The evaluation homomorphisms

Friday, August 18, 2017 12:29 AM

In the previous lecture we defined <u>the evalution at a</u>:

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

Since both $R[x]$ and R have distribution law, when R is a commutative ring, it is easy to see that

$$\phi_a(f+g) = \phi_a(f) + \phi_a(g)$$

and

$$\phi_a(f\,g) = \phi_a(f)\,\phi_a(g);$$

which means:

<u>Proposition.</u> Let $R_1 \subseteq R_2$ be commutative rings. Then for any $a \in R_2$, $\phi_a : R_1[x] \to R_2$, $\phi_a(f) = f(a)$ is a ring homomorphism.

(Its proof is straightforward; justify this for yourself.)

<u>Ex.</u> The evaluation ϕ_0 at 0 maps $a_0 + a_1 x + \cdots + a_n x^n$ to the constant term. And so

$$\ker \phi_0 = x\,R[x] := \text{the set of multiples of } x.$$
$$= \{ a_1 x + a_2 x^2 + \cdots + a_n x^n \mid a_i \in R \}.$$

The evaluation homomorphisms

Friday, August 18, 2017 12:44 AM

Ex. Give one non-zero element of $\ker(\phi_i)$ where

$\phi_i : \mathbb{Q}[x] \to \mathbb{C}$ is the evaluation at i;

$\phi_i(f(x)) = f(i)$ where $i^2 = -1$.

Solution. $f \in \ker(\phi_i) \Leftrightarrow f(i) = 0$.

So we need to find $f(x) \in \mathbb{Q}[x]$ s.t. i is a zero of f. By the definition of i we know that it is a zero of x^2+1. So $x^2+1 \in \ker \phi_i$. ■

Ex. Find all $a \in \mathbb{C}$ s.t. $x^2 - x - 12 \in \ker \phi_a$ where

$\phi_a : \mathbb{Q}[x] \to \mathbb{C}$ is the evaluation at a.

Solution. $x^2 - x - 12 \in \ker \phi_a \Leftrightarrow \phi_a(x^2 - x - 12) = 0$

$\Leftrightarrow a^2 - a - 12 = 0$

$\Leftrightarrow (a-4)(a+3) = 0$ in $\mathbb{C}$ (and $\mathbb{C}$ is a field.)

$\Leftrightarrow a = 4$ or $a = -3$. ■

Ex. Find a non-zero element of $\ker(\phi_{\sqrt{2}})$ where

$\phi_{\sqrt{2}} : \mathbb{Q}[x] \to \mathbb{C}$ is the evaluation at $\sqrt{2}$.

Solution. $f \in \ker \phi_{\sqrt{2}} \Leftrightarrow f(\sqrt{2}) = 0$.

The evaluation homomorphisms

Friday, August 18, 2017 12:54 AM

So we need to find a polynomial which has a zero at $\sqrt{2}$.

By the definition of $\sqrt{2}$, we have that it is a zero of x^2-2. So $x^2-2 \in \ker \phi_{\sqrt{2}}$. ■

Ex. Is there a non-zero element in $\ker \phi_{\pi}$ where $\phi_{\pi} : \mathbb{Q}[x] \to \mathbb{C}$ is the evaluation at the Pi?

Solution. No, it is a not-so-easy theorem in number theory that π is NOT a zero of a polynomial with rational coefficients. Such a number is called a transcendental number. ■

Def. • $a \in \mathbb{C}$ is called algebraic if $\ker \phi_a \neq \{0\}$ where $\phi_a : \mathbb{Q}[x] \to \mathbb{C}$ is the evaluation at a.

- $a \in \mathbb{C}$, which is not algebraic, is called a transcendental number.

Ex. Find $\phi_2(x^{12}-x)$ where $\phi_2 : \mathbb{Z}_{11}[x] \to \mathbb{Z}_{11}$ is the evaluation at 2.

Solution. Since 11 is prime, $\forall\, a \in \mathbb{Z}_{11}$, $a^{11}=a$.
So $2^{12} = 2^{11} \times 2 = 2 \times 2$, which implies $\phi_2(x^{12}-x) = 4-2 = 2$. ■

The division algorithm

Friday, August 18, 2017 1:08 AM

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

Theorem. Suppose R is a unital commutative ring and $0 \neq 1$. 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 $b_m \in U(R)$. 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.

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

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

The division algorithm (existence)

Friday, August 18, 2017 11:14 AM

Case of $f=0$. Set $q=r=0$. Then

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

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

Case 1. $\deg g = m > 0$.

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

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

Case 2. $\deg g = m = 0$.

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

Set $q(x) = a_0 b_0^{-1}$ and $r(x) = 0$. Then

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

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.

The division algorithm (existence)

Friday, August 18, 2017 12:53 PM

<u>Case 2.</u> $\deg f = k \geq \deg g = m$.

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 $q_1(x), r_1(x) \in R[x]$ s.t. ① $\deg r_1 < \deg g$

② $f(x) - a_k b_m^{-1} x^{k-m} g(x) = q_1(x)\, g(x) + r_1(x)$.

② implies that $f(x) = (a_k b_m^{-1} x^{k-m} + q_1(x))\, g(x) + r_1(x)$. ⊛

Let $r(x) = r_1(x)$ and $q(x) = a_k b_m^{-1} x^{k-m} + q_1(x)$.

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

$f(x) = q(x)\, g(x) + r(x)$. ∎

The division algorithm (uniqueness)

Friday, August 18, 2017 1:54 PM

<u>Proof of uniqueness</u>. Suppose

① $\deg r_1, \deg r_2 < \deg g$

② $f(x) = q_1(x)\, g(x) + r_1(x) = q_2(x)\, g(x) + r_2(x)$.

We have to show $q_1 = q_2$ and $r_1 = r_2$.

② implies $(q_1(x) - q_2(x))\, g(x) = r_2(x) - r_1(x)$. ⊛

$\deg(r_2 - r_1) \le \max(\deg r_1, \deg r_2) < \deg g$.

Since the leading coeff. of g is a unit, we get

$$\deg((q_1 - q_2) g) = \deg(q_1 - q_2) + \deg g \quad \text{(why?)}$$

(In class we proved this in integral domains.)

Hence $\deg(q_1 - q_2) + \deg g = \deg(r_2 - r_1) < \deg g$.

And so $\deg(q_1 - q_2) < 0$, which implies $\deg(q_1 - q_2) = -\infty$

and $q_1 - q_2 = 0$. Using ⊛ we get that $r_2 - r_1 = 0$.

So $q_1 = q_2$ and $r_1 = r_2$. ∎

Next we use the division algorithm to study zeros of a polynomial.

The factor theorem

Friday, August 18, 2017 2:03 PM

<u>Theorem</u>. Let R be a unital commutative non-zero ring, and $f(x) \in R[x]$. Then $a \in R$ is a zero of f if and only if $f(x) = (x-a)\, q(x)$ for some $q(x) \in R[x]$.

<u>Pf.</u> ($\Rightarrow$) Since the leading coeff. of $x-a$ is 1 and $1 \in U(R)$, by the division algorithm $\exists\, q(x), r(x) \in R[x]$ s.t.

① $\deg r < \deg(x-a) = 1.$ $\rightsquigarrow$ r is constant.

② $f(x) = (x-a)q(x) + r(x)$

Since a is a zero of f, ② implies

$$0 = f(a) = (a-a)\, q(a) + r(a) \text{ ; and so } r(a) = 0.$$

Since r is constant, we get that $r(x) = r(a) = 0$.

So $f(x) = (x-a)\, q(x)$.

($\Leftarrow$) $f(x) = (x-a)\, q(x)$ implies $f(a) = (a-a)\, q(a) = 0$.

And so a is a zero of f. ■

In the previous lectures we have seen that some degree 2 polynomials have more than 2 zeros. But this is not the

Zeros of a polynomial over an integral domain

Friday, August 18, 2017 2:15 PM

the case over an integral domain.

<u>Theorem</u>. Let D be an integral domain, and $f(x) \in D[x]$. Suppose $a_1, \dots, a_k$ are distinct zeros of $f(x)$. Then $\exists q(x) \in D[x]$ s.t. $f(x) = (x-a_1)\cdots(x-a_k)\, q(x)$.

In particular, a polynomial f has at most $\deg(f)$ zeros.

<u>Pf.</u> We proceed by induction on k.

<u>Base of induction</u>. $k=1$.

a_1 is a zero of f. So by the factor theorem, $f(x) = (x-a_1)\, q(x)$ for some $q(x) \in D[x]$; this proves the base of induction.

<u>Induction step</u>. Suppose $a_1, \dots, a_{k+1}$ are distinct zeros of $f(x)$.

Since a_{k+1} is a zero of f, by the factor theorem $\exists\, h(x) \in D[x]$ s.t. $f(x) = (x-a_{k+1})\, h(x)$. So, for any $1 \le i \le k$, $0 = f(a_i) = (a_i - a_{k+1})\, h(a_i)$. Since

Zeros of a polynomial over an integral domain

Friday, August 18, 2017 2:24 PM

$$\left.\begin{array}{l} 0=(a_i-a_{k+1})\,h(a_i) \\ a_i \neq a_{k+1} \text{ for } 1\le i\le k \\ D \text{ has no zero-divisor} \end{array}\right\} \Rightarrow h(a_1)=h(a_2)=\dots=h(a_k)=0.$$

So $a_1,\dots,a_k$ are distinct zeros of h. Hence by the induction hypothesis we have that

$$h(x)=(x-a_1)\cdots(x-a_k)\,q(x)$$

for some $q(x)\in D[x]$. Therefore

$$f(x)=(x-a_{k+1})\,h(x)=(x-a_1)\dots(x-a_k)(x-a_{k+1})\,q(x).$$

This gives us the first part of theorem.

To get the second part of theorem, we have

$$\deg f=\deg\big((x-a_1)\cdots(x-a_k)\,q(x)\big)$$
$$=k+\deg q,$$

which implies $\deg f\ge k$. So f has at most $\deg(f)$ zeros. $\blacksquare$