b.a \) for any \( a, b \in A \).

We say \( A \) is **unital** if it has a unity or identity; that means \( \exists e \in A \text{ s.t. } \forall a \in A, \ a.e = e.a = a \).

**Basic Properties.**
1. If \( A \) is unital, its unity is unique.
   **Pf.** Suppose \( e_1 \) and \( e_2 \) are two unities; then
Lecture 01: Basic properties of rings

Monday, April 2, 2018 10:15 AM

\[ e_1 = e_1 e_2 \quad \Rightarrow \quad e_2 \text{ is a unity} \]

\[ e_2 = e_2 \quad \Rightarrow \quad e_1 \text{ is a unity} \]

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

\[ (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a \quad \text{(distribution)} \]

\[ \Rightarrow \quad 0 \cdot a = 0 \cdot a + 0 \cdot a \quad \Rightarrow \quad 0 \cdot a = 0 \]

\[ \text{(adding } -0 \cdot a \text{ to both sides)} \]

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

\[ a \cdot (-b) + a \cdot b = a \cdot (-b + b) \quad \text{(distribution)} \]

\[ = a \cdot 0 \]

\[ = 0 \quad \text{(as we proved above)} \]

\[ \Rightarrow \quad a \cdot (-b) = -a \cdot b \]

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

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

\[ (-a) \cdot (-b) = -(a \cdot (-b)) = -(-a \cdot b) = a \cdot b \quad \text{[part (3)]} \]

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

\[ (-1) \cdot a = -(1 \cdot a) = -a \quad \text{and} \quad a \cdot (-1) = -(a \cdot 1) = -a. \]
Ex. \( \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \) and \( \mathbb{C} \) are unital commutative rings.

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

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

\[ = \{ n \in \mathbb{Z} \mid \exists m \in \mathbb{Z}, \ n \cdot m = m \cdot n = 1 \} = \{ 1, -1 \} . \]

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.