

1/9/07

Polynomial Rings

p. 260 # 4)

p. 298 # 14, 12, 17

p. 306 # 3, 4

Let R be a comm ring w/ 1 .

Recall: R is an I.D. $\leftrightarrow R[X]$ is an I.D. If so the quotient field of $R[X]$ is the field of fractions, rational functions

In this case the deg poly: $\deg q(x) = \deg(pq)$, units of $R[X]$ are units of R .

Prop Let I be an ideal of R , so $(I) \cong I[x] \subseteq R[X]$. Then:

1. $R[X]/(I) \cong (R/I)[X]$

2. If I is prime in R then (I) is prime in $R[X]$.

Proof Reducing coeffs mod I gives a ring homomorphism
 $R[X] \rightarrow R/I[X]$ with kernel (I) .

$$I \text{ prime} \Rightarrow R/I \text{ I.D.} \Rightarrow R/I[X] \text{ I.D.}$$

Rmk All works for $R[X_1, \dots, X_n]$ or even countably many variables.

Recall $F[X]$ is a Euclidean Domain where norm is degree

Proof: Long Division of polynomials

$$\Rightarrow F[X] \text{ is a PID \& UFD}$$

Recall $R[X]$ a PID $\Rightarrow R$ a field

Problem FXJ is $ED \rightarrow PID \rightarrow UFD$
 $R[X] \quad PID \leftrightarrow R \text{ a field}$

Question: When is $R[X]$ a UFD?

Tool: When R is an integral domain then $R \hookrightarrow$ field of fractions F
 so $R[X] \hookrightarrow FXJ$.

Ex $\mathbb{Z}[X] \subseteq \mathbb{Q}[X]$.

Lemma $R[X]$ a UFD $\Rightarrow R$ a UFD.

Proof Constant polynomials factor uniquely.

Goal: Converse.

Gauss Lemma Let R be a UFD, $R \hookrightarrow F$ field of fractions,
 $p(x) \in R[X]$. If $p(x)$ is reducible in FXJ then it is reducible
 in $R[X]$. Specifically suppose

$$p(x) = A(x)B(x) \text{ in } FXJ$$

Then $\exists r, s \in F$ with $rA(x) = a(x) \in R[X]$ w/ $p(x) = a(x)b(x)$
 $sB(x) = b(x)$

Example $3x^2 + x - 10 = \left(\frac{2}{3}x + \frac{4}{3}\right)\left(\frac{9}{2}x - \frac{15}{2}\right) \in \mathbb{Q}[X]$
 $= (x+2)(3x-5)$

Proof $p(x) = A(x)B(x)$, multiply by \prod denoms to get

$$(A) d p(x) = a'(x)b'(x) \quad a', b' \in R[x].$$

If d is a unit then done, else factor $d = p_1 p_2 \dots p_n$ in $R[x]$.

p_i irred \Rightarrow (or) prime $\Rightarrow (R/p_i R)[x]$ is int domain. Reduce $\pmod{p_i}$

$$0 = \overline{a'(x)} \overline{b'(x)} \text{ in } R/p_i R[x] \text{ so } p_i | a'(x) \text{ or } p_i | b'(x).$$

Thus $\overline{a'(x)}$ has all coeffs div by p_i .
Cancel, $\frac{1}{p_i} a'(x) \in R[x]$ etc.

Example $(\frac{2}{3}x + \frac{4}{3})(\frac{9}{2}x - \frac{15}{2}) = 3x^2 + x - 10$
~~4x~~ $(2x+4)(9x-15) = 6 \cdot (3x^2 + x - 10)$
 $= 3 \cdot 2 \cdot (3x^2 + x - 10)$

Thus Reducible in $F[x] \Rightarrow$ Red. in $R[x]$.

Not conversely, $6x$ red in $Z[x]$, irred in $Q[x]$

COR Suppose $p(x) \in R[x]$ and $\text{gcd of coeffs is } 1$ (eg. monic)
Then $p(x)$ is irred in $R[x]$ iff irred in $F[x]$.

Proof Red in $F \Rightarrow$ Red in R by Gauss

Suppose $p(x) = a(x)b(x)$ in $R[x]$. But neither a nor b is constant
so $p(x)$ is red in $F[x]$.

Thm R is a UFD iff $R[X]$ is a UFD.

Proof \Leftarrow \checkmark so suppose R is a UFD, $f \neq 0$ in $R[X]$, $p(x) \neq 0$ in $R[X]$.

Let $d = \gcd$ of coeffs so $p(x) = d p'(x)$ where $p'(x)$ has rel prime coeffs.

This is unique up to unit in R . so ETS $p'(x)$ factors uniquely.

Thus WLOG $p(x)$ has rel prime coeffs, $\deg p > 0$.

1. Factor $p(x)$ in $F[X]$. Each term has \gcd of coeffs = 1 so is irreducible in $R[X]$. Thus $p(x)$ factors into irreducibles in $R[X]$.

Suppose $p(x) = a_1(x) \cdots a_r(x) = b_1(x) \cdots b_s(x)$ in $R[X]$.

Now \gcd coeffs $p = 1 \Rightarrow$ same a 's b 's \Rightarrow all $\deg > 1 \Rightarrow$ all ir in $F[X]$

By unique fact in $F[X]$, $r = s$ and $a_i = b_i \cdot u_i$

WLOG

Thus suppose $a_i(x) = \frac{m}{n} b_i(x)$

$$n a_i(x) = m b_i(x)$$

\uparrow
 \gcd coeffs = n

\leftarrow
 \gcd coeffs = m

Thus $n = m$ \checkmark

COR R a UFD \Rightarrow any poly ring over R w/ arbitrary # variables is a UFD

~~Ex 1. $\mathbb{Z}[X_1, \dots, X_n]$ is a UFD~~

IRREDUCIBILITY CRITERION

PROP $p(x) \in F[x]$ has a factor $x-a$ iff $p(a)=0$

Proof \Rightarrow clear
 \Leftarrow Write $p(x) = (x-a)q(x) + r$ r is constant so
 $p(a) = r$

COR degree ≥ 3 irr \Leftrightarrow no root

EX $p(x) = x^3 + x + 1$ irr in $\mathbb{Z}_2[x]$

so $\mathbb{Z}_2[x]/(x^3+x+1)$ field of 8 elts