Historically algebra was created to understand zeros of polynomial equations. Now, being familiar with symbolic algebra, it is easy for us to find zeros of degree 1 or degree 2 polynomials. In 11th century Khayyam more or less found zeros of a degree 3. We had to wait till 16th century for Ferrari to give us a method of finding zeros of a degree 4 polynomial. In 1824 Abel proved that there is no solution in radicals to the general polynomial equation of degree $\geq 5$. In 1832 Galois taught us how one should study zeros of polynomials. Another problem which had a great deal of influence on shaping modern algebra was Fermat’s Last Conjecture.

In the above mentioned problems, one has to add a zero of a polynomial to either $\mathbb{Q}$ or $\mathbb{Z}$ and see what the properties of the new “system of numbers” are. This is how ring
Definition of ring;
Monday, August 7, 2017 12:43 AM

definition is created.

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.

Def. A ring \((R,+,.\)) 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) \( \forall a, b, c \in R \), \( a \cdot (b \cdot c) = (a \cdot b) \cdot c \).

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 unital if, \( \exists 1 \in R \), \( \forall r \in R \),

\[ 1 \cdot r = r = r \cdot 1 \]  

And such an element \(1_R\) is called the unity or identity of \(R\).

We say \(R\) is commutative if \( \forall a, b \in R \), \( a \cdot b = b \cdot a \).
. \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C} \text{ are unital commutative rings}

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

. \mathbb{M}_n(\mathbb{Q}) := \text{ the set of } n \times n \text{ rational matrixes with addition and multiplication of matrixes is a unital ring which is NOT commutative if } n \geq 2.

In fact, for any ring \( R \), \( \mathbb{M}_n(R) \) is a ring.

(Check why this is the case.)

. \mathbb{Z}^{\geq 0} \text{ is a commutative ring which is NOT unital.}

. \mathbb{Z}_n := \{0,1,...,n-1\}. \forall a,b \in \mathbb{Z}_n, \text{ let } a \oplus b \text{ be the remainder of } a+b \text{ divided by } n, \text{ and } a \otimes b \text{ be the remainder of } ab \text{ divided by } n. \text{ Then } \mathbb{Z}_n \text{ is a unital commutative ring.}

To show this we start by recalling congruence arithmetic.

Def. For two integers \( a \) and \( b \) we say \( a \mid b \) if \( b \) is an integer multiple of \( a \); that means \( b = ak \) for
some integer \( k \). We say \( a \) is congruent to \( b \) modulo \( n \)

for some \( a, b \in \mathbb{Z} \) and \( n \in \mathbb{Z}^+ \) and write \( a \equiv b \pmod{n} \)

or \( a \equiv b \) if \( n \mid a-b \); that means \( a-b=nk \)

for some integer \( k \).

---

### Basic Properties of Congruences

- \( a_1 \equiv a_2 \pmod{n} \) \( \Rightarrow \) \( a_1 \equiv a_3 \pmod{n} \)
  \( a_2 \equiv a_3 \pmod{n} \)

- \( a_1 \equiv a_2 \pmod{n} \) \( \Rightarrow \) \( \exists a_1 + b_1 \equiv a_2 + b_2 \pmod{n} \)
  \( b_1 \equiv b_2 \pmod{n} \)

- \( a_1 \equiv a_2 \pmod{n} \) \( \Rightarrow \) \( a_1 \equiv a_2 \pmod{n} \)
  \( 0 \leq a_1, a_2 < n \)

---

**Proof**

\( a_1 \equiv a_2 \pmod{n} \) \( \Rightarrow \) \( \exists k \in \mathbb{Z} \), \( a_1-a_2 = kn \).

\( b_1 \equiv b_2 \pmod{n} \) \( \Rightarrow \) \( \exists l \in \mathbb{Z} \), \( b_1-b_2 = ln \).

So \( a_1b_1-a_2b_2 = a_1b_1-a_2b_1 + a_2b_1-a_2b_2 \)

\[ = (a_1-a_2)b_1 + a_2(b_1-b_2) \]

\[ = knb_1 + a_2ln = n(kb_1 + a_2) \]

\( \Rightarrow n \mid a_1b_1-a_2b_2 \Rightarrow a_1b_1 \equiv a_2b_2 \pmod{n} \).
Recall. **Division algorithm** For any $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$, there is a unique pair $(q, r)$ of integers such that

1. $0 \leq r < n$
2. $a = nq + r$.

$q$ is called the **quotient** and $r$ is called the **remainder** of $a$ divided by $n$.

**Remark.** If $r$ is the remainder of $a$ divided by $n$, then

$$a \equiv r \pmod{n}.$$ (Why?)

Using the above remark we have:

$$\forall a, b \in \mathbb{Z}_n, \quad a \circ b \equiv a + b \pmod{n} \quad \text{"we can remove the circle!" and} \quad a \circ b \equiv ab \pmod{n}.$$ (Why?)

Part of the argument of why $(\mathbb{Z}_n, \circ, 0)$ is a ring.

$$a \circ 0 \equiv a \circ 0 \equiv a \quad \Rightarrow \quad a \circ 0 = a.$$ (Why?)

$$0 \leq a \circ 0, a < n$$

$$0 \circ a \equiv 0 + a \equiv a \quad \Rightarrow \quad 0 \circ a = a.$$ (Why?)

If $a \neq 0$ and $a \in \mathbb{Z}_n$, then $0 < a < n \Rightarrow 0 < n-a < n$.

So $n-a \in \mathbb{Z}_n$. And $(n-a) \circ a \equiv (n-a) + a \equiv n \equiv 0$. (Why?)
Integers mod $n$ is a ring

So $(n-a) \oplus a = 0$. Similarly $a \oplus (n-a) = 0$.

Complete the argument of why $(\mathbb{Z}_n, \oplus)$ is an abelian group.

**Distribution.** We have to show

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

We "remove circles" one-by-one using the arithmetic congruence.

$$(a \oplus b) \odot c \equiv (a \oplus b) c \pmod{n}. \quad \Box$$

$$a \oplus b \equiv a + b \pmod{n} \Rightarrow (a \oplus b) c \equiv (a + b) c \pmod{n} \quad \Delta$$

$$\Delta, \Box \Rightarrow (a \oplus b) \odot c \equiv (a + b)c \pmod{n}. \quad \ast$$

Similarly $(a \odot c) \oplus (b \odot c) \equiv a \odot c + b \odot c \pmod{n}$

$$a \odot c \equiv ac \pmod{n} \Rightarrow a \odot c + b \odot c \equiv ac + bc \pmod{n} \quad \Delta$$

$$b \odot c \equiv bc \pmod{n} \quad \Box$$

$$\Delta, \Box \Rightarrow (a \odot c) \oplus (b \odot c) \equiv ac + bc \pmod{n} \quad \ast$$

$\ast, \Box, \ast \ast$, and $(a+b)c = ac+bc$ imply

$$(a \oplus b) \odot c \equiv (a \odot c) \oplus (b \odot c) \pmod{n}$$

And so $(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$.

Complete the rest of the proof. \[\blacksquare\]
Ex. Write the multiplication and the addition table of $\mathbb{Z}_4$.

Solution.

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>.</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>

We will not use $\oplus$ or $\odot$ for the operations of $\mathbb{Z}_n$ anymore, observe that there is no 1 in this row.

So, 2 does not have a multiplicative inverse in $\mathbb{Z}_4$.

$2 \times 1 = 2 \times 3$  \[2 \neq 3\].

So in $\mathbb{Z}_4$ we do not have cancellation.

Ex. Find all the solutions of $x^2 - x = 0$ in $\mathbb{Z}_5$ and $\mathbb{Z}_6$.

Solution.

<table>
<thead>
<tr>
<th>x</th>
<th>$x - 1$</th>
<th>$x(x - 1) = x^2 - x$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>

So there are exactly two solutions $x = 0$ or $1$.

明确了$x^2 - x = 0$ in $\mathbb{Z}_5$.

<table>
<thead>
<tr>
<th>x</th>
<th>$x - 1$</th>
<th>$x(x - 1)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>2</td>
</tr>
</tbody>
</table>

So there are exactly 4 solutions: $x = 0, 1, 3, 4$. 

in $\mathbb{Z}_6$. 

So there are exactly 4 solutions: $x = 0, 1, 3, 4$. 

in $\mathbb{Z}_6$. 

Suppose $R_1, R_2, \ldots, R_n$ are rings. Then the direct product $R_1 \times \cdots \times R_n$ is a ring with componentwise operations; that means

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n).$$

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 \cdot b_1, \ldots, a_n \cdot b_n).$$

It is easy to see that $R_1 \times \cdots \times R_n$ is a ring.

Notice if $R_i$'s are unital rings, then

$$(1_{R_1}, \ldots, 1_{R_n})$$

is the unity of $R_1 \times \cdots \times R_n$. (why?)

Ex. Write the multiplication table of $\mathbb{Z}_2 \times \mathbb{Z}_3$.

<table>
<thead>
<tr>
<th></th>
<th>(0, 0)</th>
<th>(0, 1)</th>
<th>(0, 2)</th>
<th>(1, 0)</th>
<th>(1, 1)</th>
<th>(1, 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0, 0)</td>
<td>(0, 0)</td>
<td>(0, 0)</td>
<td>(0, 0)</td>
<td>(0, 0)</td>
<td>(0, 0)</td>
<td>(0, 0)</td>
</tr>
<tr>
<td>(0, 1)</td>
<td>(0, 0)</td>
<td>(0, 1)</td>
<td>(0, 2)</td>
<td>(0, 0)</td>
<td>(0, 1)</td>
<td>(0, 2)</td>
</tr>
<tr>
<td>(0, 2)</td>
<td>(0, 0)</td>
<td>(0, 0)</td>
<td>(0, 2)</td>
<td>(0, 0)</td>
<td>(0, 0)</td>
<td>(0, 2)</td>
</tr>
<tr>
<td>(1, 0)</td>
<td>(0, 0)</td>
<td>(1, 0)</td>
<td>(0, 0)</td>
<td>(1, 0)</td>
<td>(1, 0)</td>
<td>(1, 0)</td>
</tr>
<tr>
<td>(1, 1)</td>
<td>(0, 0)</td>
<td>(0, 1)</td>
<td>(0, 2)</td>
<td>(1, 0)</td>
<td>(1, 1)</td>
<td>(1, 2)</td>
</tr>
<tr>
<td>(1, 2)</td>
<td>(0, 0)</td>
<td>(0, 2)</td>
<td>(0, 1)</td>
<td>(1, 0)</td>
<td>(1, 2)</td>
<td>(1, 1)</td>
</tr>
</tbody>
</table>

As in group theory, what is important is the algebraic structure and not the underlying set; so next we define homomorphism and isomorphism.
Def. Let $R$ and $R'$ be two rings. A map $\phi : R \rightarrow R'$ is called a (ring) homomorphism if

1. $\phi$ is a group homomorphism of $(R,+)$.
2. $\phi(ab) = \phi(a) \phi(b)$ for any $a,b \in R$.

A bijective homomorphism $\phi : R \rightarrow R'$ is called an isomorphism. We say $R$ is isomorphic to $R'$ and write $R \cong R'$ if there is an isomorphism $\phi : R \rightarrow R'$.

Remark. 1. can be replaced with $\phi(a+b) = \phi(a) + \phi(b)$.

Notice that, if $\phi(a+b) = \phi(a) + \phi(b)$, then

- $\phi(0) = \phi(0+0) = \phi(0) + \phi(0) \Rightarrow \phi(0) = 0$
- $\phi(0) = \phi(a+(-a)) = \phi(a) + \phi(-a) \Rightarrow \phi(-a) = -\phi(a)$.

So $\phi$ is a group homomorphism of $(R,+)$.

In the next lecture we will prove:

Lemma. Suppose $m,n \in \mathbb{Z}$ and $\gcd(m,n)=1$. Then $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$. 