

Lecture 26: Existence and uniqueness of splitting fields

Wednesday, June 6, 2018 11:00 AM

Theorem. Suppose F is a field, and $f(x) \in F[x]$ has positive degree.

Then $f(x)$ has a splitting field over F ; that means

(1) \exists a field E and $i: F \hookrightarrow E$, an injective ring hom.

(2) $\exists c, \alpha_1, \dots, \alpha_d \in E$ s.t. $i(f(x)) = c(x - \alpha_1) \dots (x - \alpha_d)$

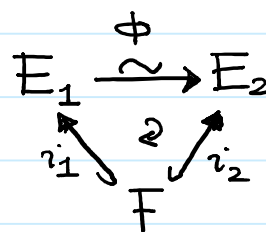
(3) The smallest subfield of E that contains $i(F)$ and $\alpha_1, \dots, \alpha_d$ is E .

Moreover, if E_1 and E_2 are two splitting fields of $f(x)$ over

F with the corresponding injective ring hom. $i_1: F \hookrightarrow E_1$ and

$i_2: F \hookrightarrow E_2$, then $\exists E_1 \xrightarrow{\phi} E_2$ s.t.

$\phi(i_1(a)) = i_2(a)$ for any $a \in F$.



Pf. (Cont.) We were in the middle of proof of existence part.

We were using induction on $\deg f$. We discussed the base of induct.

To prove the induction step, we used the fact that $F[x]$ is a UFD

and wrote $f(x)$ as a product of irreducible factors. Assumed $p(x)$

Lecture 26: Existence of splitting fields

Wednesday, June 6, 2018 11:17 AM

By a theorem that we had proved earlier, we have

- \exists a field \overline{F} and $\overline{i}: F \hookrightarrow \overline{F}$
- $\exists \alpha \in \overline{F}$ s.t. $\overline{i}(f(\alpha)) = 0 \implies \overline{i}(f(x)) = 0$
- A subfield of \overline{F} that contains $\overline{i}(F)$ and α is \overline{F} .

$\overline{i}(f(\alpha)) = 0$ implies $\overline{i}(f(x)) = (x - \alpha) \overline{f}(x)$ for some

$\overline{f}(x) \in \overline{F}[x]$. And $\deg \overline{f} = \deg f - 1$. Hence by the induction

hypothesis,

- \exists a field E and $\hat{i}: \overline{F} \hookrightarrow E$
- $\exists c, \alpha_1, \dots, \alpha_{n-1} \in E$ s.t. $\hat{i}(f(x)) = c(x - \alpha_1) \cdots (x - \alpha_{n-1})$
- A subfield of E that contains $\hat{i}(\overline{F})$ and $\alpha_1, \dots, \alpha_{n-1}$ is E

Hence $\cdot \quad \begin{array}{ccc} F & \xrightarrow{\overline{i}} & \overline{F} \xrightarrow{\hat{i}} E \\ & \searrow \overline{i} & \nearrow \hat{i} \\ & & \end{array}$

$$\begin{aligned} \cdot \quad i(f(x)) &= \hat{i}(\overline{i}(f(x))) = \hat{i}(\overline{f}(x)(x - \alpha)) \\ &= \hat{i}(\overline{f}(x))(x - \hat{i}(\alpha)) \\ &= c(x - \alpha_1) \cdots (x - \alpha_{n-1})(x - \hat{i}(\alpha)) \end{aligned}$$

- A subfield of E that contains $i(F)$ and $\alpha_1, \dots, \alpha_{n-1}, \hat{i}(\alpha)$, contains $\hat{i}(\overline{i}(F)), \hat{i}(\alpha)$, and $\alpha_1, \dots, \alpha_{n-1}$; Hence it contains

Lecture 26: Existence and uniqueness of splitting fields

Wednesday, June 6, 2018 11:42 AM

$\hat{i}(\overline{F})$ and $\alpha_1, \dots, \alpha_{n-1}$; and so it is E_j and claim follows.

Uniqueness. To show uniqueness one needs to show slightly stronger

result by induction on $\deg f$: Suppose $F_1 \xrightarrow{\theta} F_2$ is an isomorphism

of fields, $f(x) \in F_1[x]$ is of positive \deg . $i_1: F_1 \hookrightarrow E_1$ is a

splitting field of $f(x)$ over F_1 , and $i_2: F_2 \hookrightarrow E_2$ is a splitting

field of $\theta(f)$ over F_2 , then $\exists E_1 \xrightarrow{\phi} E_2$ s.t.

$$\begin{array}{ccc} E_1 & \xrightarrow{\sim} & E_2 \\ i_1 \uparrow & \phi & \uparrow i_2 \\ F_1 & \xrightarrow{\sim} & F_2 \end{array} \quad \phi(i_1(a)) = i_2(\theta(a)).$$

Again for $\deg f = 1$, we can see that i_1 and i_2 are

isomorphism. For the induction step, $i_1(f(x)) = c^{(1)}(x - \alpha_1^{(1)}) \dots (x - \alpha_n^{(1)})$

for $\alpha_1^{(1)}, \dots, \alpha_n^{(1)}, c^{(1)} \in E_1$ and $i_2(\theta(f(x))) = c^{(2)}(x - \alpha_1^{(2)}) \dots (x - \alpha_n^{(2)})$

for $\alpha_1^{(2)}, \dots, \alpha_n^{(2)}, c^{(2)} \in E_2$. Suppose $p(x)$ is an irreducible factor

of $f(x)$. So one of $\alpha_j^{(1)}$'s is a zero of $i_1(p)$ and one of

$\alpha_j^{(2)}$'s is a zero of $i_2(\theta(p))$. W.L.O.G we can assume $\alpha_1^{(1)}$ and

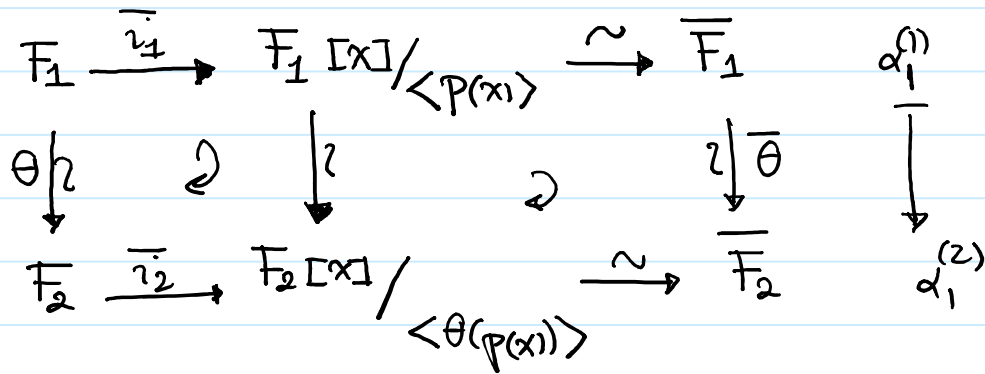
$\alpha_1^{(2)}$ are zeros of $i_1(p)$ and $i_2(\theta(p))$, respectively.

Lecture 26: Uniqueness of a splitting field

Thursday, June 7, 2018 9:57 PM

Let \overline{F}_i be the smallest subfield of E_i that contains F_i and $\alpha_1^{(i)}$. Then by a theorem that we proved about irreducible

polynomials $h(x) + \langle p(x) \rangle \mapsto i_1(h(\alpha_1^{(1)}))$ and



$$h(x) + \langle \theta(p(x)) \rangle \xrightarrow{\sim} i_2(h(\alpha_1^{(2)}))$$

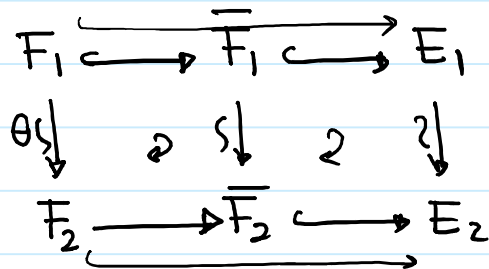
$$f(x) = (x - \alpha_1^{(1)}) \overline{f}(x) \text{ and } \theta(f(x)) = (x - \alpha_1^{(2)}) \overline{\theta}(\overline{f}(x))$$

One can show E_1 is the splitting field of \overline{f} over \overline{F}_1

and E_2 is the splitting field of $\overline{\theta}(\overline{f})$ over \overline{F}_2 and

use the induction hypothesis to finish proof using the

following diagram



A very brief outline of uniqueness was mentioned during lecture

Lecture 26: Finite fields

Thursday, June 7, 2018 10:08 PM

We have seen that if $f(x) \in \mathbb{Z}_p[x]$ is an irreducible poly. of deg d , then $\mathbb{Z}_p[x]/\langle f(x) \rangle$ is a field of order p^d . Next we show for any prime p and any $d \in \mathbb{Z}^+$, there is a finite field of order p^d . We have already showed that if there is a finite field E of order p^d , then

$$x^{p^d} - x = \prod_{\alpha \in E} (x - \alpha) \text{ in } E[x].$$

This means all the zeros of $x^{p^d} - x$ are in E and all the elements of E are zeros of $x^{p^d} - x$. This would be our guideline.

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

Pf. Let E be a splitting field of $x^{p^d} - x$ over \mathbb{Z}_p . Let

$$X := \{ \alpha \in E \mid \alpha^{p^d} - \alpha = 0 \}.$$

Claim 1. X is a subring of E

Pf of claim 1. Closed under addition. Since \mathbb{Z}_p is a subring of E , $\text{char } E = p > 0$. Hence for any $x, y \in E$, $(x+y)^p = x^p + y^p$ using

Lecture 26: Finite fields

Friday, June 8, 2018 1:07 AM

binomial expansion. Hence as we have seen earlier in the course

$$(x+y)^{p^d} = x^{p^d} + y^{p^d} \quad (\text{using induction on } d)$$

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

Closed under multiplication

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

Closed under negation

$$\alpha \in X \Rightarrow -\alpha = (p-1)\alpha \in X$$

char $E = p > 0$

Closed under addition

Claim 2. X is a finite field and $|X| \leq p^d$.

Pf of claim 2. A polynomial of degree n has at most n zeros

in a field. Hence $x^{p^d} - x$ has at most p^d zeros in E ; and

so $|X| \leq p^d$. Since X is a subring of a field E and $1 \in X$,

X is an integral domain. A finite integral domain is a field.

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

Claim 3. $X = E$. Pf. Since E is a splitting field of $x^{p^d} - x$ over

Lecture 26: Finite fields

Friday, June 8, 2018 1:19 AM

\mathbb{Z}_p and X is a subfield of E which contains \mathbb{Z}_p and all the zeros of $x^{p^d} - x$, claim 3 follows.

To see $|E| = p^d$, we need to show $x^{p^d} - x$ has distinct zeros.

To this end we borrow an idea from calculus: a poly. $p(x)$ has a zero with multipli. ≥ 2 at $\alpha \iff p(\alpha) = p'(\alpha) = 0$.

But we cannot use limits in order to define derivative. For poly. we formally define its derivative:

Def. For $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in F[x]$, let

$$f'(x) := n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + a_1.$$

Check that product rule holds: $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.

Lemma. If $f(x) = (x-\alpha)^2 g(x)$, then $f(\alpha) = f'(\alpha) = 0$.

Pf. $f(\alpha) = (\alpha - \alpha)^2 g(\alpha) = 0$

$$f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x) \implies f'(\alpha) = 2(\alpha-\alpha)g(\alpha) + (\alpha-\alpha)^2 g'(\alpha) = 0. \quad \square$$

To see all the zeros of $f(x) = x^{p^d} - x$ are distinct, it is enough to

notice $f'(x) = p^d x^{p^d-1} - 1 = -1$ has no zeros. (Char $E = p$)