Lecture LIV: R UFD $\Rightarrow R[x]$ UFD

TODAY'S GOAL: Show R UFD $\Rightarrow R[x]$ UFD.

§54.1 Gauss's Irreducibility Criterion:

We will need the following notations and results from Lecture 53.

Fix R a UFD & let $F = F(R)$ be its field of fractions.

Recall: $F(R) = S^{-1}R$ when $S = R \setminus \{0\}$ is the multiplicatively closed set of all non-zero elements of R.

We are going to view $R \subseteq F$ and $R[x] \subseteq F[x]$ (as subrings)

Definition: A polynomial $p \in R[x] \setminus \{0\}$ is said to be *primitive* if

$$\gcd(\text{coefficients of } p(x)) = 1 \quad \text{in } R.$$

That is, if $p = \sum_{j=0}^{n} c_j x^j \in R[x]$ with $c_n \neq 0$ Then, $d \mid c_j \ \forall j = 0, \ldots, n \Rightarrow d \in R^\times$

Lemma (Gauss): If R is a UFD and $p(x) \in R[x]$ is a primitive polynomial, then: $p(x)$ is irreducible in $R[x]$ if, and only if, $p(x)$ is irreducible in $F[x]$.

Proof. ($\Leftarrow$) Lecture 53

($\Rightarrow$) Assume $p(x)$ is irreducible over $R[x]$.

Claim 1: $\deg(p(x)) = n \geq 1$ (Lecture 53)

- We argue by contradiction and assume $p(x) = A(x)B(x)$ for some $A(x), B(x) \in F[x]$ that are not units, ie $\deg(A(x)) = k \geq 1$ & $\deg(B(x)) = n-k \geq 1$.

Clearing denominators, we can find some $d \in R \setminus \{0\}$ such that:

$$(*) \qquad \boxed{d \cdot p(x) = a(x)\, b(x) \quad \text{with } a(x), b(x) \in R}$$

Here, $a(x) = r A(x)$, $b(x) = s B(x)$ with $r, s \in R$, so $d = r \cdot s$.

Claim 2: $\exists\, \alpha, \beta \in R$ s.t. $d = \alpha\beta$ & $\frac{a(x)}{\alpha} \in R[x]$, $\frac{b(x)}{\beta} \in R[x]$

Pf/ If d is a unit, there is nothing to prove. Otherwise, we can write $d = p_1 \cdots p_\ell$ where $p_1, \ldots, p_\ell \in R$ are irreducible/prime elements.

We will find $c \in \{1,\dots,\ell\}$ and $i_1 < i_2 < \dots < i_c$ with $\{1,\dots,\ell\} \setminus \{i_1,\dots,i_c\} = \{i_{c+1},\dots,i_\ell\}$ such that $\alpha = p_{i_1}\cdots p_{i_c}$ & $\beta = p_{i_{c+1}}\cdots p_{i_\ell}$ satisfy $\frac{a(x)}{\alpha}, \frac{b(x)}{\beta} \in R[x]$.

We proceed as follows. Take $P_1 = (p_1) \subseteq R$.

Since p_1 is irreducible & R is a UFD, then p_1 is prime & $p_1 \neq 0$.

Then: $P_1 = (p_1) \subsetneq R$ is a non-zero prime ideal.

Consider (*) modulo $P_1 R[x]$:

$$0 = \Big(\sum_{i=0}^{k} (a_i \bmod P_1) x^i\Big) \Big(\sum_{j=0}^{n-k} (b_j \bmod P_1) x^j\Big)$$

Since R/P_1 is a domain, we know $(R/P_1)[x]$ is also a domain. Thus, one of the two factors above is 0. Thus, either:

(1) $a_0,\dots,a_k \in P_1 \Rightarrow \frac{a(x)}{p_1} \in R[x]$

or

(2) $b_0,\dots,b_{n-k} \in P_1 \Rightarrow \frac{b(x)}{p_1} \in R[x]$

By induction on $\ell \geq 1$, we can continue to find α & β as above, ie

$$p(x) = \left(\frac{a(x)}{p_{i_1}\cdots p_{i_c}}\right)\left(\frac{b(x)}{p_{i_{c+1}}\cdots p_{i_\ell}}\right) \quad \text{in } R[x].$$

$\square$

As a consequence $p(x) = \left(\frac{a(x)}{\alpha}\right)\left(\frac{b(x)}{\beta}\right)$ in $R[x]$ combined with the irreducibility over $R[x]$ says $\frac{a(x)}{\alpha} \in R[x]^\times = R^\times$ or $\frac{b(x)}{\beta} \in R[x] = R^\times$.

Thus, $k = \deg(a(x)) = 0$ or $n-k = \deg(b(x)) = 0$ which contradicts our assumption on k.

We conclude, $p(x)$ is irreducible over $F[x]$, as we wanted. $\square$

Corollary: Given $p(x) \in R[x]$ and $p(x) = A_1(x)\cdots A_r(x)$ with $A_1,\dots,A_r \in F[x]$, we can find $\lambda_1,\dots,\lambda_r \in F^\times$ st $a_i = \lambda_i A_i(x) \in R[x]$ $\forall i$ and

$$p(x) = a_1(x)\cdots a_r(x) \quad \text{in } R[x].$$

Proof: By induction on $r \geq 1$. The case $r=2$ is discussed in the proof of Gauss's Lemma and it is the key to certify the inductive step. $\square$

§4.2 Main Results:

Theorem 1: If R is a UFD, then so is $R[x]$.

Before we prove the theorem we need two technical results

Lemma 1: If $r \in R$ is irreducible, then r is irreducible in $R[x]$ as well.

Proof: By viewing $r \in R[x]$ in $F[x]$, and applying $\deg(\ )$, we see that any expression $r = f(x)\,g(x)$ with $f(x), g(x) \in R[x]$ has $f(x), g(x) \in R$.

Since $R^{\times} = (R[x])^{\times}$, the result follows.

Lemma 2: Let R be a UFD and fix $p(x), a(x), b(x) \in R[x]$ with $p(x) = a(x)\,b(x)$. Then: $p(x)$ is primitive $\iff$ both $a(x)$ and $b(x)$ are.

Proof: $(\Rightarrow)$ If $d \mid$ all coefficients of $a(x)$, then $d \mid$ all coefficients of $p(x)$ by construction. Thus, $d \in R^{\times}$ because $p(x)$ is primitive. This shows $a(x)$ is primitive.

By symmetry, the same is true for $b(x)$

$(\Leftarrow)$ If $d = \gcd(\text{coeff of } p(x))$, then $p(x) = d\,\bar{p}(x)$ with $\bar{p}(x)$ primitive.

Then, $d\,\bar{p}(x) = a(x)\,b(x)$ in $R[x]$. We want to show $d \in R^{\times}$.

The claim in the proof of Gauss's Lemma ensures $\exists\, \alpha, \beta \in R$ with $\alpha\beta = d$ s.t.

$$\frac{a(x)}{\alpha} \in R[x] \quad \& \quad \frac{b(x)}{\beta} \in R[x].$$

Since both $a(x)$ & $b(x)$ are primitive we conclude $\alpha \in R^{\times}$ & $\beta \in R^{\times}$, hence $d = \alpha\beta \in R^{\times}$. Thus, $p(x)$ is primitive.

Corollary 1: Let R be a UFD and fix $p(x), a_1(x), \dots, a_r(x) \in R[x]$ with $p(x) = a_1(x) \cdots a_r(x)$. Then: $p(x)$ is primitive $\iff$ $a_1(x), \dots, a_r(x)$ are.

Proof: $(\Rightarrow)$ is clear. Take $a = a_i(x)$ & $b = a_1 \cdots \hat{a}_i \cdots a_r$ & use Lemma 2.

$(\Leftarrow)$ We proceed by induction on r

Base case $r = 1$ is clear.

Inductive Step: Take $a_1(a_2 \cdots a_r)$ & set $b(x) = a_2 \cdots a_r$

By (IH) $a_2, \dots, a_r$ prim $\Rightarrow$ $b(x)$ is primitive.

Then, the Lemma applied to $a = a_1(x)$ & b implies $p(x) = a(x)\,b(x)$ is primitive.

$\square$

Proof of Theorem 1: We need to show both existence and uniqueness of factorizations into irreducibles

(1) Existence: Pick $p(x) \in R[x]$, $p(x) \neq 0$ & $p(x) \notin R[x]^{\times}$. We want to write $p(x)$ as a product of irreducible factors. To begin, we write

$$\alpha = \text{gcd of the coefficients of } p(x)$$

Then, $\alpha \in R$ and $p(x) = \alpha\, \overline{p}(x)$ where $\overline{p}(x) \in R[x]$ is primitive

Since $\alpha \in R \setminus \{0\}$ it is either in $R(x)^{\times}$ or it can be written (uniquely) as a product of irreducible elements of R. By Lemma 1, these elements remain irreducible in $R[x]$. Thus, it is enough to prove the factorization exists for the primitive polynomial $\overline{p}(x)$.

Assuming $\overline{p}(x)$ is not a unit, we know $\deg(\overline{p}(x)) \geq 1$.
Since $F[x]$ is a UFD (Corollary 2 §50.3) we can write

$$\overline{p}(x) = A_1(x) \cdots A_r(x) \qquad (**)$$

uniquely as a product of irreducible polynomials in $F[x]$.
By Corollary §54.1, we can rewrite $(**)$ as

$$\overline{p}(x) = a_1(x) \cdots a_r(x)$$

where $a_1(x), \dots, a_r(x) \in R[x]$ and $\forall i: a_i = \lambda_i A_i$ for some $\lambda_i \in F^{\times}$

Since $\overline{p}(x)$ is primitive, it follows that all $a_{1(x)}, \dots, a_{r(x)}$ are primitive as well. by Corollary 1.

Now, Gauss's Lemma implies that each $a_j(x)$ is irreducible in $R[x]$. This proves the existence of the factorization of $p(x)$.

(2) Uniqueness: To prove uniqueness assume $p_{(x)} \in R[x]$, $p_{(x)} \notin R[x]^{\times}$, $p_{(x)} \neq 0$ has 2 factorizations $p(x) = a_1 \cdots a_r = b_1 \cdots b_s$ with $a_1, \dots, a_r, b_1, \dots, b_s \in R[x]$ all irreducible.

We assume $\exists k, l$ s.t. $a_1, \dots, a_k \in R$, $a_{k+1}, \dots, a_r \in R[x] \setminus R$
$b_1, \dots, b_l \in R$, $b_{l+1}, \dots, b_s \in R[x] \setminus R$

Then $a_{k+1}, \dots, a_r, b_{l+1}, \dots, b_s$ must be primitive.

We have $p(x) = \underbrace{(a_1 \cdots a_k)}_{\in R} \underbrace{a_{k+1} \cdots a_r}_{\overset{\shortparallel}{A(x)}} = \underbrace{(b_1 \cdots b_\ell)}_{\in R} \underbrace{(b_{\ell+1} \cdots b_s)}_{\overset{\shortparallel}{B(x)}}$

with $A(x), B(x) \in R[x]$ primitive by Corollary 1 §53.2.

Thus $\gcd(\text{coefficients of } p(x)) = a_1 \cdots a_k$ (from the LHS), so
$b_1 \cdots b_\ell$ (from the RHS)

$\exists\, u \in R^\times$ st $a_1 \cdots a_k = u\, b_1 \cdots b_\ell \in R$.

Since R is a UFD: $k = \ell$ and $\exists\, \sigma \in S_\ell$ st $\forall i: a_i$ is associated to $b_{\sigma(i)}$

Thus, we have $u\, A(x) = B(x)$ with $u \in R^\times$ & both $A(x)$ & $B(x)$ are primitive. Absorbing u into a_{k+1} we can assume $u = 1$.

- Since $a_{k+1}, \ldots, a_r, b_{\ell+1}, \ldots, b_s \in R[x]$ are primitive and irreducible in $R[x]$, Gauss' Lemma implies they are irreducible over $F[x]$.

As $F[x]$ is a UFD we get $r - k = s - \ell$ (so $r = s$ since $k = \ell$) and after relabelling, for each $j = \ell+1, \ldots, s$ we have

$$b_j(x) = \lambda_j\, a_j(x) \quad \text{for some } \lambda_j \in F^\times$$

As both $a_j, b_j \in R[x]$ are primitive, we conclude $\lambda_j \in R^\times = R[x]^\times$.

(Indeed, write $\lambda_j = \frac{\alpha_j}{\beta_j}$ with $\alpha_j, \beta_j \in R$ to get $\beta_j b_j = \alpha_j a_j$. As both a_j, b_j are primitive, we get $\alpha_j \mid \beta_j$ in R & $\beta_j \mid \alpha_j$ in R, so $\frac{\alpha_j}{\beta_j} \in R^\times$)

Conclusion: $r = s$ and, up to relabelling, each $a_i(x)$ is associate to $b_i(x)$ ie
$\forall i = 1, \ldots, r$: $\exists\, u_i \in R[x]^\times = R^\times$ with $a_i = u_i b_i$. $\square$