L13: Polynomial Rings over UFDs

Lemma 13.1: Gauss's 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. Then since $p(X)$ is reducible, $A(X)$ and $B(X)$ are non-units, and hence

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

Example 13.1. Consider the polynomial

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

Then see that by looking to clear the denominators of $A(X)$ and $B(X)$ we get,

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

Now we have factored the a multiple of our polynomial, so we get back to the original polynomial by dividing $2 \cdot 3 \cdot 5$ in such a way that we redistribute where they end up

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

Proof.
Write out the polynomials $A(X), B(X)$ where $\deg A(X) = n$ is not necessarily equal to $\deg B(X) = m$,

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

We want to clear out the denominators, so let

$$\left.\begin{aligned}\alpha &= \alpha_0\alpha_1\dots\alpha_n\\ \beta &= \beta_0\beta_1\dots\beta_m\end{aligned}\right\} d = \alpha\bullet\beta$$

(1) Since R is an integral domain and none of the α_i's and β_i's can be 0 (as they are in denominators of fractions), so $\alpha, \beta, d \neq 0$
(2) Now after clearing out the denominators, denote the new polynomials

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

For example

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

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

Therefore $d\bullet p(X) = a'(X)\bullet b'(X)$.
Write $d = q_1\bullet q_2\bullet\dots\bullet q_k$, where q_i is irreducible $\forall i\in\{1,\dots,k\}$. Then $(q_i)\subset R$ is prime, hence

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

Furthermore,

$$q_i \mid d \implies \overline{d\bullet p(X)} = \bar{0} \in (R/(q_i))[X] \implies \overline{a'(X)}\bullet\overline{b'(X)} = \bar{0}$$

Since $a'(X)$ or $b'(X)$ are equal to the 0 coset, then it is equivalent to say $a'(X)$ or $b'(X)$ are in $q_iR[X]$ (the ideal being modded out). In other words, whichever of the two is equal to $\bar{0}$ will have q_i as a factor of the numerators of their coefficients. Therefore

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

Now assuming w.l.o.g. it is $a'(X)$ which has q_i then

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

If we continue doing this process for all the irreducibles that appear in the factorization of d, then eventually we will clear all of d on the left, and at each stage we are ending up with polynomials in $R[X]$. So, in the end we get

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

Going back to the previous example, what we were doing is

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

To rephrase Gauss's Lemma in the form of its contrapositive:
If $p(X)$ is irreducible in $R[X]$, then it is **still** irreducible in $F[X]$. The point being that if R is a UFD and F is its field of fractions, knowing that $p(X)$ is irreducible in $R[X]$ and adding structure to reach $F[X]$ isn't enough structure to make $p(X)$ reducible.

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

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

So in a more general setting with fields, it is not the case. So let us to continue consider our case where R is a UFD, to which the answer is yes.

Example 13.2. $7X$ is reducible in $\mathbb{Z}[X]$ as 7 and X are non-units. But $7 \in \mathbb{Q}^{\times}$, so $7, X$ do not constitute a reduction of $7X$ in $\mathbb{Q}[X]$. Now it could be the case that $7X$ is reducible in another way not involving 7 and X, but we can prove in fact that there **isn't** a way of writing $7X$ as the product of two irreducibles in $\mathbb{Q}[X]$.

Proof.
$7X$ is associate to X (only differ by a unit) and notably $\mathbb{Q}[X]/(X) \cong \mathbb{Q}$ and since $\mathbb{Q}$ is a field, then

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

where the last implication is since 7 is associate to X then since 7 is a unit and X is irreducible (hence not a unit), $7X$ is irreducible. ■

In fact, we see that by shifting to the field of fractions, one of the elements in $7X$ became a unit, namely 7. As a corollary to Gauss's Lemma, we will see how situations like this are the only things that turn from irreducibles to units as one goes to the field of fractions.

Corollary 13.2

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

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

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

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

Note: $\gcd(a_0, a_1, \ldots, a_n) = 1$ means we cannot factor out a non-unit from the coefficients, i.e. we cannot write

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

Proof.
This will be proved by contrapositive. In the first direction, it is to show that if $p(X)$ is reducible in $F[X]$ then it is reducible in $R[X]$ Suppose $p(X) \in R[X]$ is reducible in $R[X]$ and $\gcd(a_0, a_1, \ldots, a_n) = 1$. That is, suppose

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

Then since $\gcd(a_0, a_1, \ldots, a_n) = 1$ the note in the statement of the corollary essentially says $a(X), b(X)$ are non-constant polynomials because you can not factor out of $p(X)$ a constant non-unit. So in fact that means $\deg a, \deg b \geq 1$.
However, we know $F[X]^\times$ is exactly $F^\times$, the non-zero constant polynomials. Hence $a(X), b(X) \in F[X]$ are not units in $F[X]$ and so $p(X)$ is reducible in $F[X]$.
The other direction is Gauss's 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 since $R \subset R[X]$ is a subring then R is also a UFD.
$\Rightarrow$
Suppose 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

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

If $d \notin R^\times$, then it has unique factorization into irreducibles in R (since R is a UFD) and necessarily $p(X) = d \bullet p'(X)$ where the gcd of the coefficients in $p'(X)$ is 1.
Now assume $\gcd(a_0, a_1, \ldots, a_n) = 1$; 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 we can write

$$p(X) = A_1(X) \bullet A_2(X) \bullet \ldots \bullet A_k(X)$$

where $A_i(X) \in F[X]$ are irreducible. By Gauss's Lemma we can clear out the denominators and write

$$p(X) = a_1(X) \bullet a_2(X) \bullet \ldots \bullet a_k(X)$$

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

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

By Corollary 13.2, since $a_i(X) \in R[X]$ is associate to $A_i(X)$ in $F[X]$, hence $a_i(X)$ is irreducible in $R[X]$. So we've shown there exists a factorization of $p(X)$ as a product of irreducibles in $R[X]$.
The uniqueness follows directly from uniqueness in $F[X]$. ■