Existence and Uniqueness of Splitting Fields, Extension Lemma

Jiang-Hua Lu

The University of Hong Kong

MATH4302 Algebra II, HKU

Monday April 7, 2025

Outline

In this file

1. §3.2.3: Existence of splitting fields;
2. §3.2.4: Uniqueness of splitting fields.

Recall: let K be a field and let $f \in K[x]$ with $n = \deg(f) \geq 1$.

Definition. A splitting field of f over K a field extension L of K such that

1. f splits completely in L, i.e., $\exists \alpha_1, \ldots, \alpha_n \in L$ such that

$$f(x) = a_n(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n);$$

2. $L = K(\alpha_1, \alpha_2, \cdots, \alpha_n)$.

An example: $\mathbb{Q}(\sqrt[3]{2})$ is NOT a splitting field of $f = x^3 - 2$ over $\mathbb{Q}$.

Suppose $f(x) \in K[x]$ has a repeated root α in some extension L of K. Then

$$f(x) = a_0(x-\alpha)^2 g(x) \in L[x]$$

$$\Rightarrow \quad f'(\alpha) = f(\alpha) = 0$$

$\Rightarrow$ $f(x) \in K[x]$ and $f'(x) \in K[x]$ are not co-prime in $K[x]$

($\Rightarrow$ $a(x)f(x) + b(x)f'(x) = 1$ for some $K[x]$)

Conclusion: If $f(x) \in K[x]$ & $f'(x) \in K[x]$ are co-prime in $K[x]$, then f has no repeated roots in any extension of K.

Theorem to be proved in this file:

Theorem

For any field K and any $f \in K[x]$ with positive degree,

1. *splitting fields of f over K exist;*
2. *splitting fields of f over K are "unique".* needs explanation

Observations.

- If $K \subset L$, f splits completely in L, and $\{\alpha_1, \ldots, \alpha_n\}$ are the roots of f in L, then
$$K(\alpha_1, \alpha_2, \ldots, \alpha_n)$$
is a splitting field of f over K.

- Enough to find extension $K \subset L$ such that f splits completely over L.

Recall facts:

- Any irreducible $p(x) \in K[x]$ has a root in $K[x]/\langle p(x) \rangle$.
- Consequently, any non-constant $f \in K[x]$ has a root in some extension L of K.

Theorem

For any field K, every non-constant $f \in K[x]$ has a splitting field over K.

Proof. Induction on $n = \deg(f)$. Assume that f in monic.

- $n = 1$: nothing to prove: K is a splitting field of f over K.
- $n > 1$: let $L_1 \supset K$ be such that f has a root α_1 in L_1. Write

$$f(x) = (x - \alpha_1) f_1(x) \in L_1[x],$$

  where $f_1(x) \in L_1[x]$ (in fact $f(x) \in K(\alpha_1)[x]$ and $[L_1 : K] \leq n$).
- By induction assumption, $\exists L \supset L_1$ and $\alpha_2, \ldots, \alpha_n \in L$ such that

$$f_1 = (x - \alpha_2) \cdots (x - \alpha_n) \in L[x].$$

- $L_f = K(\alpha_1, \ldots, \alpha_n)$ is a splitting field of f over K.

Remark. Can show that $[L_f : K] \leq n!$ in above proof.

For uniqueness, assume $f(x) \in K[x]$, and
$K \subset L$ is a splitting field of f over K.

Assume $\varphi: K \to M$, $\varphi \neq 0$, a ring homo, M is field

Let $\tilde{K} = \varphi(K) \subset M$. For any $f(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$

Let $\tilde{f}(x) = \sum_{i=0}^{n} \varphi(a_i) x^i \in \tilde{K}[x] \subset M[x]$

Assume furthermore that M is a splitting field of $\tilde{f}(x)$ over $\tilde{K}$.

Want to show that $\exists$ a ring isomorphism

$$\begin{array}{ccc} L & \xrightarrow{\tilde{\varphi}} & M \\ \cup & & \cup \\ K & \xrightarrow[\varphi]{} & \tilde{K} \end{array}$$

s.t. $\tilde{\varphi}(k) = \varphi(k) \quad \forall\, k \in K$

$K_1[x]/(f_1(x)) \cong K_1[x]/(f(x)) \subseteq K_2[x]/(f_2(x))$

$f(x)$ $K_1 \xrightarrow[\text{isom } \varphi]{} K_2$ $f_2(x)$

$L \supseteq K(x_1, \ldots, x_n)$

$K \subset L \qquad K \subset M$

§3.2.4: Uniqueness of splitting fields.

A crucial but simple observation: Let $p(x) \in K[x]$ be irreducible. Suppose

1. $K \subset L$ is a field extension;
2. $\alpha, \beta \in K$ are two roots of $p(x)$ in L.

Then the composition of

$$L \supset K(\alpha) \xleftarrow{\sim} K[x]/\langle p \rangle \xrightarrow{\sim} K(\beta) \subset L,$$

gives a field isomorphism $\varphi : K(\alpha) \to K(\beta)$ such that

$$\varphi|_K = \mathrm{Id} \quad \text{and} \quad \varphi(\alpha) = \beta.$$

$\mathbb{Q}(e^{\frac{2\pi i k_1}{n}}) = \mathbb{Q}(e^{\frac{2\pi i k_2}{n}})$, $\forall\ k_1, k_2 \in [1, n-1]$ $(k_1, n) = 1$ $(k_2, n) = 1$

$\cong C_n$

Extension lemmas.

Need to talk about two extensions, so introduce following convention:

1. $K \subset L$, as a subset, for one extension;
2. $\varphi : K \to M$, a non-zero ring homomorphism, as another extension.
3. Let $\widetilde{K} = \varphi(K) \subset M$, so $\varphi : K \to \widetilde{K}$ is an isomorphism.
4. A ring homomorphism $\tilde{\varphi} : L \to M$ such that
$$\tilde{\varphi}|_K = \varphi : \ K \longrightarrow M$$
is called a *K-extension of φ* or a *K-homomorphism*.
5. Have ring isomorphism $\varphi : K[x] \to \widetilde{K}[x]$: $f \longmapsto \widetilde{f}$
$$\varphi(a_0 + a_1 x + \cdots + a_n x^n) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n.$$
(f on the left, $\widetilde{f}$ on the right)

One-Step Extension Lemma

Lemma. Let $p \in K[x]$ be irreducible and let $\tilde{p} = \varphi(p) \in \widetilde{K}[x]$. For any root $\alpha \in L$ of p in L and any root $\beta \in M$ of $\tilde{p}$ in M, $\exists$ an isomorphism

$$\varphi_1 : \ L \supset K(\alpha) \longrightarrow \widetilde{K}(\beta) \subset M$$

such that $\varphi_1(k) = \varphi(k)$ for all $k \in K$ and $\varphi_1(\alpha) = \beta$.

Proof. Can take φ_1 as the composition

$$K(\alpha) \xrightarrow{\sim} K[x]/\langle p \rangle \xrightarrow{[\varphi]} \widetilde{K}[x]/\langle \tilde{p} \rangle \xrightarrow{\sim} \widetilde{K}(\beta),$$

where

$$[\varphi] : \ f + \langle p \rangle \longmapsto \varphi(f) + \langle \tilde{p} \rangle.$$

Q.E.D.

Theorem (Extension Lemma.)

Let K be a field and $f \in K[x]$ non-constant. Assume

1. *$K \subset L$ is a splitting field of f over K;*
2. *$\varphi : K \to M$ an extension s. t. $\tilde{f} = \varphi(f)$ completely splits in $M[x]$.*

Then

1. *There is a K-extension $\tilde{\varphi} : L \to M$ of φ.* $\tilde{\varphi}(k) = \varphi(k), \ \forall k \in K$
2. *All K-homomorphism $\tilde{\varphi} : L \to M$ have same image, namely*

$$\tilde{\varphi}(L) = \widetilde{K}(R),$$

where R is the set of roots of $\tilde{f}$ in M.

Proof. Assume f is monic. Induction on $n = \deg(f) \geq 1$.

- $n = 1$: then $L = K$ and take $\tilde{\varphi} = \varphi$.

- Let p be any irreducible factor of f and write
$$f(x) = p(x)q(x) \quad \text{with} \quad \deg(p) < n,\ \deg(q) < n.$$
- At least one root α of f in L is also a root of p.
- Since $\tilde{f} = \tilde{p}\tilde{q}$, at least one root β of $\tilde{f}$ in M is also a root of $\tilde{p}$.
- By One-Step Extension Lemma, there exists isomorphism
$$\varphi_1 :\ L \supset K(\alpha) \longrightarrow \widetilde{K}(\beta) \subset M.$$
- Write $f(x) = (x - \alpha)f_1(x)$. Then $f_1(x) \in K(\alpha)[x]$.
- L is a splitting field of f_1 over $K(\alpha)$, and $\varphi_1(f_1) \in \widetilde{K}(\beta)[x]$ completely splits over M;

Proof cont'd:

on f_1

- Applying induction assumption, know that $\exists$ $K(\alpha)$-extension

$$\tilde{\varphi} : L \longrightarrow M$$

of φ_1, which is a desired K-extension of ϕ.

- If $\{\alpha_1, \ldots, \alpha_n\}$ are all the roots of f in L, then

$$R = \{\tilde{\varphi}(\alpha_1), \ldots, \tilde{\varphi}(\alpha_n)\}$$

are all the roots of $\tilde{f}$ in M. Since $L = K(\alpha_1, \ldots, \alpha_n)$, we have

$$\tilde{\varphi}(L) = \widetilde{K}(\tilde{\varphi}(\alpha_1), \ldots, \tilde{\varphi}(\alpha_n)) = \widetilde{K}(R).$$

Q.E.D.

Corollary (Uniqueness of splitting fields)

If $K \subset L$ and $\varphi : K \to M$ are two splitting fields of $f \in K[x]$, then there exists a K-isomorphism $\tilde{\varphi} : L \to M$ extending φ.

For any $K \subset L$

$$\mathrm{Aut}_K(L) = \{\sigma : L \to L \text{ ring isomorphism} \mid \sigma|_K = \mathrm{id}_K\}$$

Ex: C_n = nth cyclotomic $= \mathbb{Q}(e^{\frac{2\pi i}{n}})$

$$\cong \mathbb{Q}[x]/\langle \Phi_n(x) \rangle$$

$$\Phi_n(x) = \prod_{\substack{k \in [1,n) \\ (k,n)=1}} \left(x - e^{\frac{2\pi i k}{n}}\right) = p(x).$$

~~Fact~~ For each $k \in (1,n)$ s.t. $(k,n)=1$,

we have $\sigma_k \in \mathrm{Aut}_{\mathbb{Q}}(C_n)$ s.t.

$$\sigma_k\left(e^{\frac{2\pi i}{n}}\right) = e^{\frac{2\pi i k}{n}}.$$

Ex: Suppose L is a field of char. $p > 0$.

Consider the map $\sigma: L \to L$

$$a \longmapsto a^p$$

$$\sigma(a+b) = (a+b)^p = a^p + b^p = \sigma(a) + \sigma(b)$$

$$\sigma(ab) = (ab)^p = a^p b^p = \sigma(a)\,\sigma(b)$$

Ex: $L = \mathbb{F}_p(x)$. $\ni f = a_0 + a_1 x + \cdots + a_n x^n$

$$\sigma(f) = f^p = a_0^p + a_1^p x^p + \cdots + a_n^p x^{np}$$

$$= a_0 + a_1 x^p + a_2 x^{2p} + \cdots + a_n x^{np}$$

So σ is not surjective

Lemma: $\sigma: L \to L$ is surjective if $|L| < \infty$.