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

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

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 $\{\alpha_1, \ldots, \alpha_n\}$ 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 $\boxed{K[x]/\langle p(x)\rangle.}$
- 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 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

$|L_1 : K| \leq n$

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

$\deg f_1 = n-1$

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 $\alpha_2, \ldots, \alpha_n \in L$ such that

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

$\alpha_1 \in L_1 \subset L$

- $L_f \overset{\text{def}}{=} \boxed{K(\alpha_1, \ldots, \alpha_n)}$ 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.

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, injective as another extension.
3. Let $\widetilde{K} = \varphi(K) \subset M$, so $\varphi : K \to \widetilde{K}$ is an isomorphism.

$$\begin{tikzcd} K \arrow[dr, "\varphi"'] & \subset & L \arrow[d, "\hat{\varphi}"] \\ \widetilde{K} = \varphi(K) & \subseteq & M \end{tikzcd}$$

4. A ring homomorphism $\tilde{\varphi} : L \to M$ such that

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

   is called a K-extension of φ or a K-homomorphism.
5. Have ring isomorphism $\varphi : K[x] \to \widetilde{K}[x]$:
   $$\varphi(a_0 + a_1 x + \cdots + a_n x^n) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n.$$

One-Step Extension Lemma

$K \subset L$ and $\varphi : K \to M$

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

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 $\varphi_1(k) = \phi(k)$ for all $k \in K$ and $\varphi_1(\alpha) = \beta$.

$$\begin{tikzcd} & M \\ K(\alpha) \arrow[r, "\varphi_1"] & \tilde{K}(\beta) \arrow[u, phantom, "\subset"] \\ K \arrow[u, phantom, "\subset"] \arrow[ur, "\varphi"'] & \end{tikzcd}$$

Proof. Can take φ_1 as the composition

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

Q.E.D.

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

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

$$\begin{tikzcd} K(\alpha) \arrow[r, "\varphi"] \arrow[dr, phantom, "\cong" description, near start] & K(\beta) \subset L \arrow[dl, phantom, "\cong" description, near start] \\ & K[x]/\langle p \rangle \end{tikzcd}$$

$\varphi(\alpha) = \beta$

$\varphi|_K = id_K$

More precise:

$$\begin{tikzcd} & K[x]/\langle p\rangle \arrow[dl, "\varphi_1"', "\sim"] \arrow[dr, "\varphi_2", "\sim"'] & \\ L \supset K(\alpha) & & K(\beta) \subset L \end{tikzcd}$$

$$f(\alpha) \leftarrow\!\shortmid f(x) + \langle p \rangle \mapsto f(\beta)$$

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

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. *$\varphi : K \to M$ 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.* $|M:L| \geq 1$
2. *All K-homomorphism $\tilde{\varphi} : L \to M$ have same image, namely*

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

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

- 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

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

$K' = K(\alpha)$

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

Apply induction assumption to L as a splitting field of $f_1(x)$ 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 $\{\alpha_1, \ldots, \alpha_n\}$ 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 $\hat{\varphi}$ $L \to M$ extending φ.

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

$$\begin{tikzcd} K \arrow[r, hook, "i"] \arrow[dr, "\varphi"'] & L \arrow[d, "\hat{\varphi}"] \\ & M \end{tikzcd}$$

$k \in L$

$\hat{\varphi}(k)$

$= \varphi(k)$

$\forall k \in K.$