Math200b, lecture 18

Golsefidy

Finite fields

In the previous lecture we proved that a finite field F has order p^d for some prime p and positive integer d. And we have $x^{p^d} - x = \prod_{\alpha \in F}(x - \alpha)$. Now we want to prove the existence and uniqueness of a field of order p^d.

Theorem 1 *Suppose p is a prime p and d is a positive integer. Then there is a unique, up to an isomorphism, field of order p^d.*

We denote a field of order p^d by $\mathbb{F}_{p^d}$; in particular we let $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

Proof. Let E be a splitting field of $x^{p^d} - x$ over $\mathbb{F}_p$. And let

$$X := \{\alpha \in E | \, \alpha^{p^d} = \alpha\}.$$

We prove that X is a subfield of E.

$\mathbb{F}_p \subseteq X$. By Fermat's little theorem, $a^p = a$ for any $a \in \mathbb{F}_p$; and so $\mathbb{F}_p \subseteq X$.

Closed under addition. Notice that E is of characteristic p. And so $(x+y)^{p^d} = x^{p^d} + y^{p^d}$ for any $x, y \in E$. Hence

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

Closed under negation. Notice if p is odd, $(-1)^{p^d} = -1$. If $p = 2$, $-1 = 1$ in E. Hence

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

Closed under multiplication.

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

Closed under taking inverse.

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

Since E is generated by zeros of $x^{p^d} - x$ and $\mathbb{F}_p$, by the above results we deduce that $E = X$.

$|E| = p^d$. We have already proved that E consists of zeros of $x^{p^d} - x$; and so $|E| \leq p^d$. It is enough to show that $x^{p^d} - x$ does not have multiple roots in E. If it does, then $x^{p^d} - x = (x-\beta)^2 q(x)$ for some $\beta \in E$ and $q(x) \in E[x]$. Let's take the formal derivative of both sides;

$$(p^d)x^{p^d-1} - 1 = 2(x-\beta)q(x) + (x-\beta)^2 q'(x) \Rightarrow (x-\beta)h(x) = -1,$$

for some $h(x) \in E[x]$, which is a contradiction. This shows the existence of a finite field of order p^d.

On the other hand, if F is a field of order p^d, then its characteristic should be a prime divisor of p^d; and so it is p. This implies that $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a subfield of F. We also know that $x^{p^d} - x = \prod_{\alpha \in F}(x - \alpha)$ in $F[x]$; and so F is a splitting field of $x^{p^d} - x$ over $\mathbb{F}_p$; and so up to an isomorphism is unique. $\blacksquare$

Algebraic extensions.

Lemma 2 (Tower lemma) *Suppose E/F and K/E are finite field extensions. Then K/F is a finite field extension and $[K : F] = [K : E][E : F]$.*

Proof. Suppose $\{e_1, \ldots, e_m\}$ is an F-basis of E and $\{k_1, \ldots, k_n\}$ is an E-basis of K. We show that $\{e_i k_j | 1 \leq i \leq m, 1 \leq j \leq n\}$ is an F-basis of K.

Independence. Suppose $\sum_{i,j} f_{ij} e_i k_j = 0$ for some $f_{ij} \in F$. Then $\sum_i f_{ij} e_i \in E$ and $\sum_j (\sum_i f_{ij} e_i) k_j$. As k_j's are E-linearly independent, we deduce that $\sum_i f_{ij} e_i = 0$ for any j. As e_i's are F-linearly independent, we get that $f_{ij} = 0$ for any i and j.

Span. Since the E-span of k_j's is K, there are c_i's in E, for any $k \in K$ there are c_j's in E such that $k = \sum_j c_j k_j$. Since E is the F-span of e_i's, there are f_{ij}'s in F such that $c_j = \sum_i f_{ij} e_i$. Hence $k = \sum_j (\sum_i f_{ij} e_i) k_j = \sum_{i,j} f_{ij} e_i k_j$; and claim follows. ■

Notice that if $[K : F] < \infty$, then clearly $[K : E] < \infty$ and $[E : F] < \infty$; and so we get:

Lemma 3 *Suppose E/F and K/E are field extensions. Then*

$$E/F \textit{ and } K/E \textit{ are finite} \Leftrightarrow K/F \textit{ is finite.}$$

These are the type of field extension properties that we like the most.

We say E/F is an algebraic extension if any $\alpha \in E$ is algebraic over F.

Lemma 4 *Suppose E/F is a finite field extension. Then E/F is an algebraic field extension.*

Proof. For any $\alpha \in E$, the set $\{1, \alpha, \alpha^2, \ldots\}$ is F-linearly dependent as otherwise $[E : F] = \infty$. Hence there are $f_0, \ldots, f_n \in F$ such that $f_n \neq 0$ and $f_0 + f_1\alpha + \cdots + f_n\alpha^n = 0$. Hence α is a zero of $p(x) := \sum_{i=0}^{n} f_i x^i \in F[x] \setminus F$; and claim follows. ■

Lemma 5 *Suppose* E/F *is a field extension. If* $\alpha, \beta \in E \setminus \{0\}$ *are algebraic over* F*, then* $\alpha \pm \beta, \alpha\beta^{\pm 1}$ *are algebraic over* F*.*

Proof. Since α is algebraic over F, $[F[\alpha] : F] = \deg m_{\alpha,F} < \infty$. Since β is algebraic over F, it is algebraic over $F[\alpha]$; and so $[F[\alpha, \beta] : F[\alpha]] < \infty$. Since $F[\alpha, \beta]/F[\alpha]$ and $F[\alpha]/F$ are finite extensions, $F[\alpha, \beta]/F$ is a finite extension. Therefore it is an algebraic extension, and so $\alpha \pm \beta$ and $\alpha\beta^{\pm 1}$ are algebraic over F. ■

Proposition 6 *Suppose* E/F *is a field extension. Let*

$$K := \{\alpha \in E |\ \alpha \textit{ is algebraic over } F\}.$$

Then K *is a subfield of* E *and* K/F *is an algebraic extension.* K *is called the algebraic closure of* F *in* E*.*

Proof. By the previous Lemma, K is a subfield of E. Notice that for any $a \in F$, a is a zero of $x - a \in F[x]$; and so $F \subseteq K$. ■

Theorem 7 *Suppose* E/F *and* K/E *are algebraic field extensions. Then Then* K/F *is an algebraic field extension.*

Proof. Suppose $\alpha \in K$. Since K/E is algebraic, α is a zero of a polynomial $\sum_{i=0}^{n} e_i x^i \in E[x] \setminus E$. Since E/F is algebraic, e_i's are algebraic over F. Hence $F[e_0]/F$, $F[e_0, e_1]/F[e_0], \ldots$, $F[e_0, \ldots, e_n]/F[e_0, \ldots, e_{n-1}]$ are finite field extensions. Thus $F[e_0, \ldots, e_n]/F$ is a finite field extension. Since α is a zero of $\sum_{i=0}^{n} e_i x^i$, α is algebraic over $F[e_0, \ldots, e_n]$. Therefore

$$F[e_0, \ldots, e_n, \alpha]/F[e_0, \ldots, e_n]$$

is a finite extension. Another application of the tower lemma implies that

$$F[e_0, \ldots, e_n, \alpha]/F$$

is a finite extension; and so α is algebraic over F.

■

Algebraic closure.

For a given polynomial $p(x) \in F[x]$, we have found a field E that contains all the zeros of $p(x)$ (and it is generated by these zeros and F). Can we find a field that contains zeros of all the non-constant polynomials over F?

Definition 8 *A field E is called algebraically closed if any polynomial in $E[x] \setminus E$ has a zero in E.*

Lemma 9 *Suppose E is algebraically closed. Then for any $f(x) \in E[x] \setminus E$ there are α_i's in E such that*

$$f(x) = \alpha_0 \prod_{i=1}^{n} (x - \alpha_i).$$

Proof. We proceed by induction on the degree of f. If f is of degree 1, there is nothing to prove. Suppose $f(x) \in E[x]$ is of degree $n+1$. Since E is algebraically closed, there is $\alpha \in E$ such that $f(\alpha) = 0$. Hence by factor theorem, there is $p(x) \in E[x]$ such that $f(x) = (x - \alpha)p(x)$. In particular, $\deg p = n$; and so by the induction hypothesis it can be written as a product of degree 1 factors; and claim follows. ■

Theorem 10 *Suppose F is a field. Then there is a field extension E/F such that E is algebraically closed.*

Proof. First we will construct a field E_1 such that any non-constant monic polynomial of $F[x]$ has a zero in E_1. This means for any monic polynomial $f \in F[x] \setminus F$, we need to have $\alpha_f \in E_1$ such that $f(\alpha_f) = 0$. This means there should be a ring homomorphism from the ring of polynomials

$$A := F[x_f | \, f \in F[x] \setminus F \text{ is monic}]$$

to E_1 which sends x_f to α_f. And the kernel of this homomorphism contains $f(x_f)$ as $f(\alpha_f) = 0$. This gives us the idea of considering the ideal $\mathfrak{a}$ of A that is generated by $\{f(x_f) | \, f \in F[x] \setminus F \text{ is monic}\}$. If we show $\mathfrak{a}$ is a proper ideal, then there is $\mathfrak{m} \in \mathrm{Max}(A)$ such that $\mathfrak{a} \subseteq \mathfrak{m}$. Then we can set $E_1 := A/\mathfrak{m}$ and $\alpha_f := x_f + \mathfrak{m}$; then E_1 is a field and $f(\alpha_f) = f(x_f) + \mathfrak{m} = 0$ (as $f(x_f) \in \mathfrak{a} \subseteq \mathfrak{m}$).

$\mathfrak{a}$ is proper. Suppose to the contrary that $\mathfrak{a} = A$. Then there are monic polynomials $f_1, \ldots, f_n \in F[x] \setminus F$ and $g_1, \ldots, g_n \in A$ such that

$$g_1 f_1(x_{f_1}) + g_2 f_2(x_{f_2}) + \cdots + g_n f_n(x_{f_n}) = 1.$$

Let $y_1 := x_{f_1}, \ldots, y_n := x_{f_n}$ and $y_{n+1}, \ldots, y_m$ be the rest of variables that appear in g_i's. And so

$$g_1(y_1,\ldots,y_m)f_1(y_1)+\cdots+g_n(y_1,\ldots,y_m)f_n(y_n)=1. \tag{1}$$

Let K be a splitting field of $\prod_{i=1}^n f_i(x)$ over F. So there are $\alpha_i \in K$ such that $f_i(\alpha_i)=0$. Let's evaluate both sides of (1) at $(\alpha_1,\ldots,\alpha_n,0,\ldots,0)$. Then we get $0=1$ which is a contradiction.

Recursively we define a sequence of fields

$$E_0 := F \subseteq E_1 \subseteq E_2 \subseteq \cdots$$

such that any non-constant monic polynomial in $E_i[x]$ has a zero in E_{i+1}. Let $E := \bigcup_{i=1}^\infty E_i$.

E is a field. For any $\alpha,\beta \in E\setminus\{0\}$, there are i,j such that $\alpha \in E_i$ and $\beta \in E_j$. W.L.O.G. we can and will assume that $i \le j$; and so $\alpha,\beta \in E_j$; and so $\alpha\pm\beta, \alpha\beta^{\pm 1} \in E_j$. Therefore $\alpha\pm\beta, \alpha\beta^{\pm 1} \in E$.

E is algebraically closed. Let $p(x) \in E[x]\setminus E$ is a monic polynomial. Since $p(x)$ has only finitely many coefficients, $p(x) \in E_i[x]$ for some i. And so $p(x)$ has a zero in E_{i+1}; thus $p(x)$ has a zero in E, and claim follows. ■

In the next lecture, we show that if E/F is a field extension and E is algebraically closed, then the algebraic closure of F in E is algebraically closed as well. And this is called an algebraic closure of F.