Lecture 15 Monday Feb 22

LEM 5 (Eisenstein) Assume R is an integral domain

Given prime ideal $I \neq R$

Given monic poly $f \in R[x]$ with $\deg \geq 1$:

$$f = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} + x^n \qquad c_i \in R$$

Assume $c_i \in I$ $0 \leq i \leq n-1$

$$c_0 \notin I^2$$

Then f is irred in $R[x]$

pf Suppose not. $\exists$ nonunits $a, b \in R[x]$ s.t.

$$f = ab$$

Write

$$a = a_0 + a_1 x + \cdots + a_r x^r \qquad a_i \in R$$

$$b = b_0 + b_1 x + \cdots + b_s x^s \qquad b_j \in R$$

$$r \geq 1, \quad s \geq 1$$

$$r + s = n$$

$$a_r b_s = 1$$

$$a_r, b_s \notin I$$

claim $a_i \in I$ $0 \le i \le r-1$ and

$b_j \in I$ $0 \le j \le s-1$

pf of cl def

$$r = \min\{ i \mid 0 \le i \le r,\ a_i \notin I \}$$

$$s = \min\{ j \mid 0 \le j \le s,\ b_j \notin I \}$$

show $r = r$, $s = s$

Suppose not. Then

$$r + s < r + s = n$$

Consider image of $f = ab$ in $R/I[x]$:

$$x^n = \left(\underset{\neq 0}{\bar{a}_0} x^0 + \cdots + \bar{a}_r x^r \right)\left(\underset{\neq 0}{\bar{b}_0} x^0 + \cdots + \bar{b}_s x^s \right)$$

For this poly the coef of x^{r+s} is

$\bar{a}_0 \bar{b}_0$, which is $\neq 0$ since R/I is an integral domain.

This is a contradiction. claim proved ✓

By constr

$$c_0 = a_0 b_0$$

By the claim,

$$a_0 \in I \quad , \quad b_0 \in I$$

So $c_0 = a_0 b_0 \in I^2$ cont.

Therefore f is irred. □

Now consider $R = \mathbb{Z}$

LEM 6 (Eisenstein) Given monic poly $f \in \mathbb{Z}[x]$ with degree $n \geq 1$:

$$f = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} + x^n \qquad c_i \in \mathbb{Z}$$

Assume $\exists$ prime $p \in \mathbb{Z}$ st

$$p \mid c_i \qquad 0 \leq i \leq n-1$$

and $$p^2 \nmid c_0$$

Then f is irreducible in $\mathbb{Z}[x]$

pf Apply LEM 5 to the ideal $I = p\mathbb{Z}$

9.5 Polynomials over fields, II

Next general goal:

Let F denote a field

Recall group of units $F^\times = F \setminus 0$

Show each finite subgroup of $F^\times$ is cyclic.

First we obtain some results about groups.

Given relatively prime integers $r, s \geq 2$

Let G denote an abelian group with $|G| = rs$

Define

$$A = \{ a \in G \mid a^r = 1 \}$$ subgroups of G

$$B = \{ b \in G \mid b^s = 1 \}$$

LEM 1 With above notation

$$|A| = r, \qquad |B| = s$$

Moreover the map

$$\varphi: \begin{array}{ccc} A \times B & \longrightarrow & G \\ (a, b) & \longmapsto & ab \end{array}$$

is an isomorphism of groups.

pf Each element of A has order that divides r
so this order is rel prime to s

So $|A|$ is rel prime to s by Cauchy thm (541)

Also $|A|$ divides $|G| = rs$ by Lagrange thm

So $|A|$ divides r

So $|A| \leq r$

Similarly $|B| \leq s$

By constr φ is hom of groups.

Show φ is bijective.

First show φ is surjective.

Since r, s are rel prime, $\exists$ integers e, f st

$$1 = er + fs$$

Fix $\theta \in G$ show θ is an image of φ

Define $a = \theta^{fs}$, $b = \theta^{er}$

Note $(\theta^A)^r = \theta^{rA} = \theta^{|G|} = 1$

So $\theta^A \in A$

so $a = (\theta^A)^f \in A$

Similarly $b \in B$

Also $\theta = \theta^1 = \theta^{er+fA} = ab = \varphi(a,b)$

So θ is in image of φ

φ is surjective.

Now $rA = |G| \leq |A \times B| = |A||B|$
$\leq r \quad \leq A$

So $|A| = r, \quad |B| = A$

and φ is a bijection. □

Given a finite abel group G with $|G| > 1$
$= n$

Factor n:

$$n = \overbrace{p_1^{e_1}}^{n_1} \overbrace{p_2^{e_2}}^{n_2} \cdots \overbrace{p_t^{e_t}}^{n_t} \qquad t \geq 1$$

$p_1, p_2, \ldots, p_t$ mut distinct primes
$e_i \geq 1 \qquad 1 \leq i \leq t$

For $1 \leq i \leq t$ define a subgroup

$$G_i = \{ a \in G \,/\, a^{n_i} = 1 \}$$

By LEM 1 and induction on t,

$$|G_i| = n_i \qquad (1 \leq i \leq t)$$

Moreover the map

$$\varphi : \begin{array}{ccc} G_1 \times G_2 \times \cdots \times G_t & \to & G \\ (a_1, a_2, \ldots, a_t) & \to & a_1 a_2 \cdots a_t \end{array}$$

is an isomorphism of groups.

2/22/16
10

LEM 2 Given a finite abel group G with $n = |G| > 1$.

TFAE

(i) G is cyclic

(ii) $\forall$ pos integers d that divide n,

$$|\{a \in G \mid a^d = 1\}| = d$$

(iii) $\forall$ pos integers d that divide n,

$$|\{a \in G \mid a^d = 1\}| \leq d$$

pf (i) $\rightarrow$ (ii) Let θ denote a generator for G

So $\theta^n = 1$, $\theta^i \neq 1$ $(1 \leq i \leq n-1)$

$$G = \{\theta^i \mid 0 \leq i \leq n-1\}$$

$\forall\, d/n$ we have

$$\{a \in G \mid a^d = 1\} = \{\theta^{\frac{n}{d} i} \mid 0 \leq i \leq d-1\}$$

d elements

(ii) $\rightarrow$ (iii) clear

(iii) → (i) Factor n

$$n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$$

as below LEM 1.

Fa $1 \le i \le t$ define G_i, n_i as below LEM 1.

Also define

$$\hat{G}_i = \{ a \in G \mid a^{(n_i/p_i)} = 1 \}$$

So $\hat{G}_i \subseteq G_i$

By assumption $|\hat{G}_i| \le \frac{n_i}{p_i}$

So $|\hat{G}_i| \le \frac{n_i}{p_i} < n_i = |G_i|$

So $\hat{G}_i \subsetneq G_i$

$\exists$ $a_i \in G_i \setminus \hat{G}_i$

By exists a_i has order n_i

Define $\theta = a_1 a_2 \cdots a_t$

Note n_i, n_j rel prime $(1 \le i < j \le t)$

So θ has order $n_1 n_2 \cdots n_t = n$ by CH REM THM

So θ generates G, so G is cyclic. □