Lec 10/7

Monday, October 7, 2019 11:35

Polynomial Rings ctd (everything is commutative)

$R[x_1, \dots, x_n]$ has the universal property: given $u_1, \dots, u_n \in S$,

$$\begin{tikzcd} R \arrow[r, "\eta"] \arrow[d, hook] & S \\ R[x_1, \dots, x_n] \arrow[ur, dashed, "\exists!\, \eta_{u_1, \dots, u_n}"'] & \end{tikzcd}$$

s.t. $\eta_{u_1, \dots, u_n}(x_i) = u_i$.

Def if $R \xhookrightarrow{id} S$ then $u_1, \dots, u_n \in S$ are algebraically independent over R if $\operatorname{Ker}(id_{u_1, \dots u_n}) = 0$.

i.e. $R[u_1, \dots, u_n] \cong R[x_1, \dots, x_n]$.

Polynomial Rings II

Thm if D is a domain, so is $D[x_1, \dots, x_n]$.

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

Thm if D is a domain, then the units of $D[x_1, \dots, x_n]$ are just the units of D.

Pf $fg = 1 \Rightarrow \deg(f) + \deg(g) = 0$. Induct.

<u>Thm (division alg)</u> Let R be a comm. ring, $f(x), g(x) \in R[x]$ with $g(x) \neq 0$. Let $b_m \neq 0$ be the leading coeff of $g(x)$. Then $\exists k \in \mathbb{Z}$ and $q(x), r(x) \in R[x]$ s.t.

$$b_m^k f(x) = q(x) g(x) + r(x), \qquad \deg(r(x)) < \deg(g(x)).$$

<u>Proof</u> induct on $\deg(f(x))$. If $\deg(f(x)) < \deg(g(x))$, then

$$f(x) = 0 \cdot g(x) + f(x).$$

Suppose $\deg(f(x)) \geq \deg(g(x))$. If $f(x) = a_0 + \cdots + \overset{\neq 0}{a_\ell} x^\ell$, $g(x) = b_0 + \cdots + \overset{\neq 0,}{b_m} x^m$

$$b_m f(x) - a_\ell x^{\ell - m} g(x) = f_1(x). \qquad (*)$$

then $\deg(f_1(x)) < \deg(f(x))$, so apply inductive hypothesis:

$\exists k \in \mathbb{Z}$, $q_1(x), r(x) \in R[x]$ s.t.

$$b_m^k f_1(x) = q_1(x) g(x) + r(x), \qquad \deg(r(x)) < \deg(g(x)).$$

Substituting back into $(*)$, we get

$$b_m^{k+1} f(x) - a_\ell b_m^k x^{\ell-m} g(x) = q_1(x) g(x) + r(x).$$

Let $q(x) = q_1(x) + a_\ell b_m^k x^{\ell - m}$. $\square$

<u>Remark:</u> an upper bound for # iterations this takes is

Remark: an upper bound for # iterations this takes is

$$\max\{0, \ell - m + 1\}.$$

Corollary if $R = F$ is a field, $0 \neq g(x)$, $f(x) \in F[x]$, there are unique $q(x), r(x)$ s.t.

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

Remark This is also true if the leading coeff of g is a unit.

Corollary if $f(x) \in R[x]$, $a \in R$, then $\exists$ unique $q(x) \in R[x]$ s.t.

$$f(x) = (x-a)q(x) + f(a).$$

Def $\overset{0}{\underset{\#}{}}g(x)$ divides $f(x)$ if $\exists q(x)$ w/ $f(x) = q(x)g(x)$.

Ex if $R = F$ is a field, $g(x) \mid f(x) \iff \underbrace{r(x)}_{\text{remainder of div. alg.}} = 0$

Corollary Let $a \in R$, $f(x) \in R[x]$. $(x-a) \mid f(x) \iff f(a) = 0$.

Def A domain D is called a principal ideal domain (PID) if every ideal in D is principal (generated by one element).

<u>Thm</u> F is a field $\Longrightarrow$ $F[x]$ is a PID.