Irreducibility Criterion

Lecture 26

Q1 If R is an UFD then is $R[x]$ an UFD?

Q2 Can we relate the factorization of a poly in $K[x]$ with factorization of a poly in $R[x]$?

$R \rightsquigarrow K$ – quotient field of R

$R \subseteq R[x] \subseteq K[x]$ ⇝ is an UFD

$f(x)$

Let $f(x) \in R[x]$ then $f(x) \in K[x]$

Let $f(x) = p_1(x)\, p_2(x) \cdots p_r(x)$

where $p_i(x) \in K[x]$.

Throughout R is an UFD

Defn Let R be an UFD. The content of $f(x) \in R[x]$ denoted by $c(f)$ is the gcd of coeffs of $f(x)$. If $c(f) = 1$ we say that $f(x)$ is primitive.

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 p is a prime in R dividing the coeffs of $f(x)g(x)$.

Consider the map

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

given by $\pi\left(\sum a_n x^n\right) = \sum \bar{a}_n x^n$ where $\bar{a}_n$ denotes the image of a_n in R/p.

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

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

$\Rightarrow$ either $p \mid c(f)$ or $p \mid c(g)$.

which is a contradiction.

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

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

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

Then $f(x) = a f_1(x)$ and $g(x) = b g_1(x)$

where $f_1(x), g_1(x) \in R[x]$ are primitive. Hence $f_1(x) g_1(x)$ is also primitive.

Since $f(x) g(x) = ab f_1(x) g_1(x)$

$c(fg) = ab = c(f) c(g)$.

Propn: 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: Let $f(x) = \frac{a}{b} g(x)$ where $a, b \in R$ and $b \neq 0$.

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 of the coeffs of a non-zero poly is unique upto units hence $a = ub$ for some unit $u \in R$.

Therefore $f(x) = u g(x)$ where u is a unit in R and hence they are associates in $R[x]$.

Propn [Gauss' lemma]:

Let R be an UFD with quotient field F and let $p(x) \in R[x]$. If $p(x)$ is reducible in $F[x]$ then $p(x)$ is reducible in $R[x]$. More precisely, if $p(x) = A(x)B(x)$ for some non-constant polys $A(x), B(x) \in F[x]$, then there are non-zero elts $r, s \in F$ 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 $A(x), B(x) \in F[x]$.

Now multiplying by common denominators for all these coeffs we obtain $d\,p(x) = a'(x)b'(x)$ where $a'(x), b'(x) \in R[x]$ ↓ (1).

and d is a non-zero elt of R.

If d is an unit in R then the propn is proved as we can take $d^{-1}a'(x) = a(x)$, $b'(x) = b(x)$.

Assume d is not an unit

$d = p_1 \cdots p_n$ where p_i's are irreducibles in R.

$\Rightarrow (p_1)$ is a prime ideal and hence $R/p[x]$ is an int domain.

Now reducing the eq (1) mod p_1 we have $0 = \overline{a'(x)}\ \overline{b'(x)}$

where bar denotes the image in $R/p[x]$. which implies one of the two factors say $\overline{a'(x)} = 0$ in $R/p[x]$.

which means all the coeffs of $a'(x)$ is divisible by p_1

$\frac{1}{p_1} a'(x) \in R[x]$.

Therefore by cancelling the factor p_1 from both the sides of the eq (1) we get an eqn in $R[x]$. Proceeding in this way by cancelling all the factors of d from both the sides we can have an eqn of the form

$p(x) = a(x)\, b(x)$ where $a(x), b(x) \in R[x]$ and have the following relation:

$\cdot\, d\, A(x) = a'(x)$ and $\frac{1}{p_i}\, a'(x) = a(x)$

$\therefore \frac{d}{p_i} A(x) = a(x)$ i.e. $p\, A(x) = a(x)$.

Q If $f(x) \in R[x]$ is reducible in $F[x]$ then we have seen that $f(x)$ is reducible in $R[x]$.

If $f(x) \in R[x]$ is reducible over $R[x]$ is it reducible over $F[x]$? where F is the quotient field.

$\exists x \in \mathbb{Z}[x]$. $\ni$ $f(x)$ is primitive poly.

$f(x) = p_1(x)\, p_2(x)$

$\exists x$ $\qquad$ x.

$\exists x \in \mathbb{Q}[x]$.

But $\exists x$ is irreducible in $\mathbb{Q}[x]$.

Remark. The elts of the ring R become units in $F[x]$.

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

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

Pf: By Gauss's lemma if $p(x)$ is reducible in $F[x]$ 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 $a(x)$ nor $b(x)$ is constant poly in $R[x]$. This same factorization shows that $p(x)$ is reducible in $F[x]$.

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

Pf: Let R be an UFD

WTS $R[x]$ is an UFD.

Let F be the quotient field of R and $p(x) \in R[x]$ be a non-zero elt. WLOG we may assume $p(x)$ is primitive (if $p(x)$ is not primitive then $p(x) = d\,p'(x)$ where $d \in R$, so d has unique factorization & $p'(x)$ is primitive) and $p(x)$ is non unit in $R[x]$ i.e $\deg p(x) > 0$,

Since $F[x]$ is an UFD $p(x)$ can be factored uniquely into irreducibles in $F[x]$. By Gauss's lemma such a factorization implies there is a factorization of $p(x)$ in $R[x]$. Since $p(x)$ is primitive each factor of $p(x)$ is also primitive. Then by previous corollary each factor is irreducible in $R[x]$. This shows that $p(x)$ can be written as a finite product of irreducible in $R[x]$. The uniqueness of the

factorization of $p(x)$ in $R[x]$ follows from the uniqueness of $F[x]$.

Let $p(x) = q_1(x) \cdots q_r(x) = q_1'(x) \cdots q_s'(x)$ are two factorization in $R[x]$.

Now viewing it as a factorization in $F[x]$ we have $q_i(x)$ & $q_i'(x)$ are associates in $F[x]$ hence by previous propn they are associates in $R[x]$.

Prop 17. Let $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$. If $r/s \in \mathbb{Q}$ with $\gcd(r, s) = 1$ is a root of $p(x)$ then $r \mid a_0$ and $s \mid a_n$.

In particular, if $p(x)$ is monic (i.e the leading coeff of the poly is one) and $p(d) \neq 0$ for all integers dividing a_0, then $p(x)$ has no root in $\mathbb{Q}$.

Pf: Let $r/s \in \mathbb{Q}$ is a root of $p(x)$.

i.e $p(r/s) = 0$

$$a_n \frac{r^n}{s^n} + a_{n-1} \frac{r^{n-1}}{s^{n-1}} + \cdots + a_0 = 0$$

$\Rightarrow a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_0 s^n = 0$

Thus $a_n r^n = s\left(-a_{n-1} r^{n-1} - \cdots - a_0 s^{n-1}\right)$

$\Rightarrow s \mid a_n$

Similarly $r \mid a_0$.

Example. $f(x) = x^3 - 3x - 1 \in \mathbb{Z}[x]$

We have to check the irreducibility of $f(x)$ over $\mathbb{Q}[x]$. The possible roots are ± 1 but none of them satisfies the eqn. Hence it is irreducible.

Prop? Let I be a proper ideal in an UFD R and let $p(x)$ be a non-constant monic poly in $R[x]$. If the image of $p(x)$ in $(R/I)[x]$ can not be factored into two polys of smaller deg then $p(x)$ is irreducible in $R[x]$.

Pf: Suppose $p(x)$ can not be factored in $(R/I)[x]$ but $p(x)$ is reducible in $R[x]$ i.e $p(x) = a(x)\,b(x)$ where $a(x)$ & $b(x)$ are monic polys in $R[x]$.

Now reducing the coeffs modulo I gives a factorization in $(R/I)[x]$ with non-constant factors which is a contradiction.

Example. $f(x) = x^3+x+1 \in \mathbb{Z}[x]$.

Consider $\bar{f}(x) = x^3+x+\bar{1} \in \mathbb{Z}/2\mathbb{Z}[x]$.

it is irreducible over $\mathbb{Z}/2\mathbb{Z}[x]$

hence it is irreducible over $\mathbb{Z}[x]$.

Example. $f(x) = x^2+1 \in \mathbb{Z}[x]$.

$f(x)$ is irreducible over $\mathbb{Z}/3\mathbb{Z}[x]$

but it is reducible over $\mathbb{Z}/2\mathbb{Z}[x]$

Propn [Eisenstein's Criterion]

Let P be a prime ideal of the integral domain R and let

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in R[x]$

where $(n \geq 1)$.

Suppose $a_{n-1}, a_{n-2}, \ldots, a_1, a_0 \in P$ and $a_n \notin P$ and $a_0 \notin P^2$.

Then $f(x)$ has no divisor of deg d s.t $1 \leq d \leq n-1$.

i.e $f(x)$ is irreducible over $F[x]$ and if $f(x)$ is monic then f is irreducible over $R[x]$,

Example (1) $f(x) = x^4 + 10x + 5 \in \mathbb{Z}[x]$ is irreducible by EC with the prime ideal $P = (5)$.

(2) $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

$$= \frac{x^p - 1}{x - 1}.$$

$$f(x) = \Phi_p(x+1)$$

$$= \frac{(x+1)^p - 1}{x}$$

$$= x^{p-1} + \binom{p}{1} x^{p-2} + \cdots + \binom{p}{p-1} \in \mathbb{Z}[x].$$

Then by EC $f(x)$ irreducible for the prime p and hence $\Phi_p(x)$ irreducible