Finite field extensions

Jiang-Hua Lu

The University of Hong Kong

MATH4302 Algebra II

Monday, March 31, 2025

Outline

In this file:

Review:

- Degree of a field extension: Given $K \subset L$, regard L as a vector space over K, and define

$$[L : K] = \text{dimension of } L \text{ as a vector space over } K.$$

- Finite extensions: $[L : K] < \infty$.
- Tower Theorem: For $K \subset M \subset L$, a tower of fields,

$$[L : K] = [L : M][M : K].$$

- If $p(x) \in K[x]$ is irreducible, then

$$K[x]/\langle p(x)\rangle$$

is an extension of K of degree equal to $n = \deg(p(x))$.

- Given a field extension $K \subset L$ and subset S of L, define

$$K(S) = \text{the smallest subfield of } L \text{ containing } S \text{ and } K.$$

When $S = \{a\}$, $K(a)$ is called a simple extension of K.

Review continued: Let $K \subset L$ be an extension (e.g. $\mathbb{Q} \subset \mathbb{C}$).

- Algebraic elements: An element $a \in L$ is algebraic over K if

$$E_a : \quad K[x] \longrightarrow L, \ f(x) \longmapsto f(a)$$

monic

has a non-zero kernel $I(a) = \{f(x) \in K[x] : f(a) = 0\}$. In this case, the ~~nomic~~ generator $p(x)$ of $I(a)$ is called the minimal polynomial of a over K, and

$$E_a : \quad K[x]/\langle p(x)\rangle \longrightarrow K[a] = K(a)$$

is an isomorphism of fields.

- An element $a \in L$ is algebraic over K iff $[K(a) : K] < \infty$.
- If $a \in L$ is not algebraic over K, say that a is transcendental over K.

Adjoining finitely many algebraic elements:

For a field extension $K \to L$, define the subring of L generated by $a_1, \ldots, a_n \in L$ over K as

$$K[a_1, \cdots, a_n] = \{f(a_1, \ldots, a_n) : f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]\}.$$

~~Example:~~ Recall that the sub-field of L generated by $a_1, \cdots, a_n$ ~~is~~ over K is

$$K(a_1, \cdots a_n) = \left\{ \frac{f(a_1, \cdots, a_n)}{g(a_1, \cdots a_n)} : \begin{array}{l} f, g \in K[x_1, \cdots x_n] \\ g(a_1, \cdots a_n) \neq 0 \end{array} \right\}$$

Main Proposition. If $a_1, a_2, \cdots a_n$ are all algebraic over K, then

1. $K(a_1, a_2, \cdots, a_n)$ is a finite extension of K;
2. $K(a_1, a_2, \cdots, a_n) = K[a_1, a_2, \cdots, a_n] \subset L$.

Proof. Let $K_0 = K$ and for $1 \leq i \leq n$, let

$$K_i = K(a_1, \ldots, a_i) = K_{i-1}(a_i)$$

- Then we have a tower of field extensions

$$K \subset K_1 \subset \cdots \subset K_n \subset L.$$

- Each a_i, being algebraic over K, is also algebraic over K_{i-1}.
- Thus each K_i is a finite extension of K_{i-1}.
- By the Tower Theorem, K_n is a finite extension over K. Moreover,

$$\begin{aligned} K_n &= K_{n-1}[a_n] = K_{n-2}[a_{n-1}][a_n] = K_{n-2}[a_{n-1}, a_n] = \cdots \\ &= K[a_1, \ldots, a_{n-1}, a_n]. \end{aligned}$$

Q.E.D.

Consequences of the Main Proposition:

Recall that ~~very~~ every element in a finite extension L of K is algebraic over K.

Theorem. An extension L of K is finite iff there exist $a_1, a_2, \cdots, a_n \in L$ which are algebraic over K such that $L = K(a_1, a_2, \cdots, a_n)$.

Proof.

- Assume first that L is a finite extension of K.
- Let $\{a_1, \ldots, a_n\}$ be a basis of L over K.
- Then every a_j is algebraic over K and $L = K(a_1, a_2, \cdots, a_n)$.
- The converse holds by the Main Proposition.

Q.E.D.

Very important examples.

For any $f \in \mathbb{Q}[x]$, let $a_1, \ldots, a_n$ be all the roots of f in $\mathbb{C}$. Then

- $L = \mathbb{Q}[a_1, a_2, \ldots, a_n]$ is a finite extension of $\mathbb{Q}$;

  $= \mathbb{Q}(a_1, a_2, \cdots, a_n)$

- Every element in $L = \mathbb{Q}[a_1, a_2, \ldots, a_n]$ is algebraic over $\mathbb{Q}$;
- The field L is called the splitting field of f in $\mathbb{C}$.

Then $f(x) = \alpha(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \in L[x]$

Q.E.D.

Ex: $f(x) = x^n - 1$, let $\omega_n = e^{\frac{2\pi i}{n}} \in \mathbb{C}$

Then $\alpha_j = \omega_n^j$ $j = 1, \cdots n$.

So $L = \mathbb{Q}(\omega_n) = \mathbb{Q}(\alpha_1, \cdots \alpha_n)$

$[L:\mathbb{Q}] = \varphi(n) = |\{k \in [1,n] : (k,n) = 1\}|$

Claim: (Proof in Tutorial)

The minimal poly of ω_n ~~over~~ over $\mathbb{Q}$ is

$$\Phi_n = \prod_{\substack{k\in[1,n-1] \\ (k,n)=1}} (x-\omega_n^k)$$

Later: $K \subset L$ $\quad Aut_K(L) = \{\sigma \in Aut(L) : \sigma|_K = id_K\}$

Tutorial

Compute the degree of $K[a_1, \ldots, a_n]$ over K by the Tower Theorem.

Example. The field $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a finite extension of $\mathbb{Q}$ since both $\sqrt{2}$ and $\sqrt{3}$ are algebraic over $\mathbb{Q}$.

- $[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$;
- Let $\alpha = \sqrt{2} + \sqrt{3}$ and $K = \mathbb{Q}[\alpha]$. Minimal polynomial of α is
$$p(x) = x^4 - 10x^2 + 1,$$
so $[K : \mathbb{Q}] = 4$, so $K = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. $= \mathbb{Q}(\sqrt{2} + \sqrt{3})$
- Seen another way: It follows from
$$\begin{cases} \alpha = \sqrt{2} + \sqrt{3}, \\ \alpha^3 = 15\sqrt{2} + 5\sqrt{3} \end{cases}$$
that
$$\sqrt{2} = \frac{-5\alpha + \alpha^3}{10}, \qquad \sqrt{3} = \frac{15\alpha - \alpha^3}{10}.$$
Thus $L \subset K$, so $K = L$.

Primitive Element Theorem. Every finite extension of $\mathbb{Q}$ is of the form $\mathbb{Q}(\alpha)$ for a single algebraic number over $\mathbb{Q}$.

Enough to prove that

$$\mathbb{Q}(a_1, a_2) = \mathbb{Q}(\alpha)$$

$\mathbb{Q}(a_1)$

$\mathbb{Q}(a_2)$ are proper subspaces

Choose $b \notin \mathbb{Q}(a_1) \cup \mathbb{Q}(a_2)$