Lecture 39

Friday, April 10, 2015 10:04 AM

Schömmann's Criterion R an integral domain, $f \in R[x]$ monic of deg n. Suppose for some $a \in R$ & some prime ideal $I \trianglelefteq R$,

$$f \equiv (x-a)^n \mod I[x]$$

& $f(a) \not\equiv 0 \mod I^2$. Then f is irred mod $I^2[x]$ & thus irred in $R[x]$.

Pf Suppose $f \equiv f_1 f_2 \mod I^2[x]$. Then

$f_1 f_2 \equiv (x-a)^n \mod I[x]$. I.e.

$$\overline{f_1 f_2} = \overline{(x-a)}^n \in (R/I)[x].$$

R/I is an integral domain & thus has a field of fractions $F = \mathrm{Frac}(R/I)$. So

$$\overline{f_1 f_2} = \overline{(x-a)}^n \text{ in } F[x]. \implies \begin{aligned} \bar{f_1} &= (x-a)^{n_1} \\ \bar{f_2} &= (x-a)^{n_2} \end{aligned}$$

Friday, April 10, 2015 10:10 AM

b/c $F[x]$ is a UFD. These are eq'ns w/o denominators, thus the equations

$\overline{f_i} = \overline{(x-a)^{n_i}}$ hold in $(R/I)[x]$.

Thus $f_i(a) \equiv 0 \mod I$. i.e. $f_1(a), f_2(a) \in I$.

Thus $f_1(a) f_2(a) \in I^2$

$\qquad\qquad \parallel$

$\qquad f(a) \mod I$. $\square$

Eisenstein's Criterion R an integral domain, $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ monic in $R[x]$, $I \trianglelefteq R$ prime. Suppose that $a_i \in I$ but $a_0 \notin I^2$ then f is irred in $R[x]$.

Pf $a=0$ in Schönemann's crit. $\square$

$(R/I)[x] \subseteq F[x]$

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

Frobenius endomorphism of characteristic p rings:

R comm ring w/ $1 \neq 0$ has characteristic $n > 0$ if

$\underbrace{1 + 1 + \cdots + 1}_{n} = 0$ & n is the smallest pos integer such that this happens.

Note If R has char n, then $\underset{\underbrace{r + r + \cdots + r}_{n \text{ times}}}{\overset{}{n \cdot r}} = 0 \ \forall r \in R$.

Suppose R has char p, p a rational prime.

Then $\mathrm{Frob} : R \longrightarrow R$ is a ring hom.

$r \longmapsto r^p$

$$\mathrm{Frob}(rs) = (rs)^p = r^p s^p$$

$$\mathrm{Frob}(r+s) = (r+s)^p = \sum_{k=0}^{p} \binom{p}{k} r^k s^{p-k} = r^p + s^p$$

b/c $\binom{p}{k} = \dfrac{p!}{k!(p-k)!}$ so if $0 < k < p$, then $p \mid \binom{p}{k}$.

So in $(\mathbb{Z}/p\mathbb{Z})[x]$,

$$(x-1)^p = x^p + (-1)^p = x^p - 1 \in (\mathbb{Z}/p\mathbb{Z})[x].$$

$$\sum_{k=0}^{p} \binom{p}{k} r^k s^{p-k} = \underbrace{r^0 \cdot s^p}_{k=0} + \underbrace{r^p s^{p-p}}_{k=p} + \cancel{p\sum_{k=1}^{p} l_k r^k s^{p-k}} \to 0$$

$$= s^p + r^p.$$

Loose ends w/ polys over fields:

F a field.

<u>Prop</u> Maximal ideals in $F[x]$ are of the form $(f(x))$ where f is irred in $F[x]$.

So $F[x]/(f(x))$ is a field $\Leftrightarrow$ f is irred.

<u>pf</u> $F[x]$ is a Euclidean domain and thus it's a PID. Maximal ideals of a PID are principal ideals gen by irreds. $\square$

e.g. $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.

Prop If g is nonconstant in $F[x]$, $g = f_1^{n_1} \cdots f_k^{n_k}$ fact'n into irreds w/ f_i distinct, then

$$F[x]/(g) \cong F[x]/(f_1^{n_1}) \times \cdots \times F[x]/(f_k^{n_k})$$

Pf CRT. $\square$

Prop If $f(x)$ has roots $\alpha_1, \ldots, \alpha_k \in F$ then f has $(x-\alpha_1)\cdots(x-\alpha_k)$ as a factor.

Thus a polynomial of deg n has $\leq n$ roots (even when counted w/ multiplicity).

Pf Induction on k + $F[x]$ is a UFD. $\square$

Prop A finite subgroup of the multiplicative gp of units in a field is cyclic.

Pf Let $G \leq F^\times$ be a finite subgp of $F^\times$, F a field. Then

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

(FT f.g. ab gps)

for $n_k \mid n_{k-1} \mid \cdots \mid n_2 \mid n_1$ integers.

Thus each direct factor $\mathbb{Z}/n_i\mathbb{Z}$ contains n_k elts of order dividing n_k.

If $k > 1$, this says that there are more than

$x^{n_k} - 1$ has $> n_k$ roots

which contradicts $x^{n_k} - 1$ having $\leq n_k$ roots.

Thus $k = 1$, & $G \cong \mathbb{Z}/n_k\mathbb{Z}$, which is cyclic! $\square$

Cor $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}_{p-1}$. $\square$