

# L13: Polynomial Rings over UFDs

## Lemma 13.1: Gauss' Lemma

Let  $R$  be a UFD and  $F$  its field of fractions. Let  $p(X) \in R[X]$ , then if  $p(X)$  is reducible in  $F[X]$  then  $p(X)$  is reducible in  $R[X]$ .

Explicitly, if  $p(X) = A(X) \cdot B(X)$  and  $A \cdot B \in F[X]$ , then there exist  $r, s \in F$  such that

$$r \cdot A(X) = a(X) \in R[X], \quad s \cdot B(X) = b(X) \in R[X]$$

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

Observe that  $F[X]^\times = F$ , i.e the constant polynomials.

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

**Example 13.1.** Consider the polynomial

$$15X^2 + 13X + 2 = \underbrace{\left(\frac{5}{2}X + \frac{5}{3}\right)}_{=A(X)} \cdot \underbrace{\left(6X + \frac{6}{5}\right)}_{=B(X)}$$

The see that

$$\begin{aligned} 2 \cdot 3 \cdot 5(15X^2 + 13X + 2) &= \left[2 \cdot 3 \cdot \left(\frac{5}{2}X + \frac{5}{3}\right)\right] \cdot \left[5 \cdot \left(6X + \frac{6}{5}\right)\right] \\ &= [15X + 10] \cdot [30X + 6] \\ 15X^2 + 13X + 2 &= \left[\frac{2 \cdot 3}{5} \left(\frac{5}{2}X + \frac{5}{3}\right)\right] \cdot \left[\frac{5}{2 \cdot 3} \left(6X + \frac{6}{5}\right)\right] \\ &= \underbrace{[3X + 2]}_{a(X)} \cdot \underbrace{[5X + 1]}_{b(X)} \end{aligned}$$

**Proof.** Write

$$\begin{aligned} A(X) &= \frac{a_0}{\alpha_0} + \frac{a_1}{\alpha_1}X_1 + \cdots + \frac{a_n}{\alpha_n}X^n \\ B(X) &= \frac{b_0}{\beta_0} + \frac{b_1}{\beta_1}X_1 + \cdots + \frac{b_n}{\beta_n}X^n \end{aligned}$$

Let

$$\left. \begin{aligned} \alpha &= \alpha_0 \alpha_1 \cdots \alpha_n \\ \beta &= \beta_0 \beta_1 \cdots \beta_n \end{aligned} \right\} d = \alpha \cdot \beta$$

(1)  $R$  is an integral domain, so  $\alpha, \beta, d \neq 0$

(2)

$$\begin{aligned} \alpha \cdot A(X) &= a'(X) \\ \beta \cdot B(X) &= b'(X) \end{aligned} \in R[X]$$

For example

$$\underbrace{(2 \cdot 3)}_{\alpha} \cdot \underbrace{\left(\frac{5}{2}X + \frac{5}{3}\right)}_{A(X)} = \underbrace{15X + 10}_{a'(X)}$$

$$\underbrace{5}_{\beta} \cdot \underbrace{\left(6X + \frac{6}{5}\right)}_{B(X)} = \underbrace{30X + 6}_{b'(X)}$$

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

Write

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

Then  $(q_i) \subset R$  is prime, hence

$$R[X]/q_i R[X] \cong (R/(q_i))[X] \text{ is an integral domain}$$

Furthermore,

$$q_i | d \implies \overline{dp(X)} = \bar{0} \in (R/(q_i))[X] \implies \overline{a'(X)} \cdot \overline{b'(X)} = \bar{0}$$

Since  $a'(X)$  and  $b'(X)$  are equal to the 0 coset, we say  $a'(X)$  or  $b'(X)$  are in  $q_i R[X]$  (the ideal being modded out). Therefore

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

Doing this process for all  $q_i$ 's, we get

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

For example

$$\begin{aligned} 30 \cdot p(X) &= (15X + 10) \cdot (30X + 6) \\ 15 \cdot p(X) &= (15X + 10) \cdot (15X + 3) \\ p(X) &= (3X + 2) \cdot (5X + 1) \end{aligned}$$

■

To rephrase Gauss' Lemma:

If  $p(X)$  is irreducible in  $R[X]$ , then it is **still** irreducible in  $F[X]$

**Q:** Are there any irreducibles in  $F[X]$  that **are not** irreducible in  $R[X]$ ?

Recall that if  $F, K$  are fields with  $F \subset K$  then

$$p(X) \text{ irreducible in } F[X] \iff p(X) \text{ irreducible in } K[X]$$

**Example 13.2.**  $7X$  is reducible in  $\mathbb{Z}[X]$  as they are non-units. But  $7 \in \mathbb{Q}^\times$ , so  $7, X$  do constitute a reduction of  $7X$  in  $\mathbb{Q}[X]$ .

Moreover,  $7X$  is associate to  $X$  and notably  $\mathbb{Q}[X]/(X) \cong \mathbb{Q}$  and since  $\mathbb{Q}$  is a field, then

$$(X) \text{ is maximal} \implies (X) \text{ is prime} \implies X \text{ is irreducible} \implies 7X \text{ is irreducible}$$

### Corollary 13.2

Let  $R$  be a UFD and  $F$  its field of fractions. Let

$$p(X) = a_0 + a_1X + \cdots + a_nX^n \in R[X]$$

and  $\gcd(a_0, a_1, \dots, a_n) = 1$ . Then

$$p(X) \text{ irreducible in } R[X] \iff p(X) \text{ irreducible in } F[X]$$

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

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

**Proof.** Suppose  $p(X) \in R[X]$  is reducible in  $R[X]$  and  $\gcd(a_0, a_1, \dots, a_n) = 1$ . Further suppose

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

Then

$$\gcd(a_0, a_1, \dots, a_n) = 1 \implies a(X), b(X) \text{ non-constant polynomials} \implies \deg a, \deg b \geq 1$$

However, we know  $F[X]^\times$  is exactly  $F^\times$ , the non-zero constant polynomials. Hence  $a, b \in F[X]$  are not units in  $F[X]$  and so  $p(X)$  is reducible in  $F[X]$ . The other direction is Gauss' Lemma. ■

### Theorem 13.3: $R$ UFD $\iff R[X]$ UFD

$R$  is a UFD if and only if  $R[X]$  is a UFD.

**Proof.**

$\Leftarrow$

If  $R[X]$  is a UFD, then  $R \subset R[X]$  implying that  $R$  is also a UFD.

$\Rightarrow$

Suppose, conversely, that  $R$  is a UFD and  $F$  is its field of fractions. We can write

$$p(X) = a_0 + a_1X + \cdots + a_nX^n \in R[X]$$

The goal is to uniquely factor  $p(X)$  in  $R[X]$ . Let

$$d = \gcd(a_0, a_1, \dots, a_n) \in R$$

If  $d \notin R^\times$ , then it has unique factorization into irreducibles in  $R$  and necessarily  $p(X) = d \cdot p'(X)$  where the gcd of the coefficients in  $p'(X)$  is 1.

Now assume  $\gcd(a_0, a_1, \dots, a_n) = 1$ ; in particular, if  $p(X) \notin R[X]^\times$  then  $\deg p \geq 1$ .

Consider  $p(X) \in F[X]$  and note the  $F[X]$  is a UFD (actually a Euclidean domain). This implies

$$p(X) = A_1(X) \cdot A_2(X) \cdot \dots \cdot A_k(X)$$

where  $A_i(X) \in F[X]$  are irreducible. By Gauss' Lemma we then know

$$p(X) = a_1(X) \cdot a_2(X) \cdot \dots \cdot a_k(X)$$

where  $a_i(X) \in R[X]$ . Then

$$\gcd(a_0, \dots, a_n) = 1 \implies \gcd(\text{coeffs of } a_i(X)) = 1 \quad \forall i$$

By Corollary 13.2,  $a_i(X) \in R[X]$  is associate to  $A_i(X)$  in  $F[X]$ , hence  $a_i(X)$  is irreducible in  $R[X]$ .

The uniqueness follows directly from uniqueness in  $F[X]$ . ■