

MATH4302 Algebra II, HKU, 2022

Jiang-Hua Lu

The University of Hong Kong

Monday April 4, 2022

In this file

- 1 §2.2.5: Normal extensions.

Normal Extensions.

$K \subset L$ algebraic
means every $a \in L$ is
algebraic
over K

Definition. An algebraic field extension $K \subset L$ is said to be **normal** if every irreducible polynomial in $K[x]$ that has a root in L splits over L .

Examples.

- K is a normal extension of itself.
- $\mathbb{Q}[\sqrt[3]{2}]$ is **NOT** a normal extension of \mathbb{Q} .

$$p(x) = x^3 - 2$$

Let $p(x) \in K[x]$ be irreducible.

Then p has a root in $K \Leftrightarrow \deg p = 1$
 $(\Rightarrow) p(x) = ax + b$
 $a, b \in K$
 $a \neq 0$

Lemma. A finite normal extension of K must be a splitting field of some $f(x) \in K[x]$.

Proof. Let a_1, \dots, a_n be a basis of L over K .

- Each a_i is algebraic over K . Let $p_i \in K[x]$ be the minimal polynomial of a_i over K .
- Let $f = p_1 \cdots p_n$. By assumption, each p_i completely splits over L , so f completely splits over L .
- Let R be the set of all roots of f in L . Then $\{a_1, \dots, a_n\} \subset R$.
 $\forall i=1, \dots, n$
 $p_i(a_i) = 0$
 $\Rightarrow f(a_i) = 0$
- $L = K(a_1, \dots, a_n)$ $\subset K(R)$ $\subset L$, so $L = K(R)$.
- By definition, L is a splitting field of f over K .

Q.E.D.

finite

Theorem. Any splitting field over K is a normal extension.

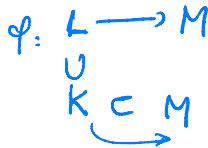
 $\deg p = k$

Proof. Let L be a splitting field of $f(x) \in K[x]$, and let $p(x) \in K[x]$ be irreducible. Let $\alpha \in L$ be a root of p . Want to prove that p has k roots in L

- Let M be a splitting field of $g(x) = f(x)p(x)$ over K . Then both f and p completely split over M . Indeed, $f(x)p(x)$ is a product of linear factors in $M[x]$, uniqueness of prime factorization implies that both f and p are products of linear factors in $M[x]$.

products

- By Extension Lemma, can identify $K \subset L \subset M$.
- Want to prove all roots of p in M are in L .
- Let $\beta \in M$ be any root of p . Want to show that $\beta \in L$.

 $p(x) \in K[x]$ irred.

Proof cont'd:

$$K \subset L \subset M$$

- Both $\alpha \in L$ and $\beta \in M$ are roots of p , so have isomorphism

$$\varphi : K(\alpha) \longrightarrow K[x]/\langle p(x) \rangle \longrightarrow K(\beta) \subset M$$

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

- L is a splitting field of f over $K(\alpha)$. By Extension Lemma again, $\exists \tilde{\varphi} : L \rightarrow M$ such that

$$\tilde{\varphi}|_{K(\alpha)} = \varphi : K(\alpha) \longrightarrow K(\beta).$$

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

- Now $K \subset M$ is extended to two embeddings $L \subset M$ and $\tilde{\varphi} : L \rightarrow M$. Extension Lemma implies that $\tilde{\varphi}(L) = L$, so

$$\beta = \tilde{\varphi}(\alpha) \in L.$$

- Thus all roots of p in M are in L .

$$\uparrow \quad \tilde{\varphi}(L) = L$$

Q.E.D.

Conclusion.

Theorem

Splitting fields over $K \Leftrightarrow$ finite and normal extensions of K

Example. $\mathbb{Q}[\sqrt[3]{2}]$ is not the splitting field of any $f \in \mathbb{Q}[x]$.

Easy to check that $\mathbb{Q}[\sqrt[3]{2}]$ is not ~~the~~ splitting field of $f(x) = x^3 - 2 \in \mathbb{Q}[x]$.

Eg: If K is a subfield of \mathbb{C} , then $\forall f \in K[x]$,
 $K(R_f) \subseteq \mathbb{C}$ is the splitting field of f/K .
 R_f : the set of all roots of f in \mathbb{C} .