MATH4302, Algebra II, HKU

Jiang-Hua Lu

The University of Hong Kong

Thursday March 18, 2022

Outline

Today:

1. §2.1.4: Finite field extensions

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

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

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

$\bar{x} \in L$ is a root of $p(x)$ in L.

Note: $p(x)$ has no root in K, for otherwise $p(x) = (x-\alpha)g(x)$ $\alpha \in K$, $g(x) \in K[x]$ contradiction.

- 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

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

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

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

$[K(a):K] = \deg p < \infty$

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.

In this case $K(a) \cong K(x)$ is an ∞ ext. of 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

$= \sum \alpha_{k_1,\cdots k_n} a_1^{k_1} \cdots a_n^{k_n} : \alpha_{k_1,\cdots k_n} \in K, \ (k_1, \cdots k_n) \in \mathbb{Z}_{\geq 0}^n$

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

Example: $K = \mathbb{Q}, \quad a_1 = \sqrt{5}, \quad a_2 = \pi$

$K[\sqrt{5}, \pi] \ni 9\sqrt{5} + 2\pi^2 + 3\sqrt{5}\pi^3 - 2$

$K(a_1, a_2, \cdots a_n) = \left\{ \frac{f(a_1, \cdots a_n)}{g(a_1, \cdots a_n)} : \begin{array}{l} f(x_1, \cdots x_n), g(x_1, \cdots x_n) \in K[x_1, \cdots x_n] \\ g(a_1, \cdots a_n) \neq 0 \end{array} \right\}$

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

$K[x] \subset K_1[x]$

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

$K_1 = K(a_1)$

$K_2 = K_1(a_2) = K(a_1, a_2)$

$K_3 = K_2(a_3) = K(a_1, a_2, a_3)$

$K_n = K(a_1, \cdots a_n)$

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

$$K \subset K_1 \subset \overset{\text{finite ?}}{K_2} \cdots \subset K_n \subset L.$$

- Each a_i, being algebraic over K, is also algebraic over K_{i-1}.

$K[x] \subset K_{i-1}[x]$

- 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,

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

$K_{n-1} = K_{n-2}[a_{n-1}]$

def

$K_n = K_{n-1}(a_n) = K_{n-1}[a_n]$

Thm before

Q.E.D.

Consequences of the Main Proposition:

$a \in L \Rightarrow 1, a, a^2, \cdots$ is linearly dependent.

Recall that very 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. If $L = K(a_1, \cdots a_n)$, where $a_1, \cdots a_n \in L$ are algebraic over K, then Main proposition $\Rightarrow |L:K| < \infty$.

Conversely, assume that $|L:K| < \infty$. Induction on $|L:K|$

If $|L:K| = 1$, then $L = K$, nothing to prove.

Assume statement holds for $|L:K| \leq m-1$. Now for $|L:K| = m \geq 2$ choose any $a_1 \in L \setminus K$, so $K < K(a_1) \subseteq L$

$m \leq 2m-2$

$|L:K(a_1)| \underbrace{|K(a_1):K|}_{\geq 2} = m \Rightarrow |L:K(a_1)| \leq \frac{m}{2} \leq m-1$

By induction, $\exists\ a_2, \cdots a_n \in L$ s.t.

$$L = K(a_1)(a_2, \cdots a_n) = K(a_1, \cdots a_n)$$ //

Method II: Since $|L:K| < \infty$, $\exists$ a basis $a_1, a_2, \cdots a_n$ of L over K.

Let $L' = K(a_1, \cdots a_n)$. Then $L' \subset L$

$L \subset L' \Rightarrow L' = L$. //

$k_1 a_1 + \cdots + k_n a_n \in L'$

$f(x) = x^9 - 7x^5 + 8x^4 - 2 \in \mathbb{Q}[x]$

Very important examples.

For any monic $f \in \mathbb{Q}[x]$, 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 $\mathbb{Q}$;
- 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 $\mathbb{C}$.

When $f(x) \in \mathbb{Q}[x]$ is regarded as in $L[x]$, **Q.E.D.**

we have $f(x) = \underbrace{\underbrace{(x-a_1)}_{L[x]} \underbrace{(x-a_2)}_{L[x]} \cdots \underbrace{(x-a_n)}_{L[x]}}$

splits into linear factors. //