Math200b, lecture 17

Golsefidy

Splitting fields

In the previous lecture we proved (most parts of) the following theorem.

Theorem 1 *Suppose* E/F *is a field extension,* $\alpha \in E$ *is algebraic over* F*. Then*

1. *there is a unique monic polynomial* $m_{\alpha,F}(x) \in F[x]$ *such that*

$$m_{\alpha,F}(x)|p(x) \Leftrightarrow p(\alpha) = 0$$

   for $p(x) \in F[x]$.

2. $m_{\alpha,F}(x)$ *is irreducible in* $F[x]$.

3. *The ring* $F[\alpha]$ *generated by* F *and* α *is a field; and*

$$F[\alpha] \simeq F[x]/\langle m_{\alpha,F}(x)\rangle.$$

4. $F[\alpha] = \{\sum_{i=0}^{d_0-1} a_i\alpha^i | \, a_i \in F\}$ *where* $d_0 = \deg m_{\alpha,F}(x)$ *where* $d_0 := \deg m_{\alpha,F}(x)$*; in particular* $\dim_F F[\alpha] = \deg m_{\alpha,F}(x)$.

5. $\{1, \alpha, \ldots, \alpha^{d_0-1}\}$ *is an* F*-basis of* $F[\alpha]$.

Let's point out that if E/F is a field extension, E can be viewed as a vector space over F; the dimension $\dim_F E$ of E as an F-vector space is denoted by $[E : F]$ and it called the degree of the field extension E/F.

Proof. We formulated the above theorem in terms of the evaluation map $\phi_\alpha : F[x] \to E$; for instance part (1) is equivalent to saying that $\ker \phi_\alpha = \langle m_{\alpha,F}(x)\rangle$. Part (3) can be deduced using the first isomorphism theorem and maximality of $\langle m_{\alpha,F}(x)\rangle$; and so on. Now we address the last part. For any $\beta \in F[\alpha]$, there is a polynomial $f(x) \in F[x]$ such that $\beta = \phi_\alpha(f) = f(\alpha)$ where ϕ_α is the evaluation map at α. By long division there are $q(x), r(x) \in F[x]$ such that $f(x) = q(x)m_{\alpha,F}(x) + r(x)$ and $\deg r < \deg m_{\alpha,F} = d_0$. And so

$$\beta = f(\alpha) = q(\alpha)\underbrace{m_{\alpha,F}(\alpha)}_{0} + r(\alpha) = r(\alpha);$$

hence if $r(x) = \sum_{i=0}^{d_0-1} c_i x^i$, then $\beta = r(\alpha) = \sum_{i=0}^{d_0-1} c_i \alpha^i$ which implies that the F-span of $\{1, \alpha, \cdots, \alpha^{d_0-1}\}$ is $F[\alpha]$.

Next we show that $1, \alpha, \cdots, \alpha^{d_0-1}$ are F-linearly independent. Suppose $\sum_{i=0}^{d_0-1} c_i \alpha^i = 0$; and so α is a zero of $g(x) = \sum_{i=0}^{d_0-1}$. Therefore $m_{\alpha,F}(x)|g(x)$; comparing their degrees we deduce that $g(x) = 0$; and so $c_i = 0$ for any i, and claim follows. ■

We also pointed out the next lemma which gives us a way to find the minimal polynomial of a given algebraic number (using various irreducibility criteria).

Lemma 2 *Suppose E/F is a field extension, and $\alpha \in E$ is a zero of an irreducible polynomial $p(x) \in F[x]$. Then there is $c \in F^{\times}$ such that $m_{\alpha,F}(x) = cp(x)$.*

Next we proved a kind of converse of this lemma:

Lemma 3 *Suppose $p(x) \in F[x]$ is irreducible. Then there is a field extension E/F and $\alpha \in E$ such that (1) α is a zero of $p(x)$; and (2) $E = F[\alpha]$.*

Repeated application of Lemma 3 gives us the following:

Lemma 4 (Existence of a splitting field) *Suppose* $p(x) \in F[x] \setminus F$. *Then there is a field extension* E/F *and* $\alpha_1, \ldots, \alpha_n \in E$ *such that*

1. $p(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$ *for some* $c \in F$.
2. $E = F[\alpha_1, \ldots, \alpha_n]$.

(We say E is a splitting field of $p(x)$ over F.)

Proof. We proceed by induction on the degree of $p(x)$. If $\deg p = 1$, then $p(x) = c(x - \alpha)$ for some $\alpha \in F$; hence $E = F$ and $\alpha_1 = \alpha$ satisfy the claim. Since $F[x]$ is a PID, it is a UFD; and so we can write $p(x)$ as a product of irreducible polynomials $p_i(x)$'s. By Lemma 3, there is a field extension E_1/F and $\alpha_1 \in E_1$ such that

$$p_1(\alpha_1) = 0 \text{ and } E_1 = F_1[\alpha_1]. \tag{1}$$

As $p_1(x)|p(x)$, we have $p(\alpha_1) = 0$; and by the factor theorem we deduce that there is $q(x) \in E_1[x]$ such that $p(x) = (x - \alpha_1)q(x)$. As $\deg q = \deg p - 1$, by the induction hypothesis there is a field extension E/E_1 and $\alpha_2, \ldots, \alpha_n \in E$ such that

$$q(x) = c(x - \alpha_2) \cdots (x - \alpha_n) \text{ and } E = E_1[\alpha_2, \ldots, \alpha_n], \tag{2}$$

for some $c \in E_1$. By (1) and (2) we have $p(x) = (x - \alpha_1)q(x) = c\prod_{i=1}^{n}(x - \alpha_i)$ and $E = F[\alpha_1][\alpha_2, \ldots, \alpha_n] = F[\alpha_1, \ldots, \alpha_n]$. And we notice that c is equal to the leading coefficient of $p(x)$; and so it is in $F^{\times}$. And claim follows. ∎

Next we work towards uniqueness of a splitting field; and similar to the existence part, we add one zero at a time.

Lemma 5 (Towards Uniqueness of a splitting field) *Suppose* F *and* F' *are two fields,* $\theta : F \to F'$ *is a field isomorphism, and* $p(x) \in F[x]$ *is irreducible.*

1. *We can extend* θ *to an isomorphism* $\theta : F[x] \to F'[x]$ *by letting* $\theta(x) = x$*; that means* $\theta(\sum_{i=0}^{\infty} a_i x^i) := \sum_{i=0}^{\infty} \theta(a_i) x^i$. *Then* $\theta(p)$ *is irreducible in* $F'[x]$.

2. *Suppose* E/F *and* E'/F' *are field extensions,* $\alpha \in E$ *is a zero of* $p(x)$ *and* $\alpha' \in E'$ *is a zero of* $\theta(p)$. *Then there is*

$$\widehat{\theta} : F[\alpha] \xrightarrow{\sim} F'[\alpha']$$

such that $\widehat{\theta}(\alpha) = \alpha'$ *and* $\widehat{\theta}|_F = \theta$.

Proof. Part (1) is clear; so we focus on the second part. Since

$p(x)$ and $\theta(p)$ are irreducible by Lemma 2 we have that

$$\langle m_{\alpha,F}(x)\rangle = \langle p(x)\rangle \text{ and } \langle m_{\alpha',F'}(x)\rangle = \langle \theta(p)\rangle. \tag{3}$$

On the other hand, the isomorphism $\theta : F[x] \to F'[x]$ induces an isomorphism $\overline{\theta} : F[x]/\langle p(x)\rangle \to F'[x]/\langle \theta(p)\rangle$,

$$\overline{\theta}(f + \langle p(x)\rangle) := \theta(f) + \langle \theta(p)\rangle. \tag{4}$$

By Theorem 1 and (3), we have that evaluation maps induce the following isomorphisms:

$$F[x]/\langle p(x)\rangle \xrightarrow{\phi} F[\alpha] \text{ and } F'[x]/\langle \theta(p)\rangle \xrightarrow{\phi'} F'[\alpha'].$$

Hence $\widehat{\theta} := \phi' \circ \overline{\theta} \circ \phi^{-1} : F[\alpha] \to F'[\alpha']$ is an isomorphism, and $\widehat{\theta}|_F = \theta$ and $\widehat{\theta}(\alpha) = \alpha'$; and claim follows. The following diagram might illustrate better various steps of the argument.

$$\begin{tikzcd}
F \arrow[r, hook] \arrow[d, "\theta"] & F[x] \arrow[r] \arrow[d, "\theta"] & F[x]/\langle p(x)\rangle \arrow[r, "\phi"] \arrow[d, "\overline{\theta}"] & F[\alpha] \arrow[d, dashed, "\widehat{\theta}"] \\
F' \arrow[r, hook] & F'[x] \arrow[r] & F'[x]/\langle \theta(p)\rangle \arrow[r, "\phi'"] & F'[\alpha']
\end{tikzcd}$$

■

Theorem 6 (A bit more than uniqueness of a splitting field) *Suppose* F *and* F' *are two fields,* $\theta : F \longrightarrow F'$ *is a field isomorphism and* $p(x) \in F[x] \setminus F$. *Suppose* E *is a splitting of* $p(x)$ *over* F *and* E' *is a splitting of* $\theta(p)$ *over* F'. *Then there is* $\widehat{\theta} : E \xrightarrow{\sim} E'$ *such that* $\widehat{\theta}|_F = \theta$.

Proof. First we notice that if all the irreducible factors of $p(x)$ in $F[x]$ have degree 1, then there are α_i's and c in F such that $p(x) = c\prod_{i=1}^n(x - \alpha_i)$; and so $E = F$ and $\theta(p) = \theta(c)\prod_{i=1}^n(x - \theta(\alpha_i))$ which implies $E' = F'$. Therefore we $\widehat{\theta} = \theta$ satisfies the claim.

Now similar to the proof of existence, we proceed by induction on the degree of $p(x)$. Base of induction follows from the above discussion. To show the induction step, we write $p(x)$ as a product of irreducible polynomials $p_i(x)$'s in $F[x]$. By definition of a splitting field, we have that there are α_i's in E and α_i''s in E' such that

$$E = F[\alpha_1, \ldots, \alpha_n],\ p(x) = c\prod_{i=1}^n(x - \alpha_i),\ \text{and}$$

$$E' = F'[\alpha_1', \ldots, \alpha_n'],\ \theta(p) = \theta(c)\prod_{i=1}^n(x - \alpha_i') \tag{5}$$

Since $p_1(x)|p(x)$, without loss of generality we can and will assume that α_1 is a zero of $p_1(x)$; and similarly, as $\theta(p_1)|\theta(p)$, we can and will assume that α'_1 is a zero of $\theta(p_1)$. By the previous lemma, there is an isomorphism $\theta_1 : F[\alpha_1] \to F'[\alpha'_1]$ such that $\theta_1(\alpha_1) = \alpha'_1$ and $\theta_1|_F = \theta$. As α_1 is a zero of p, there is $q(x) \in F[\alpha_1][x]$ such that $p(x) = q(x)(x - \alpha_1)$. Applying θ_1 to both sides, we get that

$$\theta(p) = \theta_1(p) = \theta_1(q)(x - \theta_1(\alpha_1)) = \theta_1(q)(x - \alpha'_1).$$

Claim. E *is a splitting field of* $q(x)$ *over* $F[\alpha_1]$; *and* E' *is a splitting field of* $\theta_1(q)$ *over* $F'[\alpha'_1]$.

Proof of Claim. As $p(x) = c\prod_{i=1}^{n}(x - \alpha_i)$ and $p(x) = (x - \alpha_1)q(x)$, we deduce that $q(x) = c\prod_{i=2}^{n}(x - \alpha_i)$; similarly, as $\theta(p) = \theta(c)\prod_{i=1}^{n}(x - \alpha'_i)$ and $\theta(p) = (x - \alpha'_1)\theta_1(q)$, we have $\theta_1(q) = \theta(c)\prod_{i=2}^{n}(x - \alpha'_i)$. Since

$$E = F[\alpha_1, \ldots, \alpha_n] = (F[\alpha_1])[\alpha_2, \ldots, \alpha_n], \text{ and}$$

$$E' = F'[\alpha'_1, \ldots, \alpha'_n] = (F'[\alpha'_1])[\alpha'_2, \ldots, \alpha'_n]$$

claim follows. $\square$

As $\deg q = \deg p - 1$, by the above Claim we can use the induction hypothesis for $\theta_1 : F[\alpha_1] \to F'[\alpha'_1]$, $q(x)$, and E and

E'. Hence there is an isomorphisms $\widehat{\theta} : E \to E'$ such that $\widehat{\theta}|_{F[\alpha_1]} = \theta_1$. And this implies $\widehat{\theta}|_F = \theta_1|_F = \theta$ which finishes the proof. ■

By Lemma 4 (Existence of a splitting field) and Theorem 6 (Uniqueness of a splitting field), we get the following theorem.

Theorem 7 (Splitting field) *Suppose* $p(x) \in F[x] \setminus F$*. Then* $p(x)$ *has a splitting field* E *over* F*; and if* E *and* E' *are two splitting fields of* $p(x)$ *over* F*, then there is* $\phi : E \xrightarrow{\sim} E'$ *such that* $\phi|_F = \mathrm{id}$.

Finite fields

We will use the existence and uniqueness of splitting fields to show that for any prime power $q = p^n$ there is a unique field of order q. We start with investigating a finite field F. Since F is finite, it has a positive characteristic; and as it is an integral domain, its characteristic should be a prime number p. Hence F is a field extension of $\mathbb{Z}/p\mathbb{Z}$. Suppose $[F : \mathbb{Z}/p\mathbb{Z}] = d$; then $|F| = |(\mathbb{Z}/p\mathbb{Z})^d| = p^d$. And so for any $\alpha \in F^\times$, $\alpha^{|F^\times|} = 1$, which implies for any $\alpha \in F \setminus \{0\}$, $\alpha^{p^d - 1} = 1$. Thus any $\alpha \in F$ is a zero of $x^{p^d} - x$. Therefore by the generalized factor theorem there is $q(x) \in F[x]$ such that

$$x^{p^d} - x = q(x) \prod_{\alpha \in F} (x - \alpha).$$

Comparing the degrees of both sides, we deduce that $\deg q = 0$; and so $q(x) = c \in F^{\times}$. Next comparing the leading coefficients of both sides, we deduce that $c = 1$; and altogether we get:

Theorem 8 *Suppose* F *is a finite field. Then there is a prime* p *and positive integer* d *such that* $|F| = p^d$. *And*

$$x^{p^q} - x = \prod_{\alpha \in F} (x - \alpha)$$

in $F[x]$.