Multivariant polynomial Rings

i.e. $f = x^2 - 3xy + 2y^3$

- $R[x]$ is a commutative ring with 1 (since R is com. with $1 \in R$)

$(R[x])[y]$ — commutative ring with 1

$(R[y])[x]$ — commutative ring with 1

Show $(R[x])[y] \simeq (R[y])[x]$.

Cor $R[x_1, \ldots, x_n]$ is a commutitive ring with 1.

Evaluation Homomorphism

Thm Let R be a commutive with 1. Let $\alpha \in R$

The evaluation Homomorphism [Let $p(x) = a_n x^n + \cdots a_1 x + a_0$]

$$\phi_\alpha : R[x] \to R$$
$$: p(x) \to p(\alpha) = a_n \alpha^n + \cdots + a_1 \alpha + a_0$$

is in fact a ring hom.

Proof:

$p(x) = \sum a_i x^i \quad ; \quad q(x) = \sum b_i x^i$

$$\phi_\alpha(p(x) + q(x)) = (p+q)(\alpha) = \sum (a_i + b_i)\alpha^i$$
$$= \sum a_i \alpha^i + \sum b_i \alpha^i$$
$$= p(\alpha) + q(\alpha)$$

$$\phi_\alpha(p(x))\cdot\phi_\alpha(q(x)) = p(\alpha)\,q(\alpha)$$
$$= \left(\sum a_i\alpha^i\right)\left(\sum b_i\alpha^i\right)$$
$$= \sum_{i=0}^{m+n}\left(\sum_k a_k b_{i-k}\right)\alpha^i$$
$$= (p\cdot q)(\alpha) = \phi_\alpha(p(x)q(x))$$

■

Thm (Division Alg.) $\frac{f(x)}{g(x)}$

Let $f(x), g(x) \in F[x]$ where F is a field and $g \neq 0$

$\exists$ unique $q(x), r(x) \in F[x]$ s.t.

$$f(x) = g(x)q(x) + r(x)$$

where $\deg(r(x)) < \deg(g(x))$ (or $r(x)=0$).

Proof: will use induction

- If $f(x) = 0$ then $0 = 0\cdot g(x) + 0$

  $\therefore\ q = r = 0$] Base case

[note if $f(x) = c \in F$
- if $\deg(g(x)) \le \deg(f(x))$

then $\frac{f}{g} = q(x) \in F$]

Suppose $f(x) \neq 0$ say $\deg(f(x)) = n$

$\deg(g(x)) = m$

If $m > n$ then take $q(x) = 0$, $r(x) = f(x)$

Assume $m \le n$, do induction on n [starting from $n=0$ base case]

Say $f(x) = a_n x^n + \cdots + a_1 x + a_0$

$g(x) = b_m x^m + \cdots + b_1 x + b_0$

Let $\tilde{f}(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$

$\deg(\tilde{f}) < n$ or $\tilde{f} = 0$

$\therefore$ by induction $\exists\ \tilde{q}(x), r(x)$ s.t

$\tilde{f}(x) = \tilde{q}(x) g(x) + r(x)$ where either $r=0$ or $\deg(r) < \deg(g)$

Set $q(x) = \tilde{q}(x) + \frac{a_n}{b_m} x^{n-m}$

Then $f(x) = q(x) g(x) + r(x)$

Check $q(x) g(x) + r(x) = \overbrace{\tilde{q}(x) g(x) + r(x)}^{= \tilde{f}(x)} + g \frac{a_n}{b_m} x^{n-m}$

$= \tilde{f}(x) + g \frac{a_n}{b_m} x^{n-m}$

$= f(x)$.

and $r=0$ or $\deg(r) < \deg(g)$

Now show uniqness of q, r

Suppose $\exists\ q_1, r_1$ s.t. $f(x) = g(x) q_1(x) + r_1(x)$ with $\deg(r_1) < \deg(g)$

(or $r_1 = 0$)

So then

$$f(x) = g(x)\,q_1(x) + r_1(x) = g(x)\,q(x) + r(x)$$

$$g(x)\left[q(x) - q_1(x)\right] = r_1(x) - r(x)$$

$g(x) \neq 0$ Suppose $q \neq q_1$ $r \neq r_1$

$$\Rightarrow \quad \deg\left(g(x)\left[q(x) - q_1(x)\right]\right) \overset{\geq \deg(g(x))}{=} \deg(r_1(x) - r(x)) \geq \deg(g(x))$$

This is a contradiction

$$\therefore \quad q = q_1 \text{ and } r = r_1$$

Ex) Polynomial Long division $\Leftrightarrow$ division alg.

Suppose $f(x) = x^3 - x^2 + 2x - 3$, $g(x) = x - 2$

divide $\dfrac{f(x)}{g(x)}$ to find $q(x)$, $r(x)$.

$f(x) = a_n x^n + \dots + a_1$

$LC(f) = a_n x^n$

Compute

assume $\deg(f) > \deg(g)$

$$f - \frac{LT(f)}{LT(g)}\, g(x) = \underbrace{f - \frac{a_n}{b_m} x^{n-m} g(x)}_{\tilde{f}}$$

$$\begin{array}{r|l}
 & \quad x^2 + x + 4 \\ \hline
x - 2 & x^3 - x^2 + 2x - 3 \\
 & -(x^3 - 2x^2) \\ \hline
 & \qquad x^2 + 2x - 3 \quad \text{— first } \tilde{f} \text{ from proof.} \\
 & \qquad x^2 - 2x \\ \hline
 & \qquad\qquad 4x - 3 \quad \text{— second } \tilde{f} \\
 & \qquad\qquad 4x - 8 \\ \hline
 & \qquad\qquad\quad 5
\end{array}$$

$q(x) = x^2 + x + 4, \quad r(x) = 5.$

Let $p(x) \in F[x]$, $\alpha \in F$

α is a root of $p(x) \iff p(\alpha) = 0$

$\iff p(x) \in \ker(\phi_\alpha)$

evaluation hom. asr. to $\alpha \in F$.

<u>Coro</u> Let F be a field. $\alpha \in F$ is a root/zero of $p(x) \in F[x]$ iff $x-\alpha$ is a factor of $p(x)$ in $F[x]$.

<u>Proof:</u> First suppose $\alpha \in F$, $p(\alpha) = 0$

By the division algorithm $\exists\ q(x)\ r(x) \in F[x]$ s.t.

$p(x) = (x-\alpha)\,q(x) + r(x)$ and $\deg(r(x)) < \deg(x-\alpha) = 1$

$$\therefore \quad p(x) = (x-\alpha)\,q(x) + b$$

$$\therefore \quad 0 = p(\alpha) = \overset{\alpha-\alpha=0}{0}\,q(x) + b$$

$$\therefore \quad b = 0$$

and $p(x) = (x-\alpha)\,q(x)$.

Suppose $x-\alpha$ is a factor of $p(x)$

$$\therefore \quad p(x) = (x-\alpha)\,q(x) \Rightarrow p(\alpha) = (\alpha-\alpha)\,q(x) = 0 \cdot q(x) = 0. \ \blacksquare$$

Cor ol Let F be a field. A non-zero poly $p(x) \in F[x]$
$\deg(p(x)) = n$, can have at most n distinct roots in F.

Proof: Do induction on $\deg(p(x))$

If $\deg(p(x)) = 0 \Rightarrow p(x) = c \in F \therefore$ has no distinct roots

base case for induction

If $\deg(p(x)) = 1 \Rightarrow p(x) = ax + b$ for some $a, b \in F$

Since F is a field $0 = p(\alpha) = a\alpha + b \Rightarrow \alpha = (-b)a^{-1}$

Assume $\deg(p(x)) > 1$. If $p(x)$ has no roots in F we are done

Suppose $\alpha \in F$ is a root of p

$\Rightarrow p(x) = (x-\alpha)\, q(x)$ for some $q \in F[x]$
(by Cor. above)

Since F is a field

$$\deg(q(x)) = n-1$$

Let $\beta \neq \alpha$ be another (distinct) root of $p(x)$

$p(\beta) = (\beta - \alpha)\, q(\beta) = 0$, since $\beta \neq \alpha$
and since F is a field

$$\Rightarrow q(\beta) = 0$$

and By induction $q(x)$ has at most $n-1$ roots.

$\therefore$ $p(x)$ has at most n roots. ∎