Irreducibility Criterion

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

Pf: If $R[x]$ is an UFD then R is also 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 we can write $p(x) = d\,p'(x)$ where $d \in R$ so d has a 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 irreducible in $F[x]$.

By Gauss' lemma such a factorization in $F[x]$ implies there is a factorization of $p(x)$ in $R[x]$. Since $p(x)$ is primitive each factor of $p(x)$ is also primitive. Thus by result proved in last lecture each factor is irreducible in $R[x]$. This proves that $p(x)$ can be written as finite product of irreducibles 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 factorizations in $R[x]$

Now viewing it as a factorization in $F[x]$ we have $r = s$ & $q_i(x) \sim q_i'(x)$

are associates in $F[x]$ hence they are associates in $R[x]$.

Thus $R[x]$ is an UFD.

Propn. Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$. If $r/s \in \mathbb{Q}$ s.t $\gcd(r,s)=1$ is a root of $f(x)$ then $r \mid a_0$ and $s \mid a_n$. In particular, if $f(x)$ is monic and $f(d) \neq 0$ for all integers d dividing the constant term of $f(x)$, then $f(x)$ has no root in $\mathbb{Q}$.

Pf: By hypothesis $f(r/s) = 0$

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

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

$\Rightarrow s \mid a_n$ Similarly, $r \mid a_0$.

Example. The poly $x^3 - 3x - 1 \in \mathbb{Z}[x]$ is irreducible. We have to check the irreducibility of the poly in $\mathbb{Q}[x]$. The possible roots are ± 1. but none of them satisfies the eqn. Hence the poly is irreducible.

Propn. Let I be a proper ideal in a 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 $p(x)$ 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 mod I gives a factorization in $(R/I)[x]$ with non-constant factors which is a contradiction.

Remark The irreducibility check is possible if we can find a proper ideal I s.t the image of the poly in $(R/I)[x]$ is irreducible.

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

$I = 2\mathbb{Z}$. $\bar{f}(x) = x^3+x+1 \in \mathbb{Z}/2\mathbb{Z}[x]$ is irreducible over $\mathbb{Z}/2\mathbb{Z}[x]$ but $f(x)$ is irreducible over $\mathbb{Z}[x]$.

Example. $f(x) = x^2+1$. is irreducible in $\mathbb{Z}[x]$ as it is irreducible over $\mathbb{Z}/3\mathbb{Z}[x]$ but it is reducible in $\mathbb{Z}/2\mathbb{Z}[x]$.

Remark: x^4+1 is irreducible over $\mathbb{Z}[x]$ but is reducible modulo every prime. $\mathbb{Z}/p\mathbb{Z}[x]$.

Propn [Eisenstein's Criterion]

Let P be be a prime ideal of an int domain R and let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a poly in $R[x]$. 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 $1 \le d \le n-1$.

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 $p = (5)$.

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

We can not directly apply EC to $\Phi_p(x)$ but

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

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

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

Example. $f(x) = x^4 + 1$.

$$g(x) = f(x+1) = (x+1)^4 + 1$$
$$= x^4 + 4x^3 + 6x^2 + 4x + 2.$$

By EC's $g(x)$ is irreducible with the prime ideal 2.

Hence $f(x)$ is also irreducible.