Lecture 24: Field extension

Friday, June 1, 2018 10:58 AM

We were proving:

Theorem. Suppose F is a field and $f(x) \in F[x]$ is an irreducible polynomial. Then

(1) $\exists$ a field E and an injective ring homomorphism $i: F \hookrightarrow E$ s.t.

(1-a) for some $\alpha \in E$, $i(f)(\alpha) = 0$.

($f(x)$ has a zero in E.)

(1-b) $E = \{ i(a_0) + i(a_1)\alpha + \cdots + i(a_{n-1})\alpha^{n-1} \mid a_0, \ldots, a_{n-1} \in F \}$

where $n = \deg f$.

(2) If E' is a field and $i': F \hookrightarrow E'$ is an injective ring homomorphism that satisfy (1-a) and (1-b), then $\exists\, \phi: E \xrightarrow{\simeq} E'$ s.t. $\phi(i(a)) = i'(a)$ for any $a \in F$.

$$\begin{tikzcd} & E \arrow[d, dashed, "\phi"] \\ F \arrow[ur, hook, "i"] \arrow[dr, hook, "i'"'] \arrow[r, phantom, "\circlearrowleft"] & {} \\ & E' \end{tikzcd}$$

And based on the discussion that we had we will use $F[x]/\langle f(x) \rangle$.

Lecture 24: Field extension

Wednesday, May 30, 2018 11:19 AM

Proof of theorem (1) Since $f(x)$ is irreducible in $F[x]$ and $F[x]$ is a PID, $\langle f(x)\rangle$ is a maximal ideal. Hence $E := F[x]/\langle f(x)\rangle$ is a field. Let $i: F \to F[x]/\langle f(x)\rangle$, $i(c) = c + \langle f(x)\rangle$.

Clearly i is a ring homomorphism;

Claim i is injective.

Pf of Claim. $i(c)=0 \Rightarrow c+\langle f(x)\rangle = 0+\langle f(x)\rangle$

$\Rightarrow c \in \langle f(x)\rangle$

Since $\langle f(x)\rangle$ is a proper ideal, $\langle f(x)\rangle \cap U(F) = \emptyset$

$c=0$.

Let $\alpha := x + \langle f(x)\rangle$, and $f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_0$.

Claim. $i(f)(\alpha) = 0$.

Pf of claim. $i(f)(\alpha) = i(c_n)(x+I)^n + i(c_{n-1})(x+I)^{n-1} + \cdots + i(c_0)$

$= (c_n+I)(x^n+I) + \cdots + (c_1+I)(x+I) + (c_0+I)$ (where $I = \langle f(x)\rangle$)

$= (c_n x^n + \cdots + c_1 x + c_0) + I = f(x) + I = 0 + I$.

- By long division, for any polynomial $p(x)$, $\exists!\, q(x), r(x) \in F[x]$,

$p(x) = f(x)\, q(x) + r(x)$ and $\deg r < \deg f = n$.

Lecture 24: Field extension

Wednesday, May 30, 2018 11:32 AM

$$\Rightarrow \quad p(x)+I = \underbrace{f(x)q(x)}_{\text{in } I} + r(x) + I = r(x) + I$$

Since $\deg r < n$, $\exists!\ a_0, \dots, a_{n-1} \in F$ s.t.

$$r(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \text{ ; and so}$$

$$p(x)+I = (a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}) + I$$

$$= (a_0+I) + (a_1+I)(x+I) + \cdots + (a_{n-1}+I)(x+I)^{n-1}$$

$$= i(a_0) + i(a_1)\,\alpha + \cdots + i(a_{n-1})\,\alpha^{n-1}.$$

(2) Let $\phi_{\alpha'} : F[x] \to E'$, $\phi_{\alpha'}(p(x)) = p(\alpha')$. Then $f(x) \in \ker \phi_{\alpha'}$.

Since $f(x)$ is irreducible, $\ker \phi_{\alpha'} = \langle f(x) \rangle$. And so by the 1^{st} isomorphism theorem, $F[x]/\langle f(x)\rangle \xrightarrow{\sim} \operatorname{Im} \phi_{\alpha'}$,

$$p(x) + \langle f(x) \rangle \longmapsto p(\alpha').$$

Since E' satisfies (1-b), $\operatorname{Im}\phi_{\alpha'} = E'$. This implies

$$\begin{tikzcd} F[x]/\langle f(x)\rangle \arrow[rr, "\sim"] & \arrow[d, phantom, "\circlearrowleft"] & E' \\ & F \arrow[ul, hook] \arrow[ur, hook] & \end{tikzcd}$$

and claim follows. ■

Lecture 24: Finite fields

Friday, June 1, 2018 11:15 AM

<u>Proposition</u>. Suppose $f(x) \in \mathbb{Z}_p[x]$ is an irreducible poly. of degree n. Then $E := \mathbb{Z}_p[x]/\langle f(x)\rangle$ is a field of order p^n.

<u>Pf.</u> Let $E := \mathbb{Z}_p[x]/\langle f(x)\rangle$. Since $\mathbb{Z}_p[x]$ is a PID and $f(x)$ is irred., $\langle f(x)\rangle$ is a maximal ideal of $\mathbb{Z}_p[x]$.

Hence $E := \mathbb{Z}_p[x]/\langle f(x)\rangle$ is a field.

<u>Claim 1</u> $E = \{ a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + \langle f(x)\rangle \mid a_i \in \mathbb{Z}_p \}$

<u>Pf of claim</u>. any element of E is of the form $g(x) + \langle f(x)\rangle$. By long division, $\exists\, q(x), r(x)$ s.t. $g(x) = q(x)f(x) + r(x)$ and $\deg r < n$. Hence $g(x) + \langle f(x)\rangle = r(x) + q(x)f(x) + \langle f(x)\rangle$

$$= r(x) + \langle f(x)\rangle \in \text{RHS}.$$

Clearly RHS $\subseteq$ LHS and claim follows.

<u>Claim 2</u> $(a_0, \ldots, a_{n-1}) \in \mathbb{Z}_p^n \overset{\theta}{\longmapsto} (a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}) + \langle f(x)\rangle$

is a bijection from $\mathbb{Z}_p^n$ to E.

<u>Pf</u> The 1st claim implies θ is surjective. So it is enough to show θ is injective. Suppose $\theta(a_0, \ldots, a_{n-1}) = \theta(a_0', \ldots, a_{n-1}')$.

Lecture 24: Finite fields

Friday, June 1, 2018 11:25 AM

then $a_0+a_1x+\cdots+a_{n-1}x^{n-1}+\langle f(x)\rangle = a_0'+a_1'x+\cdots+a_{n-1}'x^{n-1}+\langle f(x)\rangle$

And so $(a_0-a_0')+(a_1-a_1')x+\cdots+(a_{n-1}-a_{n-1}')x^{n-1} = f(x)\,g(x)$

$\Rightarrow \underbrace{\deg f}_{n} + \deg g = \deg$ of LHS $< n$

$\Rightarrow \deg g < 0 \Rightarrow \deg g = -\infty$ and $g=0$

$\Rightarrow$ LHS $=0 \Rightarrow a_0=a_0',\ a_1=a_1',\ \ldots, a_{n-1}=a_{n-1}'$;

this implies θ is injective.

Hence $|E| = |\mathbb{Z}_p^n| = p^n$. ∎

<u>Warning</u>. E is NOT $\mathbb{Z}_p^n$ as a ring. $\mathbb{Z}_p^n$ has many zero-divisors if $n>1$, but E is a field.