Lecture 20: Finite fields

Sunday, March 17, 2019 9:57 PM

In the previous lecture we proved that if F is a finite field of order p^d, then $x^{p^d}-x = \prod_{\alpha\in F}(x-\alpha)$.

This would be our guideline to show the following:

<u>Theorem</u>. For any prime p and any $d\in\mathbb{Z}^+$, there is a finite field of order p^d.

<u>Pf</u>. Let E be a splitting field of $x^{p^d}-x$ over $\mathbb{Z}_p$. Let $X := \{\alpha\in E \mid \alpha^{p^d}-\alpha=0\}$.

<u>Claim 1</u>. X is a subfield of E.

<u>Pf of claim 1</u>. <u>Closed under addition</u>. Since $\mathbb{Z}_p$ is a subring of E, $\operatorname{char} E = p>0$. Hence for any $x,y\in E$, $(x+y)^p = x^p+y^p$ using binomial expansion. Hence as we have seen earlier in the course $(x+y)^{p^d} = x^{p^d}+y^{p^d}$ (using induction on d)

$\cdot\ \alpha,\beta\in X \Rightarrow (\alpha+\beta)^{p^d} = \alpha^{p^d}+\beta^{p^d} = \alpha+\beta \Rightarrow \alpha+\beta\in X$

<u>Closed under negation</u>. $(-1)^p=-1$ if $2\nmid p$ and $(-1)^p = 1 = -1$ if $p=2$. Hence for $\alpha\in X$ we have

Lecture 20: Finite fields

Sunday, March 17, 2019 10:01 PM

$(-\alpha)^{p^d} = (-1)^{p^d} \alpha^{p^d} = -\alpha \Rightarrow -\alpha \in X.$

Closed under multiplication

$\alpha, \beta \in X \Rightarrow (\alpha\beta)^{p^d} = \alpha^{p^d} \beta^{p^d} = \alpha\beta \Rightarrow \alpha\beta \in X.$

Multiplicative inverse

$\alpha \in X \setminus \{0\} \Rightarrow (\alpha^{-1})^{p^d} = (\alpha^{p^d})^{-1} = \alpha^{-1} \Rightarrow \alpha^{-1} \in X.$

(in any group G, $(g^{-1})^m = (g^m)^{-1}$.) ■

Claim 2. $X = E$.

Pf of Claim 2. Clearly $X \subseteq E$

. X is a field; $1^{p^d} = 1 \Rightarrow \mathbb{Z}_p \subseteq X$;

. All the zeros of $x^{p^d} - x$ are in X

So the smallest field that contains $\mathbb{Z}_p$ and zeros of $x^{p^d} - x$ is a subset of $X \Rightarrow E \subseteq X$. Therefore $E = X$.

Claim 3. $|E| = p^d$.

Pf of Claim 3. Since $E = X$ is the set of zeros of

Lecture 20: Finite fields

Sunday, March 17, 2019 10:32 PM

a polynomial $x^{p^d}-x$ of degree p^d in a field E, it has at most p^d elements (Recall. A poly. of degree m has at most m zeros in an integral domain.) So

$$|E| \leq p^d.$$

To show equality, it is enough to show $x^{p^d}-x$ does not have multiple zeros; that means there is no α such that $(x-\alpha)^2 \mid x^{p^d}-x$.

We use an idea from calculus: a poly. $p(x)$ has a multiple zero at α if and only if

$p(\alpha)=p'(\alpha)=0$ where $p'(x)$ is the derivative of $p(x)$.

Here we define $p'(x)$ in a formal way:

for $p(x)=a_n x^n + a_{n-1}x^{n-1}+\cdots+a_0 \in F[x]$, let

$p'(x) = n a_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$.

One can check that for $f_1, f_2 \in F[x]$ we have

$(f_1+f_2)' = f_1' + f_2'$ and $(f_1 f_2)' = f_1' f_2 + f_1 f_2'$.

Lecture 20: Finite fields

Sunday, March 17, 2019 10:42 PM

Suppose to the contrary that $(x-\alpha)^2 \mid x^{p^d}-x$ for some $\alpha \in E$. Then $x^{p^d}-x = (x-\alpha)^2 q(x)$ for some $q(x) \in E[x]$.

$$\Rightarrow \quad p^d x^{p^d-1} - 1 = 2(x-\alpha)q(x) + (x-\alpha)^2 q'(x)$$

$$\Rightarrow \quad -1 = 2(x-\alpha)q(x) + (x-\alpha)^2 q'(x)$$

char(E)=p

Evaluate at $\alpha \Rightarrow$

$$-1 = 2\underbrace{(\alpha-\alpha)}_{0} q(\alpha) + \underbrace{(\alpha-\alpha)^2}_{0} q'(\alpha) = 0$$

$\Rightarrow -1 = 0$ which is a contradiction.

Hence $x^{p^d}-x$ has p^d distinct zeros $\Rightarrow |E| \geq p^d$ as all the zeros of $x^{p^d}-x$ are in E. Overall we get that E is a field of order p^d. ∎

(In the rest of this lecture we reviewed all the topics covered in this course.)