Lecture 23: Finite fields

Tuesday, February 27, 2018 10:51 AM

. Let F be a finite field. Then $\mathbb{Z}/p\mathbb{Z} =: \mathbb{F}_p$ is a subfield of F where p is the characteristic of F (i.e. the additive order of 1).

Let $d := [F : \mathbb{F}_p]$. So $|F| = p^d$. Hence $\forall x \in F^\times$, $x^{p^d-1} = 1$; this implies $x^{p^d} = x$ $\forall x \in F$.

<u>Theorem</u>. For a prime p and positive integer d, there is a unique (up to isomorphism) finite field of order $q := p^d$. (It is denoted by $\mathbb{F}_q$ or $\mathbb{F}_q$.)

<u>Pf.</u> Let E be the splitting field of $x^{p^d} - x$ over $\mathbb{F}_p$; and let $\Omega := \{\alpha \in E \mid \alpha^{p^d} = \alpha\}$.

<u>Claim 1</u>. Ω is a subring of E.

<u>Pf.</u> For $a, b \in E$, $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = a^p + b^p$

$$\boxed{p \mid \binom{p}{i} \text{ if } 1 \le i \le p-1 \,;\ \mathrm{char}(E) = p}$$

Hence $(a+b)^{p^k} = a^{p^k} + b^{p^k}$.

$$\alpha, \beta \in \Omega \Rightarrow \left.\begin{cases} (\alpha-\beta)^{p^d} = \alpha^{p^d} + (-1)^{p^d} \beta^{p^d} = \alpha - \beta \\ (\alpha\beta)^{p^d} = \alpha^{p^d} \beta^{p^d} = \alpha\beta \end{cases}\right\} \Rightarrow \alpha - \beta,\ \alpha\beta \in \Omega.$$

<u>Claim 2</u>. $\Omega = E$.

Lecture 23: Finite fields

Tuesday, February 27, 2018 11:09 AM

Pf. $\forall \alpha \in \Omega \setminus \{0\}$, $\alpha^{p^d-2} = \alpha^{-1} \in \Omega$. So Ω is a subfield of E which contains all the zeros of $x^{p^d}-x$. So $\Omega = E$ as E is the splitting field of $x^{p^d}-x$.

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

Pf. We need to show $x^{p^d}-x$ does not have multiple roots.

Suppose $x^{p^d}-x = (x-\alpha)^2 p(x)$. Then after taking derivative

$\underbrace{p^d}_{0} x^{p^d-1} - 1 = 2(x-\alpha)\,p(x) + (x-\alpha)^2 p'(x)$; evaluate at α:

$-1 = 0$ which is a contradiction.

Hence E is a finite field of order p^d.

Now suppose F is a finite field of order p^d. Then any $\alpha \in F$ is a zero of $x^{p^d}-x$. Hence $x^{p^d}-x = q(x) \prod_{\alpha \in F} (x-\alpha)$.

Comparing degrees and the leading coeff. we get that $x^{p^d}-x = \prod_{\alpha \in F}(x-\alpha)$. Therefore F is the splitting field of $x^{p^d}-x$ over $\mathbb{F}_p$. (and we get the uniqueness.) ■

Remark. If $F^\times = \langle \alpha \rangle$, then $F = \mathbb{F}_p[\alpha]$. So $m_\alpha(x) \in \mathbb{F}_p[x]$ is irred. of degree d. Hence we get the existence of irred. poly. of any degree.

Lecture 23: Tower of finite extensions

Tuesday, February 27, 2018 12:19 PM

Lemma. Suppose E/F and K/E are two field extension, and $[E:F]$ and $[K:E]$ are finite. Then $[K:F]=[K:E][E:F]$; in particular it is finite.

Pf. Suppose $\{e_1,\dots,e_m\}$ is an F-basis of E, and $\{k_1,\dots,k_n\}$ is an E-basis of K. Then

$$K=\sum_{i=1}^{n} E k_i=\sum_{i=1}^{n}\sum_{j=1}^{m} F e_j k_i.$$

So the F-span of $\{e_j k_i\}$ is K. So to show $\{e_j k_i\}_{\substack{1\le j\le m\\ 1\le i\le n}}$ is an F-basis of K, it is enough to show $e_j k_i$ are F-linearly independent.

Suppose $\sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij} e_j k_i \overset{\circledast}{=} 0$. Since $\sum_{j=1}^{m} a_{ij} e_j \in E$ and k_i's are E-linearly indep., $\circledast$ implies $\sum_{j=1}^{m} a_{ij} e_j = 0$. $(\dagger)$

Since e_j's are F-linearly indep., $(\dagger)$ implies $a_{ij}=0$. ∎

Proposition A finite field extension E/F is algebraic; that means $\forall \alpha\in E$ is algebraic over F.

Pf. Suppose $[E:F]=d$. Then $\forall\alpha\in E$, $1,\alpha,\dots,\alpha^d$ are F-linearly dependent. And so $\exists\, c_0,\dots,c_d\in F$ (not all zero) s.t. $c_0+c_1\alpha+\cdots+c_d\alpha^d=0$ and the claim follows. ∎

Lecture 23: Algebraic closure

Tuesday, February 27, 2018 12:31 PM

Corollary. Suppose E/F is a field extension. If $\alpha,\beta\in E$ are algebr. over F, then $\alpha\pm\beta$, $\alpha\beta$, $\alpha\beta^{-1}$ (if $\beta\neq 0$) are algebraic over F.

Pf. α is algebraic over $F \Rightarrow F[\alpha]$ is a field and $[F[\alpha]:F]<\infty$.

β is algebraic over $F \Rightarrow \beta$ is algebraic over $F[\alpha] \Rightarrow [F[\alpha,\beta]:F[\alpha]]<\infty$

So $F[\alpha,\beta]/F$ is a finite extension. Hence $F[\alpha,\beta]/F$ is algebraic; and the claim follows. ■

Corollary./Def Let E/F be a field extension. The algebraic closure of F in E is $L:=\{a\in E \mid a \text{ is algebriac over } F\}$.

Then L/F is an algebraic field extension.

Pf. $\alpha\in L$, $\beta\in L\setminus\{0\} \Rightarrow$ by the previous corollary $\alpha\pm\beta, \alpha\beta^{\pm 1}\in L$.

So L is a field. $\forall a\in F$, a is a zero of $x-a$. So $F\subseteq L$. ■

In the previous lecture for any given polynomial $f(x)\in F[x]$, we found a field extension over which f can be written as a product of deg. 1 polynomials. Can we find a field

Lecture 23: Algebraically closed fields

Wednesday, February 28, 2018 8:47 AM

over which <u>all</u> the polynomials of $F[x]$ can be written as a product of deg. 1 polynomials?

<u>Def</u>. A field E is called <u>algebraically closed</u> if any poly. $f(x)$ in $E[x]\setminus E$ has a zero.

<u>Lemma.</u> If E is algebraically closed, then any poly. of $\deg \geq 1$ can be written as a product of deg. 1 factors.

<u>Pf</u>. Easy induction!

<u>Theorem</u>. Let F be a field. Then $\exists$ a field extension E/F where E is algebraically closed.

<u>Pf</u>. We start with finding a field extension E_1/F where all the poly. $f(x) \in F[x]\setminus F$ has a zero in E_1. We use a similar idea as the case of finding an extension with a zero of a given irred. polynomial. There we looked at $F[x]/\langle p(x)\rangle$. Now we do the same. We consider the ring A of polynomials $F[x_f]_{\substack{f\in F[x]\setminus F \\ f \text{ monic}}}$.

Consider $I = \langle f(x_f) \mid \underset{f \text{ monic}}{f \in F[x]\setminus F} \rangle$. Show $I \neq A$ and find a maximal

Lecture 23: Towards algebraic closure

Wednesday, February 28, 2018 8:55 AM

ideal $\mathfrak{m}$ of A which contains I. Then $A/\mathfrak{m}$ is a field;

$\forall f \in F[x]\setminus F$ monic $f(\overline{x}_f)=0$, where $\overline{x}_f := x_f + \mathfrak{m} \in A/\mathfrak{m}$.

(We will finish this argument in the next lecture).