Lecture 19: Splitting fields

Sunday, March 17, 2019 8:33 PM

In a couple of lectures ago we proved that, if $p(x)\in F[x]$ is irreducible, then there are a field E, $\alpha\in E$, and an embedding $i: F \hookrightarrow E$ s.t. $i(p)(\alpha)$. Now that we know $F[x]$ is a UFD we can prove this result for an arbitrary non-constant polynomial, and by a repeated use of this find a field that contains all the zeros of $p(x)$.

<u>Theorem</u>. Suppose F is a field and $f(x)\in F[x]\setminus F$. Then there are a field E, $\alpha_1,\ldots,\alpha_n\in E$, and an embedding $i: F\hookrightarrow E$ s.t.

(a) $E = F[\alpha_1,\ldots,\alpha_n] = \{\sum a_{i_1,\ldots,i_n}\alpha_1^{i_1}\alpha_2^{i_2}\cdots\alpha_n^{i_n} \mid a_{i_1,\ldots,i_n}\in F\}$

(evaluating n variable poly. at $(\alpha_1,\ldots,\alpha_n)$.)

(we said "we are adding α_i's to F.")

(b) $i(p) = c\,(x-\alpha_1)\cdots(x-\alpha_n)$ for some $c\in i(F)$.

(Such a field E is called a <u>splitting field</u> of $p(x)$.)

Lecture 19: Splitting field

Sunday, March 17, 2019 8:49 PM

<u>Pf.</u> We proceed by induction on $\deg(f)$.

<u>Base.</u> If $\deg(f)=1$, then $f(x)=a_1x+a_0$ and $a_1\in F^{\times}$.

Hence $f(x)=a_1(x+\frac{a_0}{a_1})$, $\frac{a_0}{a_1}\in F$; and so F is a splitting field of $f(x)$ over F.

<u>Induction Step.</u> $F[x]$ is a UFD. So $f(x)=\prod_{i=1}^{m} p_i(x)$ where $p_i(x)$ is irreducible in $F[x]$. Hence $\exists\ F \overset{\bar{i}}{\hookrightarrow} \overline{F}$ and $\alpha\in\overline{F}$ s.t. $\bar{i}(p_1)(\alpha)=0$, (Hence $\bar{i}(f)(\alpha)=0$) and $\overline{F}$ is the smallest ring that contains α and $\bar{i}(F)$. Therefore by the factor theorem, $\exists\ \bar{f}(x)\in\overline{F}[x]$ s.t. $\deg\bar{f}=\deg f-1$ and $f(x)=(x-\alpha)\bar{f}(x)$. Now by the induction hypothesis, $\bar{f}$ has a splitting field over $\overline{F}$; that means

- $\exists$ a field E and $\hat{i}:\overline{F}\hookrightarrow E$ injective ring hom.
- $\exists\ \alpha_1,\ldots,\alpha_{n-1}\in E$, $\hat{i}(\bar{f})(x)=c(x-\alpha_1)\cdots(x-\alpha_{n-1})$ for some $c\in\overline{F}\setminus\{0\}$
- The smallest subfield of E that contains $\hat{i}(\overline{F})$ and $\alpha_1,\ldots,\alpha_{n-1}$ is E.

Lecture 19: Splitting field

Sunday, March 17, 2019 8:53 PM

<u>Consider</u>.

$$\begin{tikzcd} F \arrow[r, hook, "\bar{i}"] \arrow[rr, hook, bend right, "i"'] & \bar{F} \arrow[r, hook, "\hat{i}"] & E \end{tikzcd}$$

- $$i(f)(x) = \hat{i}(\bar{i}(f))(x)$$
$$= \hat{i}\left((x-\alpha)\,\bar{f}(x)\right)$$
$$= (x - \hat{i}(\alpha))\,\hat{i}(\bar{f})(x)$$
$$= c\,(x - \underbrace{\hat{i}(\alpha)}_{\alpha_n})(x-\alpha_1)\cdots(x-\alpha_{n-1}).$$

- A subfield of E that contains $i(F)$ and $\alpha_1, \ldots, \alpha_n$ contains $\hat{i}(\bar{i}(F))$ and $\hat{i}(\alpha)$;

  And so it contains $\hat{i}(\underbrace{\bar{i}(F)[\alpha]}_{\bar{F}})$ and $\alpha_1, \ldots, \alpha_{n-1}$.

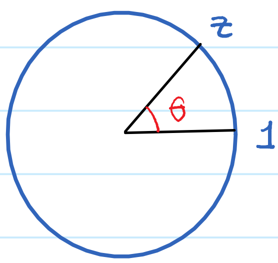
  Hence it should be E. ; and claim follows. ■

Let's see a couple of examples.

$\boxed{P}$ Describe a splitting field $E \subseteq \mathbb{C}$ of $x^n - 1$ over $\mathbb{Q}$.

[Recall from complex numbers:

if $z \in \mathbb{C}$ and $z^n = 1$, then $|z|^n = 1$ implies $|z| = 1$. And so z is on the unit circle. If the argument of z is θ, then multip. by z is



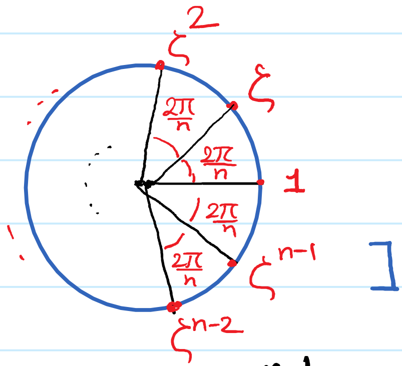
Lecture 19: Examples of splitting fields

Sunday, March 17, 2019 8:56 PM

just rotation by angle θ about the origin. We also have $e^{i\theta} = \cos\theta + i\sin\theta$. So $z^n = 1$ and $z = e^{i\theta}$ imply $e^{in\theta} = \cos n\theta + i \sin n\theta = 1$; and so $n\theta = 2k\pi$ for some $k \in \mathbb{Z}$. Hence $\theta = \frac{2k\pi}{n}$ for some $k \in \mathbb{Z}$.

Hence we get n possible values $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ where

$$\zeta = e^{\frac{2\pi i}{n}} = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right).$$



And so $y^n - 1 = (y-1)(y-\zeta) \cdots (y-\zeta^{n-1})$.

By the above discussion, $x^n - 1 = (x-1)(x-\zeta)\cdots(x-\zeta^{n-1})$ where $\zeta = e^{\frac{2\pi i}{n}}$. Hence $E = \mathbb{Q}[1, \zeta, \ldots, \zeta^{n-1}] = \mathbb{Q}[\zeta]$ is a splitting field of $x^n - 1$ over $\mathbb{Q}$.

($\mathbb{Q}[\zeta]$ contains all the zeros of $x^n - 1$; and zeros of $x^n - 1$ together with $\mathbb{Q}$ give us $\mathbb{Q}[\zeta]$.)

$\boxed{P}$ Describe a splitting field $E \subseteq \mathbb{C}$ of $x^5 - 2$ over $\mathbb{Q}$.

__Solution.__ $x^5 - 2 = 2\left(\left(x/\sqrt[5]{2}\right)^5 - 1\right)$

Lecture 19: Examples of splitting fields

Sunday, March 17, 2019 9:21 PM

$$= 2\left(\left(\tfrac{x}{\sqrt[5]{2}}\right)-1\right)\left(\left(\tfrac{x}{\sqrt[5]{2}}\right)-\zeta\right)\left(\left(\tfrac{x}{\sqrt[5]{2}}\right)-\zeta^2\right)\left(\left(\tfrac{x}{\sqrt[5]{2}}\right)-\zeta^3\right)\left(\left(\tfrac{x}{\sqrt[5]{2}}\right)-\zeta^4\right)$$

$$= 2\cdot\left(\frac{1}{\sqrt[5]{2}}\right)^5(x-\sqrt[5]{2})(x-\sqrt[5]{2}\zeta)(x-\sqrt[5]{2}\zeta^2)(x-\sqrt[5]{2}\zeta^3)(x-\sqrt[5]{2}\zeta^4)$$

$$=(x-\sqrt[5]{2})(x-\sqrt[5]{2}\zeta)(x-\sqrt[5]{2}\zeta^2)(x-\sqrt[5]{2}\zeta^3)(x-\sqrt[5]{2}\zeta^4)$$

So a splitting field $E\subseteq\mathbb{C}$ of x^5-2 over $\mathbb{Q}$ should contain $\sqrt[5]{2}$ and $\sqrt[5]{2}\,\zeta$. Hence

$$\zeta=(\sqrt[5]{2}\,\zeta)(\sqrt[5]{2})^{-1}\in E.$$ This implies $\mathbb{Q}[\sqrt[5]{2},\zeta]\subseteq E$. Conversely $\sqrt[5]{2}\,\zeta^i$ are in $\mathbb{Q}[\sqrt[5]{2},\zeta]$. So all the zeros of x^5-2 are in $\mathbb{Q}[\sqrt[5]{2},\zeta]$. Therefore $E=\mathbb{Q}[\sqrt[5]{2},\zeta]$ is a splitting field of x^5-2 over $\mathbb{Q}$. ∎

We will use the existence of splitting fields to show existence of finite fields of order p^d where p is prime and $d\in\mathbb{Z}^+$.

Suppose F is a finite field. Then its characteristic

Lecture 19: Finite fields

Sunday, March 17, 2019 9:36 PM

is not zero (as it is finite), and it is either 0 or a prime p (as it is an integral domain). Hence its characteristic is a prime $p > 0$. Therefore

$i: \mathbb{Z}_p \hookrightarrow F$, $i(n) := n 1_F$ is a well-define embedding (injective ring homomorphism). So we can view F as a $\mathbb{Z}_p$-vector space. Since $|F| < \infty$, $\dim_{\mathbb{Z}_p} F = d < \infty$. So F has a $\mathbb{Z}_p$-basis $\{\alpha_1, \ldots, \alpha_d\}$.

Thus any element of F can be written as a $\mathbb{Z}_p$-linear combination of α_i's in a unique way: An element of F is of the form $c_1 \alpha_1 + \cdots + c_d \alpha_d$ for some unique choices of c_i's in $\mathbb{Z}_p$. Hence

$$|F| = (\# \text{ of choices of } c_1) \cdot \cdots \cdot (\# \text{ of choices of } c_d).$$

$$= \underbrace{p \cdot \cdots \cdot p}_{d \text{ times}} = p^d.$$

So number of elements of a finite field is p^d for some

Lecture 19: Finite fields

Sunday, March 17, 2019 9:46 PM

prime p and $d \in \mathbb{Z}^+$.

Suppose F is a finite field of order p^d. Then $(F^\times, \cdot)$ is a group of order $p^d - 1$. Hence $\forall \alpha \in F^\times$ we have

$\alpha^{p^d - 1} = 1 \Rightarrow \alpha^{p^d} = \alpha$. This equality also holds for $\alpha = 0$.

$\Rightarrow \forall \alpha \in F$, α is a zero of $x^{p^d} - x$.

Thus by the generalized factor theorem $\exists\, h(x) \in F[x]$

s

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

Comparing degrees

$$\Rightarrow \quad p^d = \deg h + \sum_{\alpha \in F} 1 = \deg h + |F|$$
$$= \deg h + p^d$$

$\Rightarrow \deg h = 0 \Rightarrow h(x) = c \in F^\times$.

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

Comparing leading coeff. $\Rightarrow c = 1$.

<u>Theorem</u>. Suppose F is a field of order p^d. Then

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