Lecture 16: More thorough study of ring of polynomials

Wednesday, May 9, 2018 11:16 AM

In the previous lecture we saw the importance of having certain methods of finding out if a given polynomial is irreducible or not. So we focus on ring of polynomials for now. Recall

$\deg(a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0) = n$ if $a_n \neq 0$ and

$\deg(0) = -\infty$.

Then we proved:

<u>Lemma</u>. Suppose D is an integral domain. Then

$$\forall f, g \in D[x], \quad \deg(fg) = \deg f + \deg g.$$

We were proving the following:

<u>Proposition</u>. Suppose D is an integral domain. Then

(1) $D[x]$ is an integral domain.

(2) $U(D[x]) = U(D)$; in particular, if F is a field, then $U(F[x]) = \{ f(x) \in F[x] \mid \deg f = 0 \} = F \setminus \{0\}$.

<u>Pf.</u> (1) Suppose to the contrary $f, g \in D[x] \setminus \{0\}$ and $fg = 0$. Then $\deg f, \deg g \in \mathbb{Z}^{\geq 0}$, and $\deg(fg) = -\infty$, which contradicts

Lecture 16: Ring of polynomials

Wednesday, May 9, 2018 11:40 AM

the previous lemma.

(2) Suppose $f(x) \in U(D[x])$. So $\exists\, g(x) \in D[x]$ s.t.

$$f(x) \cdot g(x) = 1.$$

Hence $\deg fg = \deg 1 = 0$, which implies

$$0 = \deg f + \deg g \text{ ; and so } \deg f = \deg g = 0.$$

Hence $f(x) = a_0 \in D$ and $g(x) = b_0 \in D$ and $a_0 b_0 = 1$.

therefore $a_0 \in U(D)$; this implies $U(D[x]) \subseteq U(D)$. (I)

. Since D is a subring of $D[x]$, $U(D) \subseteq U(D[x])$. (II)

(I) and (II) imply $U(D) = U(D[x])$. ∎

Ex. • $U(\mathbb{Z}[x]) = U(\mathbb{Z}) = \{\pm 1\}$

• $U(\mathbb{Q}[x]) = U(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$

Ex. In $\mathbb{Z}_{16}[x]$, there are some non-constant units:

$1 - 2x \in U(\mathbb{Z}_{16}[x])$.

Solution. $1 = 1 - (2x)^4 = (1-2x)(1 + (2x) + (2x)^2 + (2x)^3)$. ∎

The following is a good exercise:

Lecture 16: Factor theorem

Wednesday, May 9, 2018 4:26 PM

$a_0 + a_1 x + \cdots + a_n x^n \in U(R[x]) \iff a_0 \in U(R)$ and $a_1, \ldots, a_n$ are nilpotent

that means $a_i^m = 0$.

($\Leftarrow$) You can prove. ($\Rightarrow$) more tools are needed.

<u>Theorem</u>. Suppose F is a field, $c \in F$, $f(x) \in F[x]$. Then

$\exists\, q(x) \in F[x]$ s.t. $f(x) = (x-c)\, q(x) + f(c)$.

In particular, c is a zero of f if and only if $\exists\, q(x) \in F[x]$

s.t. $f(x) = q(x)\,(x-c)$.

<u>Pf.</u> By the long division, $\exists\, q(x), r(x) \in F[x]$ s.t.

$f(x) = q(x)(x-c) + r(x)$ and $\deg r < \deg x-c = 1$. And so $r(x)$

is a constant polynomial. Evaluating at c we get

$$f(c) = \underbrace{q(c)\,(c-c)}_{0} + r(c) \Rightarrow r(c) = f(c).$$

Since $r(x)$ is constant, $r(x) = f(c)$. And so

$$f(x) = q(x)\,(x-c) + f(c). \qquad (\mathrm{I})$$

. If c is a zero of f, then $f(c) = 0$. Therefore by (I) $f(x) = q(x)(x-c)$.

. If $f(x) = q(x)\,(x-c)$, then $f(c) = q(c)\,(c-c) = 0$. ∎

Lecture 16: Number of zeros of a polynomial

Wednesday, May 9, 2018 5:03 PM

Proposition. Suppose F is a field, $f(x) \in F[x]$ is a polynomial of degree $n > 0$.

(a) If $c_1, \ldots, c_m \in F$ are distinct zeros of f, then $\exists g(x) \in F[x]$ s.t. $f(x) = (x - c_1) \cdots (x - c_m)\, g(x)$.

(b) $f(x)$ has at most n distinct zeros in F.

Pf. (a) We proceed by induction on m.

Base of induction. $m = 1$. By the factor theorem, $\exists g(x) \in F[x]$, $f(x) = (x - c_1)\, g(x)$.

Induction step. Suppose $c_1, \ldots, c_{m+1}$ are distinct zeros in F of $f(x)$. Then by the induction hypothesis, $\exists g(x) \in F[x]$ s.t.

(I) $f(x) = (x - c_1) \cdots (x - c_m)\, g(x)$. And so

$$0 = f(c_{m+1}) = \underbrace{(c_{m+1} - c_1)}_{\neq 0} \underbrace{(c_{m+1} - c_2)}_{\neq 0} \cdots\cdots \underbrace{(c_{m+1} - c_m)}_{\neq 0}\, g(c_{m+1})$$

Since F has no zero-divisors, $g(c_{m+1}) = 0$. Hence by the factor theorem $\exists q(x) \in F[x]$, $g(x) = (x - c_{m+1})\, q(x)$. And so by (I)

$f(x) = (x - c_1) \cdots (x - c_m)(x - c_{m+1})\, q(x)$.

Lecture 16: Number of zeros of a polynomial

Wednesday, May 9, 2018 5:56 PM

(b) Suppose to the contrary that $\exists\, c_1, \dots, c_{n+1}$ zeros of f.

Then by part (a), $f(x) = (x-c_1)(x-c_2)\cdots(x-c_{n+1})\, g(x)$

for some $g(x) \in F[x]$.

And so $$n = \deg f = \deg(x-c_1) + \dots + \deg(x-c_{n+1}) + \deg g$$
$$= n+1+\deg g.$$

Therefore $\deg g = -1$ which is a contradiction. ∎

<u>Recall</u>. Suppose $\mathrm{Char}(R) = p > 0$ is prime. Then

$f: R \to R$, $f(r) = r^p$ is a ring hom. This is called the

Frobenius map. Consider the Frob. map $f: \mathbb{Z}_p \to \mathbb{Z}_p$,

$f(r) = r^p$. Then for any $a \in \mathbb{Z}_p$,

$$f(a) = f(\underbrace{1+\dots+1}_{a \text{ times}}) = \underbrace{f(1)+\dots+f(1)}_{a \text{ times}} = \underbrace{1+\dots+1}_{a \text{ times}} = a$$

$\Rightarrow a^p = a$.

<u>Fermat's little theorem</u>. $\forall a \in \mathbb{Z}_p$, $a^p = a$.

. Before this you have been working with polynomials in your calc.

courses. But you mainly viewed them as functions. In this course

Lecture 16: Polynomials and functions

Wednesday, May 9, 2018 6:11 PM

there is a subtle difference between a polynomial $f(x) \in F[x]$ and its underlying function. For instance x and $x^p \in \mathbb{Z}_p[x]$ are two different polynomials one of them has degree 1 and the other one has degree p, but as functions from $\mathbb{Z}_p$ to $\mathbb{Z}_p$, they are equal as Fermat's little theorem implies.