Ring of polynomials: degree

Thursday, August 17, 2017 11:15 PM

In the previous lecture we defined the ring of polynomials with coefficients in a ring R with an indeterminate x.

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 $a_n \neq 0$.

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

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

Solution. $(2x^2-1)(2x+1) = 2^2 x^3 + 2x^2 - 2x - 1$

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

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 NOT have

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

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

Units of a ring of polynomials

Thursday, August 17, 2017 11:38 PM

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

<u>Proof</u>. 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. ■

<u>Lemma</u> Suppose D is an integral domain. Then $U(D[x]) = U(D)$.

<u>Pf</u>. Suppose $f \in U(D[x])$. Then $\exists\, g(x) \in D[x]$ s.t. $f(x)g(x) = 1$.

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 $a_0 \in U(D)$. Therefore $f \in U(D)$; which implies $U(D[x]) \subseteq U(D)$. I

Since D and $D[x]$ have the same (multiplicative) identity, it is clear that $U(D) \subseteq U(D[x])$. II Therefore by I, II one gets the claim. ■

Ex. $U(\mathbb{Z}[x]) = \{-1, 1\}$; $U(\mathbb{Q}[x]) = \mathbb{Q} \setminus \{0\}$.

Ex. For a general ring R, $U(R[x])$ might be much larger than $U(R)$: show that $1 + 2x \in U(\mathbb{Z}_4[x])$.

Solution. $(1+2x)(1-2x) = 1 - 2^2 x^2 = 1 = (1-2x)(1+2x)$. ■

Polynomials vs functions

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

$$a_0 + a_1 x + \cdots + a_n x^n \in U(R[x]) \Leftrightarrow a_0 \in U(R) \text{ and } a_1, \ldots, a_n \text{ are nilpotent.}$$

Prior to this course, you have viewed a polynomial $f \in R[x]$ as a function from R to 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

Fermat's theorem

Friday, August 18, 2017 12:16 AM

In fact we have:

Theorem. For any prime p and $a \in \mathbb{Z}_p$, we have

$$a^p = a.$$

Pf. If $a=0$, then $a^p=0$; and there is nothing to prove.

If $a \neq 0$, then $a \in \{1, \dots, p-1\}$. Since p is prime, $\gcd(a,p)=1$. Hence $a \in U(\mathbb{Z}_p)$. Therefore

$$l_a : \mathbb{Z}_p \to \mathbb{Z}_p, \quad l_a(b) = ab \text{ is a bijection.}$$

Hence $\{1, 2, \dots, p-1\} = \{(1)(a), (2)(a), \dots, (p-1)(a)\}$

$\Rightarrow \quad (p-1)! = (p-1)!\, a^{p-1}$ in $\mathbb{Z}_p$.

Since $1, 2, \dots, p-1 \in U(\mathbb{Z}_p)$, $(p-1)! \in U(\mathbb{Z}_p)$. So we can cancel it out; and get $1 = a^{p-1}$. Hence $a^p = a$. ■

So as two functions on $\mathbb{Z}_p$ we have $x^p = x$ but as two polynomials we have $x^p \neq x$.

Being aware of this issue, we still want to view a polyn. as a function and evaluate it at a given point $a \in R$.

The evaluation map

Friday, August 18, 2017 12:25 AM

For $a \in R$, let $\phi_a : R[x] \longrightarrow R$ be

$$\phi_a(f(x)) = f(a).$$

It is called the <u>evaluation at a</u>; and we will study it in the next lecture.