LECTURE 8

Author
Tom Jeong

February 3, 2025

Contents

1 L-spliting field

L-splitting field of $x^4 - 2x^2 - 10$ over $\mathbb{Q}$ $[L : \mathbb{Q}] =?$
$\alpha_1, \alpha_2, \alpha_3, \alpha_4$ - roots of f(x)

$$L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \mathbb{Q}[\alpha_1][\alpha_2][\alpha_3][\alpha_4]$$

THe tower theorem shows that

$$\begin{array}{c} L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \\ \Big\downarrow \\ \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) \\ \Big\downarrow \\ \mathbb{Q}(\alpha_1, \alpha_2) \\ \Big\downarrow \\ \mathbb{Q}(\alpha_1) \cong \mathbb{Q}[x]/\langle f(x) \rangle \\ \Big\downarrow \\ \mathbb{Q} \end{array}$$

$[L : \mathbb{Q}] \leq n!$ where $n = \partial f$ in this case. Thus $[L : \mathbb{Q}] \mid n!$

$$4 < [L : \mathbb{Q}] \leq 4! = 24$$
$$4 \mid [L : \mathbb{Q}] \mid 24$$
$$u = x^2$$
$$u^2 - 2u - 10 = 0$$
$$u = \frac{2 \pm \sqrt{4 + 40}}{2} = 1 \pm \sqrt{11}$$
$$\alpha_1 = \sqrt{1 + \sqrt{11}}$$
$$\alpha_2 = -\sqrt{1 + \sqrt{11}}$$
$$\alpha_3 = \sqrt{1 - \sqrt{11}}$$
$$\alpha_4 = -\sqrt{1 - \sqrt{11}}$$

$L = \mathbb{Q}(\alpha_1, \alpha_2)$

$$\alpha_1^2 = 1 + \sqrt{11}$$
$$\alpha_2^2 = 1 + \sqrt{11}$$
$$-\alpha_1^2 = -1 - \sqrt{11}$$
$$2 - \alpha_1^2 = 1 - \sqrt{11}$$
$$\alpha_2^2 = 2 - \alpha_1^2$$
$$\alpha_2 \text{ is a root of g}$$
$$x^2 - (2 - \alpha_1^2) \in \mathbb{Q}(\alpha_1)$$
$$\mathbb{Q}(\alpha_1) \subseteq \mathbb{R}$$
$$\alpha_2 \notin \mathbb{R} \quad \alpha_2 \notin \mathbb{Q}(\alpha_1)$$

2

$K \cong K'$ $\qquad \phi : K \to K'$ is isomorphism
$f(x) \in K[x]$ the isomorphism extends to isomorphism: $\bar{\phi} : K[x] \to K'[x]$
map the coefficients by ϕ
$f'(x) \in K'[x]$
L-splitting field of $f(x)$ and L' splitttting field of $f'(x)$

Theorem 2.1. $L \cong L'$

Proof. induction onf $m = \partial f$
base case $m = 1$ and $\partial f = 1$
$L = K \quad L' = K' \quad L \cong L'$
Inductive step:

$$m \to m + 1 \tag{1}$$
$$\partial f = m + 1 \tag{2}$$
$$f(x) = q_1, \ldots, q_s \tag{3}$$
$$q_i - \text{irreducible} \tag{4}$$
$$f' = q'_1, \ldots, q'_s \tag{5}$$
$$K_1 = K(x)/\langle q_1(x) \rangle \cong K'_1 = K'(x)/\langle q'_1(x) \rangle \tag{6}$$
$$\tag{7}$$

$$\begin{array}{ccc} L & & L' \\ \downarrow & & \downarrow \\ K_1 & \cong & K'_1 \\ \downarrow & & \downarrow \\ K & \cong & K' \end{array}$$

L is the splitting field of $f(x)$ over $K_1(x)$ and L' is the splitting field of $f'(x)$ over $K'_1(x)$
L is a splitting field of $\frac{f(x)}{x-\alpha_1}$ over K_1 where α_1 is a root of q_1
By inductive hypothesis, since $\partial(\frac{f(x)}{x-\alpha_1}) = m$, the splitting fields L and L' are isomorphic.
Thus, $L \cong L'$ for polynomials of degree $m + 1$, completing the inductive step. □

3 Finite fields with prime subfield

$\mathbb{F}$ is a finite field. Char $F = p$ p is prime.
$\mathbb{Z}_p \subseteq \mathbb{F} \quad \mathbb{Z}_p$ is prime subfield.

1. $|\mathbb{F}| = p^n$ for some n
   $\mathbb{F}/\mathbb{Z}_p$ is a field extension
   $[\mathbb{F} : \mathbb{Z}_P] = n$ (finite) then F ahs a basis over $\mathbb{Z}_p$

   Then any $w \in \mathbb{F}$ has a unique expression

$$w = \sum_{i=1}^{n} \alpha_i v_i \quad \alpha_i \in \mathbb{Z}_p$$

p choices, n times. so number of choises $= p^n = |\mathbb{F}|$

2. $\mathbb{F}$ is the splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$
   $|\mathbb{F}^*| = p^n - 1 \to x \in \mathbb{F}, x \neq 0 \quad x^{p^n - 1} - 1 = 0$
   $\to$ every element of $\mathbb{F}$ is n root of $x^{p^n} - x$
   $\partial(x^{p^n} - x) = p^n$
   $x^{p^n} - x$ has at most p^n distinct roots in $\mathbb{F}$
   $\to x^{p^n} - x$ splits into distinct linear factor over $\mathbb{F}$
   and doesn't split over any subfield
   $\to \mathbb{F}$ is the splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$

3. The splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$ has size p^n

$\mathbb{F}$finite field then$\mathbb{F} = p^n$ and there is at most 1 field of size p^n that has to be splitting filed of $x^{p^n} - x$ over $\mathbb{Z}_p$

now we would like to show that there is exactly one field of size p^n that is the splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$
(property 3)
lemma for property 3.

Lemma 3.1. $f \in K(x)$ has a multiple root r iff r is a root of $f(x)$ and $f'(x)$