Lecture 07: Division algorithm (uniqueness)

Thursday, February 21, 2019 2:03 AM

In the previous lecture we proved the existence part of division algorithm.

<u>Theorem</u> (Division algorithm) Suppose D is an integral domain, $f(x)=a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$, $g(x)=b_m x^m + \cdots + b_0 \in D[x]$, $b_m \in D^\times$. Then there is a unique pair $q(x)$ and $r(x) \in D[x]$ s.t.

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

<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.)

Lecture 07: The division algorithm (uniqueness)

Friday, August 18, 2017 1:54 PM

Hence $\deg(q_{r_1}-q_{r_2})+\deg g=\deg(r_2-r_1)<\deg g$.

And so $\deg(q_{r_1}-q_{r_2})<0$, which implies $\deg(q_{r_1}-q_{r_2})=-\infty$ and $q_{r_1}-q_{r_2}=0$. Using $\circledast$ we get that $r_2-r_1=0$.

So $q_{r_1}=q_{r_2}$ and $r_1=r_2$. $\blacksquare$

We have already pointed out that two polynomials can give us the same functions. Nevertheless thinking about polynomials as functions is extremely useful.

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

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

It is called the <u>evaluation at a</u>.

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:

The evaluation map

Friday, August 18, 2017 12:25 AM

<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> 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 $i^2 = -1$.

<u>Solution.</u> $f \in \ker(\phi_i) \iff f(i) = 0$.

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 $x^2+1 \in \ker \phi_i$. ∎

<u>Ex.</u> 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.

<u>Solution.</u> $x^2 - x - 12 \in \ker \phi_a \iff \phi_a(x^2 - x - 12) = 0$

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

The evaluation homomorphisms

Friday, August 18, 2017 12:44 AM

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

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