Introduction

Sunday, August 6, 2017 11:57 PM

. 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 11 century Khayyam more or less found zeros of a degree 3. We had to wait till 16^{th} 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 ≥ 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

theory 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 $(R,+,\cdot)$ 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) $\forall a,b,c\in R$, $a\cdot(b\cdot c)=(a\cdot b)\cdot c$.

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, $\exists\, 1_R\in R$, $\forall\, r\in R$,

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

Notice that, if 1_R and $1'_R$ are two unities, then $1_R=1_R\cdot 1'_R=1'_R$.

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

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

Examples

Monday, August 7, 2017 12:59 AM

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are unital commutative rings
- $\mathbb{Z}^{\geq 0}$ is NOT a ring as $(\mathbb{Z}^{\geq 0}, +)$ is NOT a group.
- $M_n(\mathbb{Q}) :=$ the set of $n \times n$ 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, $M_n(R)$ is a ring.

  (Check why this is the case.)
- $2\mathbb{Z}$ is a commutative ring which is NOT unital.
- $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$. $\forall a, b \in C_n$, let $a \oplus b$ be the remainder of $a+b$ divided by n, and $a \odot b$ be the remainder of ab divided by n. Then $\mathbb{Z}_n$ is a unital commutative ring.

To show this we start by recalling <u>congruence arithmetic</u>.

<u>Def.</u> For two integers a and b we say $a \mid b$ if b is an integer multiple of a; that means $b = a\,k$ for

Congruences

Monday, August 7, 2017 1:23 AM

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 $a \overset{n}{\equiv} b$ if $n \mid a-b$; that means $a-b = nk$

for some integer k.

Basic Properties of congruences.

- $\left.\begin{array}{l} a_1 \equiv a_2 \pmod{n} \\ a_2 \equiv a_3 \pmod{n} \end{array}\right\} \Rightarrow a_1 \equiv a_3 \pmod{n}$

- $\left.\begin{array}{l} a_1 \equiv a_2 \pmod{n} \\ b_1 \equiv b_2 \pmod{n} \end{array}\right\} \Rightarrow \begin{cases} a_1 + b_1 \equiv a_2 + b_2 \pmod{n} \\ a_1 b_1 \equiv a_2 b_2 \pmod{n} \end{cases}$ ⊛

- $\left.\begin{array}{l} a_1 \equiv a_2 \pmod{n} \\ 0 \le a_1, a_2 < n \end{array}\right\} \Rightarrow a_1 = a_2$

Proof of ⊛

$a_1 \overset{n}{\equiv} a_2 \Rightarrow \exists k \in \mathbb{Z},\ a_1 - a_2 = kn.$

$b_1 \overset{n}{\equiv} b_2 \Rightarrow \exists l \in \mathbb{Z},\ b_1 - b_2 = ln.$

So
$$a_1 b_1 - a_2 b_2 = a_1 b_1 - a_2 b_1 + a_2 b_1 - a_2 b_2$$
$$= (a_1 - a_2) b_1 + a_2 (b_1 - b_2)$$
$$= kn b_1 + a_2 l n = n(\underbrace{k b_1 + l a_2}_{\text{an integer}})$$

$\Rightarrow n \mid a_1 b_1 - a_2 b_2 \Rightarrow a_1 b_1 \equiv a_2 b_2 \pmod{n}$. ∎

Division algorithm and congruences

Monday, August 7, 2017 8:36 AM

<u>Recall</u>. <u>Division algorithm</u> 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.

<u>Remark</u>. If r is the remainder of a divided by n, then $a \equiv r \pmod{n}$. (why?)

Using the above remark we have:

$\forall a, b \in \mathbb{Z}_n$, $a \oplus b \equiv a + b \pmod{n}$ "we can remove the circle!" and $a \odot b \equiv ab \pmod{n}$.

<u>Part of the argument of why $(\mathbb{Z}_n, \oplus, \odot)$ is a ring</u>.

$$\left.\begin{array}{l} a \oplus 0 \overset{n}{\equiv} a + 0 \overset{n}{\equiv} a \\ 0 \leq a \oplus 0, a < n \end{array}\right\} \Rightarrow a \oplus 0 = a.$$

$$0 \oplus a \overset{n}{\equiv} 0 + a \overset{n}{\equiv} a \Rightarrow 0 \oplus a = a.$$

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 $(n-a) \oplus a \overset{n}{\equiv} (n-a) + a \overset{n}{\equiv} n \overset{n}{\equiv} 0$.

Integers mod n is a ring

Monday, August 7, 2017 8:41 AM

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.

<u>Distribution</u>. 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.

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

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

$$\text{I}, \text{II} \Rightarrow (a \oplus b) \odot c \equiv (a+b) c \pmod{n}. \quad (*)$$

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

$$\left.\begin{array}{l} a \odot c \equiv ac \pmod{n} \\ b \odot c \equiv bc \pmod{n} \end{array}\right\} \Rightarrow a \odot c + b \odot c \equiv ac + bc \pmod{n} \quad \text{IV}$$

$$\text{III}, \text{IV} \Rightarrow (a \odot c) \oplus (b \odot c) \equiv ac + bc \pmod{n} \quad (**)$$

$(*)$, $(**)$, 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. ∎

Computation in integers mod n

Monday, August 7, 2017 12:06 PM

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

Solution.

we will not use $\oplus, \odot$ for the operations of $\mathbb{Z}_n$ anymore

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

observe that there is no 1 in this row. So 2 does not have a multiplicative inverse in $\mathbb{Z}_4$

$2 \times 1 = 2 \times 3$ and $1 \neq 3$.

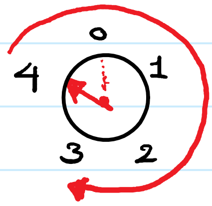
So in $\mathbb{Z}_4$ we do not have cancellation.

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

Solution.

x	$x-1$	$x(x-1) = x^2 - x$
0	4	0
1	0	0
2	1	2
3	2	1
4	3	2

in $\mathbb{Z}_5$

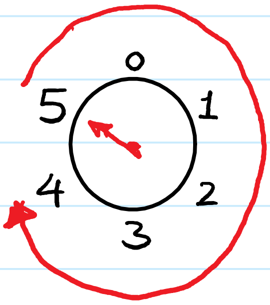


$x-1$

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

x	$x-1$	$x(x-1)$
0	5	0
1	0	0
2	1	2
3	2	0
4	3	0
5	4	2

in $\mathbb{Z}_6$



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

Direct product of rings

Monday, August 7, 2017 2:09 PM

Suppose $R_1, R_2, \dots, R_n$ are rings. Then the <u>direct product</u> $R_1 \times \dots \times R_n$ is a ring with componentwise operations; that means

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

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

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

<u>Notice</u> if R_i's are unital rings, then

$(1_{R_1}, \dots, 1_{R_n})$ is the unity of $R_1 \times \dots \times R_n$. (why?)

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

<u>Solution.</u>

	$\cdot$	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
No cancellation	(0,1)	(0,0)	(0,1)	(0,2)	(0,0)	(0,1)	(0,2)
	(0,2)	(0,0)	(0,2)	(0,1)	(0,0)	(0,2)	(0,1)
	(1,0)	(0,0)	(0,0)	(0,0)	(1,0)	(1,0)	(1,0)
the unity	(1,1)	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
	(1,2)	(0,0)	(0,2)	(0,1)	(1,0)	(1,2)	(1,1)

Product of two non-zero element might be (0,0).

As in group theory, what is important is the algebraic structure and not the underlying set: so next we define homomorphism and isomorphism.

Homomorphism and isomorphism

Monday, August 7, 2017 2:27 PM

<u>Def.</u> Let R and R' be two rings. A map $\phi : R \to R'$ is called a (ring) homomorphism if

① ϕ is a group homomorphism of $(R,+)$.

② $\phi(ab) = \phi(a)\phi(b)$ for any $a, b \in R$.

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

<u>Remark</u>. 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 ϕ is a group homomorphism of $(R,+)$.

In the next lecture we will prove:

<u>Lemma</u>. Suppose $m, n \in \mathbb{Z}$ and $\gcd(m,n) = 1$. Then

$$\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n.$$