CA LECTURE 2

SCRIBE: PETER LUMSDAINE

We continue and conclude the proof that if R is a UFD then $R[x]$ is also one. Throughout this lecture R is a UFD.

Lemma 1. *(Gauss' lemma) If f and g are primitive then fg is primitive.*

Proof. Otherwise there is $p \in R$ irreducible such that p divides all the coefficients of fg. Since R is a UFD, p is prime. So $P = (p)$ is a prime ideal and R/P is an ID.

The quotient map $R \to R/P$ induces a HM $R[x] \to R/P[x]$, We write $f \mapsto \bar{f}$ for this HM of polynomials. Clearly $\overline{fg} = \bar{f}\bar{g} = 0$. $R/P[x]$ is an ID because R/P is an ID, so without loss of generality $\bar{f} = 0$. But if $\bar{f} = 0$ then p divides all coefficients of f, a contradiction as f is primitive. □

Returning to the proof that $R[x]$ is a UFD, we note that if $f \in R[x]$ is irreducible then f is primitive if and only if $\deg(f) > 0$.

Lemma 2. *Let f and g be primitive in $R[x]$. Then f and g are associates in $F[x]$ iff they are associates in $R[x]$.*

Proof. Let $g = Af/B$ where $A, B \in R$ and $B \neq 0$. Then $Af = Bg$ so $A \neq 0$. A and B are both gcd's for the coefficients of $Af = Bg$, so A and B are associates in R and A/B is a unit of R. □

Lemma 3. *If $f \in F[x]$ is nonzero then it has an $F[x]$-associate g which is in $R[x]$ and primitive. What is more g is unique up to associates in $R[x]$.*

Proof. First find $C \in R$ nonzero such that $Cf \in R[x]$, then let D be a gcd for the coefficients of Cf and let $g = Cf/D$. The uniqueness follows from the previous lemma. □

Lemma 4. *Let $f \in R[x]$ be primitive and let $f = g_1 \dots g_n$ with $g_i \in F[x]$. Then $f = h_1 \dots h_n$ where $h_i \in R[x]$ is a primitive $F[x]$-associate of g_i.*

Proof. Let $a_i \in F$ be such that $a_i g_i \in R[x]$ is primitive. Then by Gauss $f \prod_i a_i$ is primitive, so by a previous lemma $a = \prod a_i$ is a unit of R. Now let $h_1 = a^{-1} a_1 g_1$ and $h_i = a_i g_i$ for $i > 1$. □

Remark: the hypothesis of primitivity in the next Lemma is needed for both directions. For example 2 is irreducible in $\mathbb{Z}[x]$ and a unit in $\mathbb{Q}[X]$ while $2x$ is composite in $\mathbb{Z}[x]$ but irreducible in $\mathbb{Q}[x]$.

Lemma 5. *Let $f \in R[x]$ be primitive. Then f is irreducible in $R[x]$ if and only if f is irreducible in $F[x]$.*

Proof. Let the primitive polynomial f be irreducible in $R[x]$ and $f = gh$ in $F[x]$. Then using the previous lemma, replacing g and h by suitable $F[x]$-associates we may assume $g, h \in R[x]$. Without loss of generality g is a unit in $R[x]$ and hence in $F[x]$.

Conversely let the primitive polynomial f be irreducible in $F[x]$ and $f = gh$ in $R[x]$. Withut loss of generaility g is a unit in $F[x]$, so g is a nonzero element of R. Now g divides all the coefficients of the primitive f so g is a unit in R. $\square$

Finally we can prove that $R[x]$ is a UFD. As usual there are two main claims, Existence and Uniqueness. Recall that both R and $F[x]$ are UFDs.

Existence of factorisations: let $f \in R[x]$ be a nonzero nonunit. Write $f = Cg$ where $C \in R$ is nonzero and $g \in R[x]$ is primitive. Either C is a unit in R, or C factors as $C_1 \dots C_m$ where the C_i are irreducible in R. The C_i are irreducibles of $R[x]$.

Either g is a unit in $F[x]$ (in which case g is a unit in R) or $g = g_1 \dots g_n$ where the g_i are irreducible in $F[x]$. Replacing by appropriate associates we may assume that the g_i are primitive elements of $R[x]$ and hence are irreducible in $R[x]$.

This gives us a factorisation.

Uniqueness of factorisation: let $f = C_1 \dots C_m g_1 \dots g_n = D_1 \dots D_k h_1 \dots h_l$ where the C's and D's are irreduciibles of R and the g's and h's are primitive irreducibles of $R[x]$.

By Gauss $\prod_i g_i$ and $\prod_i h_i$ are primitive, so as usual $\prod_i C_i$ and $\prod_i D_i$ are associates in R. Since R is a UFD the C's and D's coincide up to permutation and R-associates.

Similarly $\prod_i g_i$ and $\prod_i h_i$ are associates in $F[x]$, so since $F[x]$ is a UFD the g's and h's coincide up to permutation and $F[x]$-associates. If g_i and h_j are associates in $F[x]$ they are associates in $R[x]$, so the g's and h's coincide up to permutation and $R[x]$-associates.