Polynomial rings over UFDs

<u>Gauss lemma</u>: R a UFD, F - its field of fractions

$$p(X) \in R[X]$$

If $p(X)$ is reducible in $F[X]$

then $p(X)$ is reducible in $R[X]$

Explicitly, if $p(X) = A(X) \cdot B(X)$, $\quad A, B \in F[X]$

then $\exists\, r, s \in F$ s.t. $\quad r \cdot A(X) = a(X) \in R[X]$

$\quad s \cdot B(X) = b(X)$

and $p(X) = a(X) \cdot b(X)$

<u>Obs</u>: $F[X]^\times = \underbrace{F}_{\text{constant polynomials}}$

$A(X), B(X) \notin F[X]^\times \implies \deg A, \deg B \geq 1$

<u>Example</u>: $15X^2 + 13X + 2 = \underset{A(X)}{\underset{\parallel}{\left(\frac{5}{2}X + \frac{5}{3}\right)}} \cdot \underset{B(X)}{\underset{\parallel}{\left(6X + \frac{6}{5}\right)}}$

$$2 \cdot 3 \cdot 5\,(15X^2 + 13X + 2) = \left[2 \cdot 3 \cdot \left(\frac{5}{2}X + \frac{5}{3}\right)\right] \cdot \left[5 \cdot \left(6X + \frac{6}{5}\right)\right]$$

$$= [15X + 10] \cdot [30X + 6]$$

$$15X^2 + 13X + 2 = \left[\overset{r}{\overset{\parallel}{\frac{2 \cdot 3}{5}}}\left(\frac{5}{2}X + \frac{5}{3}\right)\right] \cdot \left[\overset{s}{\overset{\parallel}{\frac{5}{2 \cdot 3}}}\left(6X + \frac{6}{5}\right)\right]$$

$$= \underset{a(X)}{\underset{\parallel}{(3X + 2)}}\underset{b(X)}{\underset{\parallel}{(5X + 1)}}$$

Pf: write $A(X) = \frac{a_0}{\alpha_0} + \frac{a_1}{\alpha_1}X + \dots + \frac{a_n}{\alpha_n}X^n$

$B(X) = \frac{b_0}{\beta_0} + \frac{b_1}{\beta_1}X + \dots + \frac{b_m}{\beta_m}X^m$

Let $\alpha = \alpha_0 \alpha_1 \cdots \alpha_n$, $d = \alpha \cdot \beta$

$\beta = \beta_0 \cdot \beta_1 \cdots \beta_m$

① R int. dom. $\Longrightarrow$ $\alpha, \beta, d \neq 0$

② $\alpha \cdot A(X) = a'(X) \in R[X]$

$\beta \cdot B(X) = b'(X)$

e.g. $\frac{5}{2}X + \frac{5}{3}$, $6X + \frac{6}{5}$

$$(2 \cdot 3) \cdot \left(\frac{5}{2}X + \frac{5}{3}\right), \quad 5 \cdot \left(6X + \frac{6}{5}\right)$$

$a'(X) = 15X + 10$ $\qquad$ $b'(X) = 30X + 6$

So $d \cdot p(X) = a'(X) \cdot b'(X)$.

write $d = q_1 \cdot q_2 \cdots q_k$, q_i is irreducible $\forall i \in \{1, \dots, k\}$.

$$\Longrightarrow \quad (q_i) \subset R \quad \text{is prime.}$$

$$\Longrightarrow \quad R[X] / q_i R[X] \cong \left(R/(q_i) \right)[X] \quad \text{an int. dom.}$$

$$q_i \mid d \quad \Longrightarrow \quad \overline{d\,p(X)} = \bar{0} \in \left(R/(q_i) \right)[X]$$

$$\overline{d\,p(X)} = \overline{a'(X)} \cdot \overline{b'(X)}$$

$$\Longrightarrow \quad a'(X) \text{ or } b'(X) \in q_i R[X]$$

$$\Longrightarrow \quad \frac{1}{q_i} \cdot a'(X) \quad \text{or} \quad \frac{1}{q_i} b'(X) \in R[X]$$

$$\Longrightarrow \quad \frac{d}{q_i} \cdot p(X) = \underbrace{\left[\frac{1}{q_i} a'(X) \right]}_{\in R[X]} \cdot \underbrace{\left[b'(X) \right]}_{\in R[X]}.$$

Do this with all q_i's, we get

$$p(X) = \underbrace{a(X)}_{\in R[X]} \cdot \underbrace{b(X)}_{\in R[X]}$$

e.g.

$$30 \cdot p(X) = (15X + 10) \cdot (30X + 6)$$

$$15\, p(X) = (15X + 10) \cdot (15X + 3)$$

$$p(X) = (3X + 2) \cdot (5X + 1) \qquad \square$$

Rephrase Gauss Lemma:

If $p(x)$ is irreducible in $R[x]$

it is <u>still</u> irreducible in $F[x]$

<u>Q</u>: Are there any irreducibles in $F[x]$

that <u>aren't</u> irreducible in $R[x]$?

Recall: If F, K are fields, $F \subset K$

$p(X)$ irred. in $F[x]$ iff $p(X)$ irred. in $K[x]$

<u>Example</u>: $7X$ is reducible in $\mathbb{Z}[x]$

$7, X$ are non-units!

BUT $7 \in \mathbb{Q}^{\times}$, so $7, X$ do not

constitute a reduction of $7X$ in $\mathbb{Q}[x]$.

Moreover, $7X$ is associate to X

and $\mathbb{Q}[x]/(x) \cong \mathbb{Q}$ a field

$\Longrightarrow (X)$ is maximal $\Longrightarrow (X)$ is prime

$\Longrightarrow X$ is irreducible $\Longrightarrow 7X$ irreducible.

Cor: Let R be a UFD, F its field of fractions.

$$p(X) = a_0 + a_1 X + \_\_ + a_n X^n \in R[X]$$

and $\gcd(a_0, a_1, \_\_, a_n) = 1$

Then $p(x)$ is irred. in $R[x]$ iff $p(x)$ is irred. in $F[x]$

Note: $\gcd(a_0, a_1 \_\_, a_n) = 1$ means we cannot write

$$p(x) = d \cdot p'(x), \quad d \in R \setminus R^\times, \quad \deg p = \deg p'$$

Pf: Suppose $p(x) \in R[x]$ is reducible in $R[x]$ and $\gcd(a_0, \_\_, a_n) = 1$

Suppose $p(x) = a(x) \cdot b(x)$, $a(x), b(x) \notin R[x]^\times$

$\gcd(a_0, \_\_, a_n) = 1 \implies a(x), b(x)$ are not constant polynomials

$\implies \deg a, \deg b \geq 1$

But, $F[x]^\times$ is exactly $F^\times = \{\text{nonzero, constant polynomials}\}$

$\implies a, b \in F[x]$ are not units in $F[x]$

$\implies p(x)$ is reducible in $F[x]$

The other direction is Gauss' Lemma $\square$

<u>Thm</u>: R is a UFD iff $R[x]$ is a UFD.

<u>Pf</u>: If $R[x]$ is a UFD, then $R \subset R[x]$

$\implies R$ is a UFD

Suppose, conversely, that R is a UFD.

F is its field of fractions

$$p(X) = a_0 + a_1 X + \text{———} + a_n X^n \in R[x]$$

Goal: uniquely factor $p(x)$ in $R[x]$.

Let $d = \gcd(a_0, a_1, \text{——}, a_n) \in R$

If $d \notin R^\times$, then it has a unique factorization into irred. in R

and $p(x) = d \cdot \underbrace{p'(x)}_{\gcd(\text{coeffs}) = 1}$

we now assume $\gcd(a_0, a_1, \text{—}, a_n) = 1$.

In particular, if $p(x) \notin R[x]^\times$

Then $\deg p \geq 1$

Consider $p(x) \in F[x]$ — UFD (actually a Euclidean Domain)

$\Longrightarrow$ $p(x) = A_1(x) \cdot A_2(x) \cdot \dots \cdot A_k(x)$

where $A_i(x) \in F[x]$ is irreducible

$\underset{\text{Gauss' Lemma}}{\Longrightarrow}$ $p(x) = a_1(x) \cdot a_2(x) \cdots a_k(x)$

$a_i(x) \in R[x]$

$\gcd(a_0, \ldots, a_n) = 1 \Longrightarrow \gcd(\text{coeffs of } a_i(x)) = 1 \quad \forall i$

$\underset{\text{Cor.}}{\Longrightarrow}$ $a_i(x) \in R[x]$ is associate to $A_i(x)$

in $F[x]$

hence $a_i(x)$ is irreducible in $R[x]$

uniqueness follows from uniqueness in $F[x]$

$\square$