

## Lecture 13 Wednesday Feb 17

Recall

LEMMA: Given a field  $F$ Given  $a, b \in F[x]$  with  $b \neq 0$ .Then  $\exists$  unique pair  $q, r \in F[x]$  st

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

and

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

pf Last time we saw  $q, r$  exist.Show  $q, r$  are unique:Suppose  $\exists q', r' \in F[x]$  st

$$a = bq' + r' \quad \star$$

and

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

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

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

So

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

We have

$$\underbrace{\deg(b) + \deg(q - q')}_{\substack{IV \\ \deg(b)}} = \deg(r' - r) < \deg(b)$$

by \*\*,  
\* \*

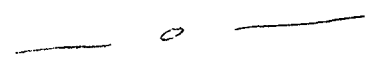
contradiction.

So

$$q = q'$$

$$r = r'$$

□



Section 9.3

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

LEMMA (Gauss) Assume  $R$  is a UFD,

with field of fractions  $F$ .

Given  $f \in R[x]$  with degree  $\geq 1$

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

then  $f$  is reducible in  $R[x]$

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

$$f = ab$$

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

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

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

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

$$a = \frac{a_0 + a_1x + \dots + a_r x^r}{A} \quad \alpha \quad r \geq 1$$

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

$$a_i, \alpha, A \text{ nonzero}$$

$$\text{GCD}(a_0, \dots, a_r) = 1,$$

$$\text{GCD}(\alpha, A) = 1$$

Similarly for  $b$ ,

$$b = \frac{b_0 + b_1 x + \dots + b_n x^n}{B} \quad \beta \quad d \geq 1$$

$$b_0, b_1, \dots, b_n, \beta, B \in \mathbb{R}$$

$$b_n, \beta, B \neq 0$$

$$\text{GCD}(b_0, \dots, b_n) = 1,$$

$$\text{GCD}(\beta, B) = 1$$

Replacing

$$a \rightarrow a \frac{A}{\alpha},$$

$$b \rightarrow b \frac{\alpha}{A}$$

if nec, WLOG

$$\alpha = 1,$$

$$A = 1$$

In  $F[x]$ ,

$$f = (a_0 + a_1 x + \dots + a_r x^r) (b_0 + b_1 x + \dots + b_n x^n) \beta / B$$

In  $R[x]$ ,

$$Bf = (a_0 + a_1x + \dots + a_r x^r) (b_0 + b_1x + \dots + b_s x^s) \neq 0$$

\*

Show  $B$  is a unit in  $R$ :

Suppose not.

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

Consider ring hom

$$\begin{array}{ccc} R & \longrightarrow & R/p \\ r & \longrightarrow & \underbrace{r + p}_{\bar{r}} \end{array}$$

This hom induces ring hom

$$\begin{array}{ccc} R[x] & \longrightarrow & (R/p)[x] \\ \sum_i r_i x^i & \longrightarrow & \sum_i \bar{r}_i x^i \end{array}$$

★

$$p \text{ prime in } R \Rightarrow R/p \text{ is int dom} \Rightarrow (R/p)[x] \text{ is int dom}$$

Apply  $*$  to each side of  $*$ :

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

cont.

So  $B$  is unit in  $R$ .

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

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

So  $f$  is reducible in  $R[x]$ . □

Assume  $R$  is a UFD.

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

Write

$$f = a_0 + a_1 x + \dots + \underbrace{a_l}_{\neq 0} x^l \quad l \geq 1 \quad a_i \in R$$

Assume

$$\text{GCD}(a_0, a_1, \dots, a_l) = 1$$

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)  $\rightarrow$  (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 const  $a \in R[x]$  so

$0 \neq a \in R$

Write

$$b = b_0 + b_1 x + \dots + \underbrace{b_l}_{\neq 0} x^l$$

$$b_i \in R$$

Recall

$$f = ab$$

So

$$a_i = ab_i$$

$$0 \leq i \leq l$$

So

$$a \mid a_i$$

$$0 \leq i \leq l$$

So

$$a \text{ divides } \text{GCD}(a_0, a_1, \dots, a_l) = 1$$

So

$$a \text{ is unit in } R$$

So

$$a \text{ is unit in } R[x]$$

Cmt

(ii)  $\rightarrow$  (i)

By Gauss Lemma.

□



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  $R$ .

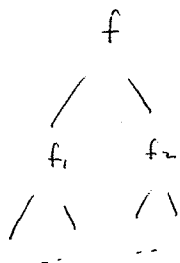
Recall  $F[x]$  is Eucl dom, PID, UFD

The units in  $F[x]$  are the non zero elements in  $F$

Given  $0 \neq f \in R[x]$ , find a unit

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

Factor  $f$  in  $R[x]$ :



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

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

Get  $f = p_1 p_2 \dots p_r f_1 f_2 \dots f_t$

$r, t \geq 0$   
 irred  $p_i \in R$   $1 \leq i \leq r$   
 irred  $f_i \in R[x]$   $\deg(f_i) \geq 1$   $1 \leq i \leq t$

\*

Consider uniqueness of factorization \* :

Suppose

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

$$S, T \geq 0$$

$$\text{irred } p_i' \in R \quad 1 \leq i \leq S$$

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

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

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

Since  $F[x]$  is a UFD,

up to assoc

$$f_1 \cdots f_t \text{ is perm of } f_1' \cdots f_t' \quad t = T$$

wlog

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

For  $1 \leq i \leq t$  write

$$u_i = \frac{u_i^+}{u_i^-} \quad \text{with } u_i^\pm \in R$$

wlog  $\text{GCD}(u_i^+, u_i^-) = 1$

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

Write

$$f_i = a_0 + a_1x + \dots + a_l x^l \quad a_j \in R \quad l \geq 1$$

$\text{GCD}(a_0, a_1, \dots, a_l) = 1$  since  $f_i$  irred in  $R[x]$

Write

$$f_i' = a_0' + a_1'x + \dots + a_l' x^l \quad a_j' \in R$$

$\text{GCD}(a_0', a_1', \dots, a_l') = 1$  since  $f_i'$  irred in  $R[x]$

In  $R[x]$

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

So in  $R$

$$u_i^- a_j' = u_i^+ a_j \quad 0 \leq j \leq l$$

Suppose  $u_i^-$  is not a unit in  $R$

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

$p$  divides each of

$$u_i^+ a_0, u_i^+ a_1, \dots, u_i^+ a_l$$

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

So  $p$  divides each of

$$a_0, a_1, \dots, a_l$$

Now

$p$  divides  $\text{GCD}(a_0, a_1, \dots, a_l) = 1$ .

So  $p$  is unit, contradiction

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  $\star$  becomes

$$p_1 p_2 \dots p_n = p'_1 p'_2 \dots p'_s u \quad u = u_1 u_2 \dots u_t$$

obs  $u$  is unit in  $R$

Since  $R$  is UFD,

up to assoc

$$p_1, p_2, \dots, p_n \text{ is perm of } p'_1, p'_2, \dots, p'_s \quad s = n$$

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

So  $R[x]$  is a UFD.

□