Lecture 13 Wednesday Feb 17

Recall

LEM 5: Given a field F

Given $a, b \in F[x]$ with $b \neq 0$.

Then $\exists$ unique pair $q, r \in F[x]$ st

$$a = bq + r \qquad *$$

and

$$r = 0 \quad \text{or} \quad \deg(r) < \deg(b) \qquad **$$

pf Last time we saw q, r exist.

Show q, r are unique:

Suppose $\exists$ $q', r' \in F[x]$ st

$$a = bq' + r' \qquad ☆$$

and

$$r' = 0 \quad \text{or} \quad \deg(r') < \deg(b) \qquad ☆☆$$

Show $q = q'$ and $r = r'$. Assume $q \neq q'$, else $r = r'$ and we are done. Combine $*$, ☆ to get

$$b(q - q') = r' - r$$

So

$$\deg(b) + \deg(q-q') = \deg(r'-r)$$

We have

$$\underbrace{\deg(b) + \overset{\overset{0}{\wedge\!\!|}}{\deg(q-q')}}_{\overset{|\vee}{\deg(b)}} = \deg(r'-r) \underset{\text{by } **,\ \star\star}{<} \deg(b)$$

contradiction.

So $\quad q = q', \quad r = r'$ $\square$

Section 9.3

Recall our commutative ring R with $1 \neq 0$

LEMM (Gauss) Assume R is a UFD, with field of fractions F.

Given $f \in R[x]$ with degree ≥ 1

Assume f is reducible in $F[x]$.

Then f is reducible in $R[x]$

pf $\exists$ nonunits $a, b \in F[x]$ such that

$$f = ab$$

<u>obs</u> a, b not unique. For $0 \neq u \in F$,

au, bu^{-1} are nonunits in $F[x]$

and $f = (au)(bu^{-1})$

Put the coefs of a over some common denominator, and simplify:

$$a = \frac{a_0 + a_1 x + \cdots + a_r x^r}{A} \alpha \qquad r \geq 1$$

$a_0, a_1, \ldots, a_r, \alpha, A \in R$

a_r, α, A nonO

$\mathrm{GCD}(a_0, \ldots, a_r) = 1.$ $\qquad \mathrm{GCD}(\alpha, A) = 1$

Similarly for b,

$$b = \frac{b_0 + b_1 x + \cdots + b_s x^s}{B} \beta \qquad s \geq 1$$

$b_0, b_1, \ldots, b_s, \beta, B \in R$

b_s, β, B nmo

$GCD(b_0, \ldots, b_s) = 1, \qquad GCD(\beta, B) = 1$

Replacing

$$a \longrightarrow a \frac{A}{\alpha}, \qquad b \to b \frac{\alpha}{A}$$

if nec, WLOG

$\alpha = 1, \qquad A = 1$

In $F[x]$,

$$f = (a_0 + a_1 x + \cdots + a_r x^r)(b_0 + b_1 x + \cdots + b_s x^s) \, \beta / B$$

In $R[x]$,

$$Bf = (a_0 + a_1 x + \cdots + a_r x^r)(b_0 + b_1 x + \cdots + b_s x^s)\, \beta$$ $*$

Show B is a unit in R:

Suppose not.

$\exists$ prime $p \in R$ st $p \mid B$

Consider ring hom

$$R \longrightarrow R/Rp$$
$$r \longrightarrow \underbrace{r + Rp}_{= \bar{r}}$$

This hom induces ring hom

$$R[x] \longrightarrow R/Rp\,[x]$$ $\star$
$$\sum_i r_i x^i \longrightarrow \sum_i \bar{r}_i x^i$$

p prime in R $\Rightarrow$ R/Rp is int dom $\Rightarrow$ $R/Rp\,[x]$ is int dom

Apply ✡ to each side of $*$:

$$0 = \underbrace{(\bar{a}_0 + \bar{a}_1 x + \cdots + \bar{a}_r x^r)}_{\substack{\neq \\ 0 \\ \text{else } p \mid a_i \ \forall i}} \underbrace{(\bar{b}_0 + \bar{b}_1 x + \cdots + \bar{b}_s x^s)}_{\substack{\neq \\ 0 \\ \text{else } p \mid b_i \ \forall i}} \underbrace{\bar{\beta}}_{\substack{\neq \\ 0 \\ \text{since } p \nmid \beta}}$$

Cont.

So β is unit in R.

Now by $*$, in $R[x]$

$$f = \underbrace{(a_0 + a_1 x + \cdots + a_r x^r)}_{\text{nonunit}} \underbrace{(b_0 + b_1 x + \cdots + b_s x^s)}_{\text{nonunit}} \beta \beta^{-1}$$

So f is reducible in $R[x]$. $\square$

Assume R is a UFD.

Given $f \in R[x]$ with $\deg(f) \geq 1$

Write

$$f = a_0 + a_1 x + \cdots + \underset{\neq 0}{a_\ell} x^\ell \qquad \ell \geq 1 \qquad a_i \in R$$

Assume

$$GCD(a_0, a_1, \ldots, a_\ell) = 1$$

LEM 2 With the above notation and assumptions,

TFAE:

(i) f is reducible in $R[x]$

(ii) f is reducible in $F[x]$, where F = field of fractions of R.

pf (i) $\to$ (ii) $\exists$ nonunits $a, b \in R[x]$ st

$$f = ab$$

a or b is a unit in $F[x]$, else done.

WLOG a is unit in $F[x]$.

So

$$0 \neq a \in F$$

By constr $a \in R[x]$ so

$$0 \neq a \in R$$

Write

$$b = b_0 + b_1 x + \cdots + \underset{\neq 0}{b_\ell} x^\ell \qquad b_i \in R$$

Recall $f = ab$

So $a_i = a b_i \qquad 0 \le i \le \ell$

So $a \mid a_i \qquad 0 \le i \le \ell$

So a divides $GCD(a_0, a_1, \ldots, a_\ell) = 1$

So a is unit in R

So a is unit in $R[x]$

Cont

$(ii) \to (i)$ By Gauss Lemma. $\square$

Prop 3 Assume R is a UFD.

Then $R[x]$ is a UFD.

pf R is int domain so $R[x]$ is int domain.

The units in $R[x]$ are the units in R

Let F = field of fractions for R

Recall $F[x]$ is Eucl dom, PID, UFD

The units in $F[x]$ are the nonzero elements in F

Given $0 \neq f \in R[x]$, f not a unit

Show that f is a product of irred elements in $R[x]$:

Factor f in $R[x]$:

$$\begin{array}{ccc} & f & \\ / & & \backslash \\ f_1 & & f_2 \\ / \ \backslash & & / \ \backslash \\ \cdots & & \cdots \end{array}$$

$\deg(f) = \deg(f_1) + \deg(f_2)$

process terminates by considering the degree, and since R is UFD

Get $f = p_1 p_2 \cdots p_s f_1 f_2 \cdots f_t$ $\quad *$

$s, t \geq 0$

irred $p_i \in R$ $\quad 1 \leq i \leq s$

irred $f_i \in R[x]$ $\quad \deg(f_i) \geq 1$ $\quad 1 \leq i \leq t$

Consider uniqueness of factorization $*$:

Suppose

$$f = p_1' p_2' \cdots p_S' f_1' f_2' \cdots f_T' \qquad **$$

$S, T \geq 0$

irred $p_i' \in R$ $\qquad 1 \leq i \leq S$

irred $f_i' \in R[x]$ $\quad \deg(f_i') \geq 1$ $\qquad 1 \leq i \leq T$

Compare $*$, $**$ in $F[x]$:

$$\underbrace{p_1 \cdots p_s}_{\text{units}} \underbrace{f_1 \cdots f_t}_{\substack{\text{each irred} \\ \text{by Gauss L}}} = \underbrace{p_1' \cdots p_S'}_{\text{units}} \underbrace{f_1' \cdots f_T'}_{\substack{\text{each irred} \\ \text{by Gauss L}}} \qquad \star$$

Since $F[x]$ is a UFD,

up to assoc

$f_1, \ldots f_t$ is perm of $f_1', \ldots, f_T'$ $\qquad t = T$

WLOG $\quad f_i' = u_i f_i \qquad 0 \neq u_i \in F \qquad 1 \leq i \leq t$

For $1 \le i \le t$ write

$$u_i = \frac{u_i^+}{u_i^-} \qquad 0 \neq u_i^\pm \in R$$

WLOG $\quad GCD(u_i^+, u_i^-) = 1$

Show u_i^+, u_i^- are units in R.

Write

$$f_i = a_0 + a_1 x + \cdots + \underset{\neq 0}{a_\ell} x^\ell \qquad a_j \in R \qquad \ell \geq 1$$

$$GCD(a_0, a_1, \ldots, a_\ell) = 1 \qquad \text{since } f_i \text{ irred in } R[x]$$

Write $\quad f_i' = a_0' + a_1' x + \cdots + \underset{\neq 0}{a_\ell'} x^\ell \qquad a_j' \in R$

$$GCD(a_0', \ldots, a_\ell') = 1 \qquad \text{since } f_i' \text{ irred in } R[x]$$

In $R[x]$

$$u_i^- f_i' = u_i^+ f_i$$

So in R

$$u_i^- a_j' = u_i^+ a_j \qquad 0 \leq j \leq \ell.$$

Suppose u_i^- is not a unit in R

$\exists$ prime $p \in R$ st $p \mid u_i^-$

p divides each of

$u_i^+ a_0, u_i^+ a_1, \ldots, u_i^+ a_\ell$

$p \nmid u_i^+$ since $GCD(u_i^+, u_i^-) = 1$

So p divides each of

$a_0, a_1, \ldots, a_\ell$

Now
p divides $GCD(a_0, a_1, \ldots a_\ell) = 1$

So p is unit, contr.

So u_i^- is unit in R.

Similarly u_i^+ is unit in R

Now $u_i = \frac{u_i^+}{u_i^-}$ is unit in R

Now f_i, f_i' are assoc in $R[x]$

After cancellation ✯ becomes

$$p_1 p_2 \cdots p_a = p_1' p_2' \cdots p_s' \; u \qquad u = u_1 u_2 \cdots u_t$$

Obs u is unit in R

Since R is UFD,

up to assoc

$p_1, p_2, \ldots, p_a$ is perm of $p_1', p_2', \ldots, p_s'$ $\quad s = a$

We have shown that the factorization ✯ is unique up to assoc and perm. $\square$

So $R[x]$ is a UFD.