Finite fields

Tuesday, September 5, 2017 8:44 PM

In the previous lecture we proved:

<u>Theorem</u>. Let F be a field, and $p(x)$ be an irreducible polynomial in $F[x]$. Then there are a field E, an embedding $F \overset{i}{\hookrightarrow} E$, and $\alpha \in E$ such that $i(p)(\alpha) = 0$.

<u>Ex.</u> Let $f_0(x) \in \mathbb{Z}_p[x]$ be an irreducible polynomial of degree d. Then there is a field extension $F \supseteq \mathbb{Z}_p$ which has a zero of f_0 and $|F| = p^d$.

<u>Solution</u>. By the previous theorem, $\exists$ a field extension $E \supseteq \mathbb{Z}_p$ and $\alpha \in E$ such that $f_0(\alpha) = 0$.

Let $\phi_\alpha : \mathbb{Z}_p[x] \longrightarrow E$ be the evaluation at α. Then

① $\exists\, m_\alpha(x) \in \mathbb{Z}_p[x]$ which is irreducible and

$$\ker \phi_\alpha = \langle m_\alpha(x) \rangle ;$$

② $\operatorname{Im} \phi_\alpha$ is a field;

③ $\operatorname{Im} \phi_\alpha = \{ c_0 + c_1\alpha + \cdots + c_{d'-1}\alpha^{d'-1} \mid c_i \in \mathbb{Z}_p \}$ where $d' = \deg m_\alpha$.

. As $f_0(\alpha) = 0$, $f_0(x) \in \ker \phi_\alpha$. So $\langle f_0(x) \rangle \subseteq \langle m_\alpha(x) \rangle$. Since $f_0(x)$

Finite fields

Tuesday, September 5, 2017 8:58 PM

is irreducible $\langle f_0(x)\rangle$ is a maximal ideal. Therefore

$$\langle f_0(x)\rangle = \langle m_\alpha(x)\rangle;$$

and $f_0(x) \mid m_\alpha(x)$, $m_\alpha(x) \mid f_0(x)$. Thus $\deg f_0 = \deg m_\alpha$.

And so $F = \{c_0 + c_1\alpha + \cdots + c_{d-1}\alpha^{d-1} \mid c_i \in \mathbb{Z}_p\}$ is a field.

<u>Claim</u>. $\mathbb{Z}_p^d \xrightarrow[\ell]{} F$, $(c_0, \ldots, c_{d-1}) \longmapsto c_0 + c_1\alpha + \cdots + c_{d-1}\alpha^{d-1}$

is a bijection.

<u>Pf of claim.</u> We already know that ℓ is surjective.

<u>why is it injective?</u>

$$\ell(c_0, \ldots, c_{d-1}) = \ell(c_0', \ldots, c_{d-1}')$$

$$\Rightarrow \quad c_0 + c_1\alpha + \cdots + c_{d-1}\alpha^{d-1} = c_0' + c_1'\alpha + \cdots + c_{d-1}'\alpha^{d-1}$$

$$\Rightarrow \quad (c_0 - c_0') + (c_1 - c_1')\alpha + \cdots + (c_{d-1} - c_{d-1}')\alpha^{d-1} = 0$$

$$\Rightarrow \quad (c_0 - c_0') + (c_1 - c_1')x + \cdots + (c_{d-1} - c_{d-1}')x^{d-1} \in \ker \phi_d = \langle m_\alpha(x)\rangle$$

$$\Rightarrow \quad m_\alpha(x)\, q(x) = (c_0 - c_0') + (c_1 - c_1')x + \cdots + (c_{d-1} - c_{d-1}')x^{d-1}$$

for some $q(x) \in \mathbb{Z}_p[x]$.

$$\Rightarrow \underbrace{\deg m_\alpha}_{d} + \deg q = \deg\left((c_0 - c_0') + \cdots + (c_{d-1} - c_{d-1}')x^{d-1}\right)$$

Finite fields

Tuesday, September 5, 2017 9:15 PM

So $q(x)=0$; and so $(c_0-c_0')+(c_1-c_1')x+\cdots+(c_{d-1}-c_{d-1}')x^{d-1}=0$,

which implies $c_0=c_0'$, $c_1=c_1'$, ..., and $c_{d-1}=c_{d-1}'$. And so

$$(c_0,c_1,\ldots,c_{d-1})=(c_0',c_1',\ldots,c_{d-1}'),$$

which means l is injective. ■

Therefore $|F|=|\mathbb{Z}_p^d|=p^d$. ■

<u>Ex.</u> (a) Show that x^3-x+1 is irreducible in $\mathbb{Z}_3[x]$.

(b) Show that there is a field F such that $|F|=27$.

<u>Solution.</u> (a) A degree 3 polynomial in $\mathbb{Z}_3[x]$ is irreducible if and only if it has no zero in $\mathbb{Z}_3$.

For $a\in\mathbb{Z}_3$, by Fermat's theorem, $a^3-a+1=a-a+1=1$.

So x^3-x+1 does not have a zero in $\mathbb{Z}_3$. And so x^3-x+1 is irreducible in $\mathbb{Z}_3[x]$.

(b) By the previous example, there is a field F of order $3^{\deg(x^3-x+1)}=3^3=27$. ■

Finite fields

Tuesday, September 5, 2017 9:26 PM

<u>Ex.</u> Let $f_0(x) \in \mathbb{Z}_p[x]$ be an irreducible polynomial of degree $d \geq 1$.

Suppose α is a zero of $f_0(x)$ in a field extension E of $\mathbb{Z}_p$.

Then $\alpha^{(p^d)} = \alpha$.

<u>Pf.</u> By the previous examples we know $F = \mathbb{Z}_p[\alpha]$ is a field of order p^d. So $\alpha \in U(F) = F \setminus \{0\}$.

$U(F)$ is a group of order $p^d - 1$. So by Lagrange theorem $\alpha^{|U(F)|} = 1$, which implies $\alpha^{(p^d-1)} = 1$; and therefore

$$\alpha^{(p^d)} = \alpha. \quad \blacksquare$$