Lecture 14 Friday Feb 19

COR 4 Assume R is a UFD.

Given mutually commuting indeterminates $x_1, x_2, \ldots, x_n$

then the polynomial ring $R[x_1, x_2, \ldots, x_n]$ is a UFD.

pf R is UFD

$\Rightarrow$ $R[x_1]$ is UFD

$\Rightarrow$ $R[x_1, x_2] = R[x_1][x_2]$ is UFD

$\Rightarrow$ ...

$\Rightarrow$ $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$ is UFD

□

9.4 Irreducibility criteria

Until further notice R denotes an integral domain.

Consider the polynomial ring $R[x]$

Recall $R[x]$ is an integral domain

What are the invertible polynomials in $R[x]$?

The answer depends on the details of R.

We look at some special cases.

Let F = field

Consider polynomial ring $F[x]$

LEM 1 For $f \in F[x]$ and $a \in F$,

TFAE

(i) $f(a) = 0$ "a is a root of f"

(ii) the polynomial $x-a$ divides f

pf (i) $\rightarrow$ (ii) Divide f by $x-a$ and consider the remainder. $\exists$ unique $q, r \in F[x]$

s.t.

$$f = (x-a)q + r \quad *$$

and

$r=0$ or $\deg r < \deg(x-a)$

$\| 1$

So $r \in F$

In * set $x = a$:

$$f(a) = (a-a)\,g(a) + r$$

$$\| \qquad\qquad \| \qquad\qquad \|$$

$$0 \qquad\qquad 0 \qquad\qquad r$$

So $r = 0$

Now * becomes

$$f = (x-a)\,g$$

so $x-a$ divides f

(ii) $\rightarrow$ (i) $\exists\ g \in F[x]$ st

$$f = (x-a)\,g$$

So $f(a) = (a-a)\,g(a)$

$$\| \quad 0$$

$$= 0$$

□

COR 2 Given $f \in F[x]$ with degree 2 or 3

TFAE

(i) f has no root in F

(ii) f is irreducible in $F[x]$

pf (i) $\to$ (ii) Suppose

$f = AB$ nonunits $A, B \in F[x]$

So $\deg A \geq 1$, $\deg B \geq 1$

Show $\deg A \geq 2$, $\deg B \geq 2$.

Suppose $\deg A = 1$

Write $A = a_0 + a_1 x$ $a_0, a_1 \in F$

$a_1 \neq 0$

$A = a_1(x - \alpha)$, $\alpha = -a_0/a_1$

$A(\alpha) = 0$

$f(\alpha) = A(\alpha) B(\alpha)$

$= 0$

α is root of f cont.

So $\deg A \geq 2$

Sim $\deg B \geq 2$

Now

$$\deg f = \deg AB = \deg A + \deg B \geq 2+2 = 4$$

$\|$

2 or 3

cont.

□

(ii) → (i) By LEM 1

Consider ring of integers $\mathbb{Z}$
and field of fractions $\mathbb{Q}$.

LEM 3 Given $f \in \mathbb{Z}[x]$ with $\deg n \geq 1$:

$$f = a_0 + a_1 x + \cdots + a_n x^n \qquad a_i \in \mathbb{Z}$$
$$\neq 0$$

Then each integer root of f divides a_0

pf Let r = integer root of f

$r \in \mathbb{Z}$, $f(r) = 0$

Obs
$$0 = f(r)$$
$$= a_0 + a_1 r + \cdots + a_n r^n$$
$$= a_0 + r\underbrace{(a_1 + a_2 r + \cdots + a_n r^{n-1})}_{b}$$

So
$$a_0 = r(-b)$$

So $r \mid a_0$ in $\mathbb{Z}$

□

Given $f \in \mathbb{Z}[x]$ with $\deg n \geq 1$:

$$f = a_0 + a_1 x + \cdots + a_n x^n \qquad a_i \in \mathbb{Z}$$
$$\neq 0$$

Assume f has a root $r \in \mathbb{Q}$

Write $r = \frac{\alpha}{\beta}$ $\qquad \alpha, \beta \in \mathbb{Z}$ $\qquad \beta \neq 0$

$$GCD(\alpha, \beta) = 1.$$

LEM 4 With above notation,

$$\alpha \mid a_0 \quad \text{and} \quad \beta \mid a_n$$

pf Observe

$$0 = \beta^n f\left(\frac{\alpha}{\beta}\right)$$

$$= \beta^n \left(a_0 + a_1 \frac{\alpha}{\beta} + \cdots a_{n-1} \frac{\alpha^{n-1}}{\beta^{n-1}} + a_n \frac{\alpha^n}{\beta^n} \right)$$

$$= \overbrace{a_0 \beta^n + a_1 \alpha \beta^{n-1} + \cdots + a_{n-1} \alpha^{n-1} \beta}^{\beta \text{ divides}} + \underbrace{a_n \alpha^n}_{\alpha \text{ divides}}$$

So

$$\alpha \mid a_0 \beta^n$$

and

$$\beta \mid a_n \alpha^n$$

Now since $GCD(\alpha, \beta) = 1$,

$$\alpha \mid a_0 \quad \text{and} \quad \beta \mid a_n$$

□

Assume R is integral domain.

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

$$f = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} + x^n \qquad c_i \in R$$

Assume f is reducible in $R[x]$

So $\exists$ non units $a, b \in R[x]$ st

$$f = ab$$

Write

$$a = a_0 + a_1 x + \cdots + a_r x^r \qquad a_i \in R$$

$$b = b_0 + b_1 x + \cdots + b_s x^s \qquad b_j \in R$$

$$r + s = n$$

$$a_r b_s = 1$$

a_r, b_s units in R

Note $r \geq 1$, else $a = a_0$ is unit in R and hence $R[x]$

Similarly $s \geq 1$

Given an ideal $I \subsetneq R$

Consider the ring hom

$$\begin{aligned} R &\longrightarrow R/I \\ r &\longrightarrow \underbrace{r+I}_{=\bar{r}} \end{aligned}$$

This induces ring hom

$$\begin{aligned} R[x] &\longrightarrow R/I[x] \\ \sum_i r_i x^i &\longrightarrow \sum_i \bar{r}_i x^i \end{aligned} \qquad \text{☆}$$

Apply ☆ to $f = ab$

In $R/I[x]$,

$$\bar{c}_0 + \bar{c}_1 x + \cdots + \bar{c}_{n-1} x^{n-1} + x^n = \underbrace{(\bar{a}_0 + \bar{a}_1 x + \cdots + \bar{a}_r x^r)}_{\neq 0}\underbrace{(\bar{b}_0 + \bar{b}_1 x + \cdots + \bar{b}_s x^s)}_{\neq 0}$$

So in $R/I[x]$, the image of f is a product of two polynomials each with degree ≥ 1.

This is useful since $R/I[x]$ might be easier to work with than $R[x]$.