

MATH4302, Algebra II

Jiang-Hua Lu

The University of Hong Kong

Thursday March 31, 2022

Today

- ① §2.2.3: Existence of splitting fields;
- ② §2.2.4: 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 is a field extension L of K such that

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

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

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

$$\omega = e^{\frac{2\pi i}{3}}$$

$$\omega^2 \sqrt[3]{2}$$

$$\omega^2 \sqrt[3]{2}$$

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

Theorem to be proved today:

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”

Observations.

- If $K \subset L$, f splits completely in L , and $\{\alpha_1, \dots, \alpha_n\}$ are the roots of f in L , then

$$\underline{K(\alpha_1, \alpha_2, \dots, \alpha_n)}$$

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 .

Take any irreducible factor $p(x)$ of $f(x)$,
and take $L = K[x]/\langle p(x) \rangle$.

$$[L:K] \leq \deg f$$

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 is 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

$$[L_1 : K] \leq n$$

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

$$\deg f_1 = n-1$$

where $f_1(x) \in L_1[x]$ (in fact $f(x) \in K(\alpha_1)[x]$).

- By induction assumption, $\exists L \supset L_1$ and $\alpha_2, \dots, \alpha_n \in L$ such that

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

$$\alpha_i \in L_1 \subset L$$

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

QED

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

$$[L : L_1] \leq (n-1)!$$

§2.2.4: Uniqueness of splitting fields

§2.2.4: Uniqueness of splitting fields.

Extension lemmas.

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

- 1 $K \subset L$, as a subset, for one extension;
- 2 $\varphi : K \rightarrow M$, a non-zero ring homomorphism, as another extension.

- 3 Let $\tilde{K} = \varphi(K) \subset M$, so $\varphi : K \rightarrow \tilde{K}$ is an isomorphism.

- 4 A ring homomorphism $\tilde{\varphi} : L \rightarrow M$ such that

Definition:

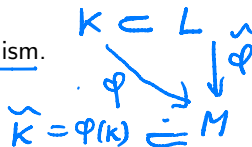
$$\tilde{\varphi}|_K = \varphi : K \rightarrow M$$

is called a K -extension of φ or a K -homomorphism.

- 5 Have ring isomorphism $\varphi : K[x] \rightarrow \tilde{K}[x]$:

$$\varphi(a_0 + a_1x + \cdots + a_nx^n) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n.$$

injective



§2.2.4: Uniqueness of splitting fields

One-Step Extension Lemma

$$K \subset L \quad \text{and} \quad \varphi: K \rightarrow M$$

$$\tilde{K} = \varphi(K) \subset M.$$

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

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

such that $\varphi_1(k) = \underline{\phi(k)}$ for all $\underline{k \in K}$ and $\underline{\varphi_1(\alpha) = \beta}$.

$$\begin{array}{ccc} K(\alpha) & \xrightarrow{\varphi_1} & \tilde{K}(\beta) \\ \cup & \nearrow \varphi & \\ K & & \end{array}$$

Proof. Can take φ_1 as the composition

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

Q.E.D.

$$\varphi: K[x] \rightarrow \tilde{K}[x], \text{ so } [\varphi]: f + \langle p \rangle \mapsto \varphi(f) + \langle \tilde{p} \rangle.$$

Special case ^{Suppose} 1) $p(x) \in K[x]$ irreducible

2) $K \subset L$ an extension

3) $p(x)$ has two roots α and β in L

Then

$$K(\alpha) \xrightarrow{\varphi} K(\beta) \subset L$$

$$\begin{array}{c} \cong \\ K[x]/\langle p \rangle \end{array}$$

$$\varphi(\alpha) = \beta$$

$$\varphi|_K = \text{id}_K$$

More precise:

$$\begin{array}{ccccc} & & K[x]/\langle p \rangle & & \\ & \swarrow \varphi_1 & & \searrow \varphi_2 & \\ L \supset K(\alpha) & & f(x) + \langle p \rangle & & K(\beta) \subset L \\ & \searrow f(\alpha) & & \swarrow f(\beta) & \end{array}$$

Define $\varphi = \varphi_2 \circ \varphi_1^{-1}: \alpha \xrightarrow{\varphi_1^{-1}} \bar{x} \xrightarrow{\varphi_2} \beta$

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 $\varphi : K \rightarrow M$ an extension s. t. $\tilde{f} = \varphi(f)$ completely splits in $M[x]$.

Then

- ① There is a K -extension $\tilde{\varphi} : L \rightarrow M$ of φ . $|M:L| \geq 1$
- ② All K -homomorphism $\tilde{\varphi} : L \rightarrow M$ have *same image*, namely

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

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 $\tilde{\varphi} = \varphi$.

§2.2.4: Uniqueness of splitting fields

- Let p be any irreducible factor of f and write

$$\underline{f(x) = p(x)q(x)} \quad \text{with} \quad \deg(p) < n, \quad \underline{\deg(q) < n.}$$

- At least one root α of f in L is also a root of p .
- Since $\underline{\tilde{f} = \tilde{p}\tilde{q}}$, 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

$$\varphi_1 : \underline{L \supset \underbrace{K(\alpha)}_{\text{New } K}} \longrightarrow \tilde{K}(\beta) \subset M.$$

$$K' = K(\alpha)$$

- Write $\underline{f(x) = (x - \alpha)f_1(x)}$. Then $f_1(x) \in \underline{K(\alpha)[x]} = K'[x]$
- L is a splitting field of f_1 over $K(\alpha)$, and $\varphi_1(f_1) \in \tilde{K}(\beta)[x]$ completely splits over M ;

Apply induction assumption to L as a splitting field of $\underline{f_1(x)}$ over $K' = K(\alpha)$ because $\deg f_1 = n-1$

Proof cont'd:

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

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

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

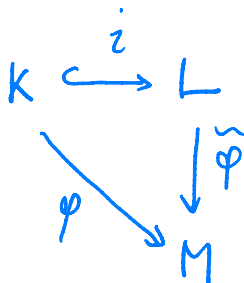
$$\tilde{\varphi}(L) = \tilde{K}(\underbrace{\tilde{\varphi}(\alpha_1), \dots, \tilde{\varphi}(\alpha_n)}) = \tilde{K}(R).$$

Q.E.D.

Corollary (Uniqueness of splitting fields)

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

$$\tilde{\varphi} \circ i = \varphi$$



$$k \in L$$

$$\tilde{\varphi}(k)$$

$$= \varphi(k)$$

$$\forall k \in K.$$