Lecture 38

Wednesday, April 8, 2015 10:01 AM

Irreducibility

Prop F a field, $p \in F[x]$. Then p has a factor of degree 1 $\iff$ p has a root in F.

I.e., $\exists \alpha \in F$ s.t. $p(\alpha) = 0$.

Pf If $p = (a_1 x + a_0) \cdot q$ then

$$p = a_1 (x - \alpha) q \text{ for } \alpha = \frac{-a_0}{a_1} \text{ so}$$

$$p(\alpha) = a_1 (\alpha - \alpha) q(\alpha) = 0.$$

Now suppose $p(\alpha) = 0$. By division algorithm

$$p = q \cdot (x - \alpha) + r \text{ where } r \text{ is a constant poly.}$$

Thus $p(\alpha) = q(\alpha) \cdot 0 + r(\alpha)$

$$\| \qquad \|$$

$$0 \qquad 0 + r = r$$

$\Rightarrow p = q \cdot (x - \alpha)$. $\square$

Prop A polynomial of degree 2 or 3 over a field F is reducible $\iff$ it has a root $\alpha \in F$.

Pf Polynomials of degree 2 or 3 are reducible $\iff$ at least one factor is degree 1

(using $\deg(fg) = \deg(f) + \deg(g) = 2 \text{ or } 3$). $\square$

Prop $p = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in R[x]$, R a UFD. If $\frac{r}{s} \in \mathrm{Frac}(R)$ w/ r, s relatively prime & $p\left(\frac{r}{s}\right) = 0$ then

$$r \mid a_0 \quad \text{and} \quad s \mid a_n$$

Cor If p is monic & $p(d) \neq 0 \ \forall d \mid a_0$, then p has no roots in $\mathrm{Frac}(R)$. $\square$

Pf of Prop $p\left(\frac{r}{s}\right) = 0 = a_n \left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_0$

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

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

$$\Rightarrow s \mid a_n r^n \Rightarrow s \mid a_n.$$

To get $r \mid a_0$, solve for $a_0 s^n$ above. $\square$

e.g. $x^3 - 3x - 1$ is reducible in $\mathbb{Z}[x]$

$\iff$ (G's L) reducible in $\mathbb{Q}[x]$

$\iff$ has a rational root (deg 3) in $\mathbb{Q}$

Rational roots of $x^3 - 3x - 1$ are in fact integers (denom(1) which divide -1 : either 1 or -1.

$1^3 - 3\cdot 1 - 1 = -3$, $(-1)^3 - 3(-1) - 1 = 1$

So $x^3 - 3x - 1$ is irreducible in $\mathbb{Z}[x]$.

Schönemann's Criterion R a UFD, $f \in R[x]$ monic of degree n. Suppose that for some $a \in R$, and some irred $\pi \in R$,

$$f \equiv (x-a)^n \bmod \pi R[x]$$

& $f(a) \not\equiv 0 \bmod \pi^2 R$

Then f is irred mod $\pi^2 R[x]$ $\Rightarrow$ irred in $R[x]$.

Pf Suppose $f \equiv f_1 f_2 \bmod \pi^2 R[x]$ and also assume $f \equiv (x-a)^n \bmod \pi R[x]$. Then

$f_1 f_2 \equiv (x-a)^n \bmod \pi R[x]$ and

$R[x]/\pi R[x] = (R/(\pi))[x]$ is a UFD b/c $R/(\pi)$ is a field. Thus $f_i \equiv (x-a)^{n_i} \bmod \pi R[x]$ for $i = 1, 2$, $n_i \in \mathbb{Z}^+$. Thus $f(a) \equiv f_1(a) f_2(a)$

$\equiv 0 \bmod \pi R$

Need R a PID???
Need mod π^2 not just mod π???

Defn Let p be a rational prime. The p-th cyclotomic polynomial $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$

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

Cor Φ_p is irred in $\mathbb{Z}[x]$.

Pf Since $(x-1)\Phi_p(x) = x^p - 1$,

$$(x-1)\Phi_p(x) \equiv (x-1)^p \mod p\mathbb{Z}[x]$$

[in $\mathbb{Z}/p\mathbb{Z}[x]$, $(f+g)^p = f^p + g^p$]

Since $\mathbb{Z}/p\mathbb{Z}[x]$ is an integral domain, we can cancel a factor of $(x-1)$ to get

$$\Phi_p(x) \equiv (x-1)^{p-1} \mod p\mathbb{Z}[x].$$

Now $\Phi_p(1) = p \not\equiv 0 \mod p^2\mathbb{Z}[x]$.

Thus by Schönemann, Φ_p is irred. □

Cor [Eisenstein's Criterion] R as in Schönemann's criterion, $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R[x]$.

Suppose that for some irred $\pi \in R$,

$\pi \mid a_i$, $i = 0, 1, \ldots, n-1$

$\pi^2 \nmid a_0$.

Then f is irred in $R[x]$.

Pf Schönemann's crit w/ $a = 0$. □

e.g. • $x^4 + 10x + 5$ irred in $\mathbb{Z}[x]$ b/c $5 \mid 5, 10$ but $5^2 \nmid 5$

• $x^n - a \in \mathbb{Z}[x]$ w/ $p \mid a$ but $p^2 \nmid a$.
then $x^n - a$ irred.