Lecture 06: Ring of polynomials

Wednesday, August 16, 2017 1:59 AM

You have seen and worked with real or complex polynomials in a given variable x. We can and will consider polynomials with coefficients in a given ring in an <u>indeterminant</u> x:

$$R[x] = \{ a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \mid n \in \mathbb{Z}^{\geq 0},\ a_i \in R \}.$$

We sometimes write $\sum_{i=0}^{n} a_i x^i$ instead of $a_0 + a_1 x + \cdots + a_n x^n$. Or $\sum_{i=0}^{\infty} a_i x^i$ with an understanding that $a_{n+1} = a_{n+2} = \cdots = 0$ for some $n \in \mathbb{Z}^{\geq 0}$.

$R[x]$ with the usuall $+$ and $\cdot$ is a ring. Here is the formal definition:

$$\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i + b_i) x^i, \quad \text{and}$$

$$\left(\sum_{i=0}^{\infty} a_i x^i\right)\left(\sum_{i=0}^{\infty} b_i x^i\right) = \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} a_i b_{n-i}\right) x^n .$$

<u>Ex.</u> Find $(x+1)^5$ in $\mathbb{Z}_4[x]$.

<u>Solution</u> $(x+1)^2 = x^2 + 2x + 1$.

$$\begin{aligned}(x+1)^4 = (x^2+2x+1)^2 &= x^4 + 2x^3 + x^2 \\ &\quad + 2x^3 + 0 + 2x \\ &\quad + x^2 + 2x + 1\end{aligned}$$

$$= x^4 + 2x^2 + 1 \Rightarrow (x+1)^5 = x^5 + x^4 + 2x^3 + 2x^2 + x + 1.$$

Lecture 06 : degree of polynomials

Thursday, August 17, 2017 11:15 PM

For $f(x) = \sum_{i=0}^{\infty} a_i x^i \in R[x]$, we say

$$\deg f = \max\{n \in \mathbb{Z}^+ \cup \{-\infty\} \mid a_n \neq 0\}.$$

So, degree of the zero polynomial is defined to be $-\infty$;

and $\deg(a_0 + a_1 x + \cdots + a_n x^n) = n$ if $a_n \neq 0$.

<u>Ex.</u> $\deg(1) = 0$ in any (non-zero) unital ring.

<u>Ex.</u> Find $\deg((2x^2-1)(2x+1))$ in $\mathbb{Z}_4[x]$.

<u>Solution</u>. $(2x^2-1)(2x+1) = 2^2 x^3 + 2x^2 - 2x - 1$

$$= 2x^2 - 2x - 1.$$

So $\deg((2x^2-1)(2x+1)) = 2$.

Notice that in the above example

$$\deg(2x^2-1) = 2, \quad \deg(2x+1) = 1, \text{ and}$$

$$\deg((2x^2-1)(2x+1)) = 2 \neq 2+1 = \deg(2x^2-1) + \deg(2x+1)$$

So, for a general ring R, in $R[x]$ we do <u>NOT</u> have

$$\deg(fg) = \deg f + \deg g.$$

Lecture 06 : Degree of product

Thursday, August 17, 2017 11:28 PM

A closer look at the previous example shows us why this equality fails; it fails because of the zero divisors.

<u>Lemma</u>. Suppose R is a ring with no zero divisors. Then for any $f, g \in R[x]$, we have

$$\deg fg = \deg f + \deg g.$$

<u>Proof</u>. If either f or g is zero, then $fg = 0$.

So the LHS $= -\infty$ and the RHS $= -\infty + \cdots = -\infty$

(as a convention : $-\infty + n = -\infty$ and $(-\infty) + (-\infty) = -\infty$.)

Suppose f and g are not zero; and

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \;,\quad a_n \neq 0 \;,$$

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0 \;,\quad b_m \neq 0 .$$

Then $f(x) g(x) = a_n b_m x^{n+m} + (\text{terms of degree} < n+m)$.

Since $a_n, b_m \neq 0$ and R has no zero divisors, $a_n b_m \neq 0$.

Hence $\deg fg = n+m = \deg f + \deg g$. ∎

<u>Corollary</u>. If R has no zero divisors, then $R[x]$ does not

has no zero divisors. If D is an integral domain, then $D[x]$ is an integral domain.

Proof. If $fg=0$, then $\deg fg = -\infty$. Since R has no zero divisors, by Lemma, $\deg fg = \deg f + \deg g$. Since two integers cannot add up to $-\infty$, either $\deg f = -\infty$ or $\deg g = -\infty$; which implies either $f=0$ or $g=0$. Hence $R[x]$ does NOT have a zero divisor.

If D is an integral domain, then

1. D is a non-zero unital ring $\Rightarrow$ $D[x]$ is a non-zero unital ring.
2. D is commutative $\Rightarrow$ $D[x]$ is commutative
3. D does NOT have a zero-divisor $\Rightarrow$ $D[x]$ does not have a zero-divisor.

Justify 1 and 2; 3 has been proved in the first part of this argument. ■

Lemma Suppose D is an integral domain. Then $D[x]^\times = D^\times$.

Pf. Suppose $f \in D[x]^\times$. Then $\exists\, g(x) \in D[x]$ s.t. $f(x)g(x)=1$.

Lecture 06 : Units of a ring of polynomials

Thursday, August 17, 2017 11:50 PM

Since D has no zero-divisors, we have

$$0 = \deg fg = \deg f + \deg g \, .$$

Notice that, since $fg \neq 0$, f and g are NOT zero. So

$\deg f, \deg g \geq 0$.

$$\left.\begin{array}{l} \deg f + \deg g = 0 \\ \deg f, \deg g \geq 0 \end{array}\right\} \Rightarrow \deg f = \deg g = 0 \; ; \text{ so}$$

$\exists\, a_0, b_0 \in D \setminus \{0\}$ s.t. $f(x) = a_0$ and $g(x) = b_0$.

Hence $a_0 b_0 = 1$, which implies $a_0 \in D^\times$. Therefore

$f \in D^\times$; which implies $D[x]^\times \subseteq D^\times$. I

Since D and $D[x]$ have the same (multiplicative) identity,

it is clear that $D^\times \subseteq D[x]^\times$ II. Therefore by I, II

one gets the claim. ■

<u>Ex.</u> $\mathbb{Z}[x]^\times = \{-1, 1\}$; $\mathbb{Q}[x]^\times = \mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$.

<u>Ex.</u> For a general ring R, $R[x]^\times$ might be much larger than

$R^\times$: show that $1 + 2x \in \mathbb{Z}_4[x]^\times$.

<u>Solution</u>. $(1+2x)(1-2x) = 1 - 2^2 x^2 = 1 = (1-2x)(1+2x)$. ■

Lecture 06 : nilpotent elements and units.

Friday, August 18, 2017 12:00 AM

A closer look at the previous example shows that the key property is the fact that $2^2=0$ in $\mathbb{Z}_4$; we say 2 is a nilpotent element: In a ring R, an element $a\in R$ is called nilpotent if $\exists\, m\in\mathbb{Z}^+$ s.t. $a^m=0$.

It is a good exercise to show that in a unital commutative ring R, we have

$$a_0+a_1x+\cdots+a_nx^n\in R[x]^\times \Leftrightarrow a_0\in R^\times \text{ and } a_1,\dots,a_n \text{ are nilpotent.}$$

The following is the key reason on why the above holds:

<u>Theorem</u>. Suppose R is a unital ring and $a\in R$ is nilpotent. Then $1-a\in R^\times$.

<u>Pf</u>. Suppose $a^n=0$. Then

$$(1-a)(1+a+a^2+\cdots+a^{n-1})=1-a^n=1.$$

(Similarly $(1+a+\cdots+a^{n-1})(1-a)=1$.) Hence $1-a\in R^\times$. ∎

Lecture 06 : Polynomials vs functions

Monday, February 18, 2019 7:19 PM

Prior to this course, you have viewed a polynomial $f \in \mathbb{R}[x]$ as a function from $\mathbb{R}$ to $\mathbb{R}$. But there is a subtle difference between them. For instance there are only 4 functions from $\mathbb{Z}_2$ to $\mathbb{Z}_2$, but there are infinitely may polynomials in $\mathbb{Z}_2[x]$: $\deg(x^n) = n$ and so $x, x^2, x^3, \ldots$ are distinct polynomials ($\sum a_i x^i = \sum b_i x^i \Leftrightarrow \forall i, a_i = b_i$.). They are however, equal as <u>functions</u>:

x	x^m
0	0
1	1

An extremely important property of ring of polynomials is the fact that we have a division algorithm:

<u>Theorem</u>. Suppose R is an integral domain. Let
$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ and
$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0$. Suppose $b_m \in R^\times$.

Then $\exists\, q(x) \in R[x]$ (called the quotient) and $r(x) \in R[x]$ (called the remainder) s.t.

① $f(x) = q(x)\, g(x) + r(x)$ ② $\deg r < \deg g$.

Moreover such pair (q, r) is unique.

Lecture 06: Division algorithm

Friday, August 18, 2017 1:08 AM

In class we proved the existence first and then showed the uniqueness when R is an integral domain.

<u>Proof of existence.</u> We proceed by the strong induction on $\deg(f)$. To do so first we have to address the case of $f=0$.

<u>Case of $f=0$.</u> Set $q=r=0$. Then

① $\deg r=-\infty<m=\deg g$. ② $f=0=0\times g+0$.

<u>Base of induction.</u> $\deg f=0$. Then $f(x)=a_0$ and $a_0\neq 0$.

<u>Case 1.</u> $\deg g=m>0$.

Set $q=0$ and $r(x)=a_0$. Then

① $\deg r=0<m=\deg g$. ② $f=a_0=0\times g(x)+r$

<u>Case 2.</u> $\deg g=m=0$

Then $g(x)=b_0$ and $b_0\in R^\times$.

Set $q(x)=a_0b_0^{-1}$ and $r(x)=0$. Then

① $\deg r=-\infty<0=\deg g$. ② $f(x)=a_0=\underbrace{(a_0b_0^{-1})}_{q}\,\underbrace{b_0}_{g}+\underbrace{0}_{r}$.

Lecture 06: Division algorithm (existence)

Friday, August 18, 2017 12:53 PM

Strong induction step. Suppose for any polynom. of deg $< k$ we can find a quotient and a remainder, and we want to get the same result for $f(x)$ with degree k.

Case 1. $\deg f = k < \deg g = m$.

Set $q = 0$ and $r(x) = f(x)$; check ① and ②.

Case 2. $\deg f = k \geq \deg g = m$.

So $f(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_0$ and $a_k \neq 0$.

We look for a monomial, i.e. $\square x^{\square}$, s.t. the leading term of $\underline{\square x^{\square} g(x)}$ is the same as the leading term $a_k x^k$ of $f(x)$.

That means we'd like to have $(\square x^{\square})(b_m x^m) = a_k x^k$.

So the monomial is $a_k b_m^{-1} x^{k-m}$ (notice that $k-m \geq 0$, and so $a_k b_m^{-1} x^{k-m}$ is a monomial). Hence

$$\deg\left(f(x) - a_k b_m^{-1} x^{k-m} g(x)\right) < k.$$

So by the strong induction hypothesis there are $q_1(x), r_1(x) \in R[x]$

Lecture 06: Division algorithm (existence)

Thursday, February 21, 2019 1:22 AM

s.t. ① $\deg r_1 < \deg g$

② $f(x) - a_k b_m^{-1} x^{k-m} g(x) = q_{r_1}(x)\, g(x) + r_1(x)$.

② implies that $f(x) = (a_k b_m^{-1} x^{k-m} + q_{r_1}(x))\, g(x) + r_1(x)$. ⊛

Let $r(x) = r_1(x)$ and $q(x) = a_k b_m^{-1} x^{k-m} + q_{r_1}(x)$.

Then ① implies $\deg r < \deg g$ and ⊛ gives us

$f(x) = q(x)\, g(x) + r(x)$. ∎