Factorization of polynomials over UFD

Lecture 33

Defn Let R be an UFD. Then content of $f(x) \in R[x]$ denoted by $c(f)$ is the greatest common divisors of coefficients of $f(x)$. If $c(f)=1$ we say $f(x)$ is primitive.

Eg. Let $f(x) = 2x^2+4x+6$.

$$c(f) = \gcd(2,4,6) = 2.$$

Q If $f(x), g(x) \in R[x]$ are primitive polys then is $f(x)g(x)$ a primitive poly?

Thm. Let R be an UFD. If $f(x), g(x) \in R[x]$ are primitive then so is $f(x)g(x)$.

Pf: Suppose $\mathfrak{p}$ is a prime in R dividing the coefficients of $f(x)g(x)$. Consider the map

$$\pi : R[x] \longrightarrow R/\mathfrak{p}[x].$$

$$\pi\left(\sum a_n x^n\right) = \sum \bar{a}_n x^n$$

Thus $\overline{f(x)g(x)} = \bar{f}(x)\,\bar{g}(x) = 0$ in $R/\mathfrak{p}[x]$

Since $R/\mathfrak{p}[x]$ is an int domain either $\bar{f}(x) = 0$ or $\bar{g}(x) = 0$,

Hence either $\mathfrak{p} \mid c(f)$ or $\mathfrak{p} \mid c(g)$.

which is a contradiction.

Cor. For $f, g \in R[x]$ we have

$$c(fg) = c(f)\, c(g).$$

Pf: Let $c(f) = a$ and $c(g) = b$.

Then $f(x) = a f_1(x)$ where $f_1(x) \in R[x]$ is primitive

$g(x) = b g_1(x)$ where $g_1(x) \in R[x]$ is primitive.

Here by previous prop^n $f_1(x) \cdot g_1(x)$ is also primitive.

Since $f(x) g(x) = a f_1(x)\, b g_1(x)$

$= ab\, f_1(x) g_1(x)$.

$\therefore c(fg) = ab = c(f)\, c(g)$.

Prop 1. Let R be an UFD with quotient field K. If $f(x), g(x) \in R[x]$ are primitive and associates in $K[x]$ then they are associates in $R[x]$

Pf: Since $f(x)$ & $g(x)$ are associates in $K[x]$, so $f(x) = \frac{a}{b} g(x)$ where $a, b \in R$, $b \neq 0$.

Then $b f(x) = a g(x)$

Since $f(x)$ & $g(x)$ are primitive $c(bf) = b$ and $c(ag) = a$.

Since in a UFD the gcd of the coeff of a nonzero poly is unique upto multiplication by units hence $a = ub$ for

for some unit $u \in R$.
Therefore $f(x) = u g(x)$ and hence they are associates in $R[x]$.

Propn [Gauss' Lemma] Let R be a UFD with quotient field K and let $p(x) \in R[x]$. If $p(x)$ is reducible in $K[x]$ then $p(x)$ is reducible in $R[x]$. More precisely if $p(x) = A(x) B(x)$ for some non-constant polys $A(x), B(x) \in K[x]$, then there are non-zero elts $r, s \in K$ s.t $rA(x) = a(x)$ & $sB(x) = b(x)$ and $p(x) = a(x) b(x)$ where $a(x), b(x) \in R[x]$ is a factorization in $R[x]$.

Pf: Let $p(x) = A(x)\,B(x)$ where $A(x), B(x) \in K[x]$. Now multiplying

$$\left[A(x) = \frac{a_n}{b_n}x^n + \frac{a_{n-1}}{b_{n-1}}x^{n-1} + \cdots + \frac{a_0}{b_0}.\right]$$

by a common denominator for all these coefficients we obtain

(*) — $d\,p(x) = a'(x)\,b'(x)$ where $a'(x), b'(x) \in R[x]$ and d is a non-zero elt of R.

If d is a unit in R then the propn is true with $a(x) = d^{-1}a'(x)$.

Assume that d is not a unit in R. write $d = p_1 \cdots p_n$ where p_i's are irreducible elts of R. $\Rightarrow (p_1)$ is

a prime ideal and hence $R/p[x]$ is an int domain. Now reducing the eqn. mod p_1 we have

$\bar{a}'(x)\,\bar{b}'(x) = 0$ where bar denote the image in the quotient ring. which implies one of the factors say $\bar{a}'(x) = 0$ in $R/p[x]$. which means all the coeff of $a'(x)$ is divisible by p_1, so $\frac{1}{p_1} a'(x) \in R[x]$.

Therefore by cancelling the factor p_1 from both sides of the eq (*) we get an eqn in $R[x]$.

Proceeding in this way by cancelling

all the factors of d from both sides we can have an eqn. of the form $p(x) = a(x)\,b(x)$ with $a(x), b(x) \in R[x]$ and the relation between $A(x)$ & $a(x)$ is $d\,A(x) = a'(x)$ and $\frac{1}{p_i} a'(x) = a(x)$

$\therefore \left(\frac{d}{p_i}\right) A(x) = a(x)$ i.e $\nabla A(x) = a(x)$ for some $x \in K$.

Obs: The elts of the ring R become units in $K[x]$

eg $7x$ factors into irreducibles $7 \& x$ in $\mathbb{Z}[x]$ but $7x$ is irreducible in $\mathbb{Q}[x]$ as 7 is a unit in $\mathbb{Q}[x]$.

Cor. Let R be an UFD and K be its quotient field and let $p(x) \in R[x]$. Let $c(f(x)) = 1$ then $p(x)$ is irreducible in $R[x]$ iff it is irreducible in $K[x]$.

Pf: By Gauss' lemma if $p(x)$ is reducible in $K[x]$ then it is reducible in $R[x]$. Conversely with $c(p(x)) = 1$ if $p(x)$ is reducible in $R[x]$ i.e $p(x) = a(x)\, b(x)$ then neither $a(x)$ or $b(x)$ is a constant poly in $R[x]$. This same factorization shows that $p(x)$ is reducible in $K[x]$.

Thm. R is an UFD iff $R[x]$ is an UFD.