Simple field extensions, I

Jiang-Hua Lu

The University of Hong Kong

MATH4302 Algebra II, HKU

Monday March 24, 2025

In this file:

- § 3.1.3: Simple field extensions, Part I

Recall Definition. Let $K \subset L$ be a field extension. For any subset S of L,

$$K(S) \stackrel{\text{def}}{=} \bigcap(\text{all sub-fields of } L \text{ containing } K \text{ and } S).$$

It is a sub-field of L, called the sub-field of L generated by S over K.

Remarks.

- Since L is a sub-field of L containing K and S, $K(S)$ is defined;
- $K(S)$ is the smallest sub-field of L containing K and S;
- For any subset S of L and $a \in L$,

$$K(S \cup \{a\}) = K(S)(a).$$

- We write $K(a) = K(\{a\})$ for $a \in L$.

$K \overset{}{\underset{d_1}{\hookrightarrow}} K(a_1)$ $\qquad$ $K \underset{d_2}{\hookrightarrow} K(a_2)$

Towers of extensions:

For $a_1, a_2, \ldots, a_n \in L$, have tower of extensions

$$\begin{aligned} K &\longrightarrow K(a_1) \longrightarrow K(a_1)(a_2) = K(a_1, a_2) \\ &\longrightarrow K(a_1, a_2)(a_3) = K(a_1, a_2, a_3) \\ &\longrightarrow \cdots \longrightarrow K(a_1, \ldots, a_{n-1})(a_n) = K(a_1, \ldots, a_n). \end{aligned}$$

Thus extensions of the form $K(a)$, for $a \in L$, are important to study.

Example: The extension $\mathbb{Q}$:

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2} + i\sqrt{3},\ \sqrt[3]{\sqrt{67}+2},\ \pi) \subset \mathbb{C}$$

as a tower: $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}+i\sqrt{3}) \subset \mathbb{Q}(\sqrt{2}+i\sqrt{3})(\sqrt[3]{\sqrt{67}+2})$
$\subset \left(\mathbb{Q}(\sqrt{2}+i\sqrt{3})(\sqrt[3]{\sqrt{67}+2})\right)(\pi) \subset \mathbb{C}$

Simple extensions

$$\alpha = \frac{1+\sqrt{5}}{2} + i\,\frac{\sqrt{17}+8i}{\sqrt{3}+1}$$

Definition. A field extension $K \subset L$ such that $L = K(a)$ for some $a \in L$ is said to be simple.

$$(2\alpha - 1)^2 = 5$$

Example. Examples of simple extensions of $\mathbb{Q}$:

$$\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}, \quad \mathbb{Q}(\pi) \subset \mathbb{R}, \quad \mathbb{Q}(\pi + i\sqrt{5}) \subset \mathbb{C}, \ldots.$$

For any extension $K \subset L$ and any finite set $S = \{a_1, a_2, \ldots, a_n\} \subset L$, we can understand the extension

$$K(S) \subset L$$

by the tower of simple extensions

$$\begin{aligned} K &\longrightarrow K(a_1) \longrightarrow K(a_1)(a_2) = K(a_1, a_2) \\ &\longrightarrow K(a_1, a_2)(a_3) = K(a_1, a_2, a_3) \\ &\longrightarrow \cdots \longrightarrow K(a_1, \ldots, a_{n-1})(a_n) = K(a_1, \ldots, a_n). \end{aligned}$$

Questions. For $K \subset L$ and $a \in L$,

- Is $K(a)$ always a finite extension of K?
- When yes, $[K(a):K] =?$.

By definition,

$$K(a) = \left\{ \frac{f(a)}{g(a)} : \ f, g \in K[x], \ g(a) \neq 0 \right\} \subset L.$$

Two examples:: $\mathbb{Q}(\pi)$ and $\mathbb{Q}(\sqrt{2})$:

$$\mathbb{Q}(\pi) \ni \frac{a_0 + a_1\pi + a_2\pi^2 + \cdots a_n\pi^n}{b_0 + b_1\pi + b_2\pi^2 + \cdots b_m\pi^m}.$$

$$\mathbb{Q}(\sqrt{2}) \ni \frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{c^2 - 2d^2} = \alpha + \beta\sqrt{2}.$$

Algebraic elements and transcendental elements:

Let $K \longrightarrow L$ be a field extension.

Definition. An element $a \in L$ is said to be algebraic over K if

$$\exists\ f(x) \in K[x] \backslash \{0\} \quad \text{such that} \quad f(a) = 0.$$

If $a \in L$ is not algebraic over K, say that a is transcendental over K.

Examples.

- π is transcendental over $\mathbb{Q}$;
- All the complex solutions to

$$x^9 - 21x^6 - 4x^3 + x - 87 = 0$$

  are algebraic over $\mathbb{Q}$.

$K(a)$ when a is transcendental. Recall that

$$K(x) = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x],\ g(x) \neq 0 \right\}.$$

Lemma. If $a \in L$ is transcendental over K, then

$$E_a : \quad K(x) \longrightarrow K(a), \quad \frac{f(x)}{g(x)} \longmapsto \frac{f(a)}{g(a)}$$

is an isomorphism. In particular, $K(a)$ is an infinite extension of K.

Proof. Since a is transcendental over K, $g(a) \neq 0$ for all $g(x) \in K[x]$ and $g(x) \neq 0$. Thus E_a is a well-defined ring homomorphism. As E_a is not identically 0, it is injective. By definition, E_a is also surjective. Thus E_a is an isomorphism of fields.

Example. $\mathbb{Q}(\pi) \cong \mathbb{Q}(e) \cong \mathbb{Q}(x)$.

Definition. By a transcendental number we mean a complex number that is transcendental over $\mathbb{Q}$.

All transcendental numbers give the isomorphic simple extensions of $\mathbb{Q}$, namely they are all isomorphic to $\mathbb{Q}(x)$.

The extensions $K(a)$ are much more interesting when $a \in L$ is algebraic over K.

Example. $\alpha = \sqrt{2} + \sqrt[3]{5}$ is algebraic over $\mathbb{Q}$ (write down one equation):

$$(\alpha - \sqrt{2})^3 = 5.$$

Continue to get rid of $\sqrt{2}$.

by $F(z) = \mathrm{Res}_x(f(x), g(z-x))$

$G(z) = \mathrm{Res}_x(f(x), x^n g(z/x))$

Is $\sqrt{\sqrt{2} + \sqrt[3]{\sqrt{5} + 3}} \in \mathbb{R}$ algebraic over $\mathbb{Q}$? How about

$$\frac{\sqrt{\sqrt{2} + \sqrt[3]{\sqrt{5} + 3}} + (\sqrt{2} + \sqrt[5]{17 + \sqrt{2}})^2}{\sqrt{13} - \sqrt[3]{17 - \sqrt{2}}}?$$

Minimal polynomial for $a \in L$ algebraic over K:

By definition, $a \in L$ is algebraic over K iff the ideal

$$I(a) = \{f(x) \in K[x] : f(a) = 0\} \subset K[x]$$

of $K[x]$ is non-zero. The monic generator p of is called the minimal polynomial of a.

Lemma. Assume that $a \in L$ is algebraic over K. Then a monic $p(x) \in K[x]$ is the minimal polynomial of a if and only if

- $p(a) = 0$;
- $p(x)$ is irreducible. because in a field, there is no zero divisor

Proof. Check directly by definitions.

let $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$

be the minimal poly. of α over $\mathbb{Q}$.

Let

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & \vdots \\ 0 & 0 & \cdots & 0 & \vdots \\ \vdots & \vdots & & & \vdots \\ 0 & 0 & \cdots & 0 & -a_{n-2} \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix} \in M_{n\times n}(\mathbb{Q})$$

~~Th~~ We know that the ~~char~~ $\det(xI-A) = p(x)$

since $p(x)$ is irred. $p(x)$ is also the minimal poly. of A.

Thus $p(x)$ is both the minimal poly of A over $\mathbb{Q}$ and the minimal poly of every ~~complex~~ root $\alpha \in \mathbb{C}$ over $\mathbb{Q}$

Main Theorem on simple extensions by algebraic elements:

Let $K \subset L$ be a field extension, let $a \in L$ be algebraic over K, and let $p(x) \in K[x]$ the minimal polynomial of a. Define the sub-ring $K[a]$ of L by

$$K[a] = \{f(a) : f(x) \in K[x]\} \subset L.$$

$\mathbb{Q}(\sqrt{2}) = \frac{a+b\sqrt{2}}{c+d\sqrt{2}}$

$a, b, c, d \in \mathbb{Q}$

Theorem. The evaluation map

$$E_a : \quad K[x]/\langle p(x)\rangle \longrightarrow K(a),\ \overline{f(x)} \longmapsto f(a). \in K[a]$$

is an isomorphism of fields.

$\Rightarrow K(a) = K[a]$

Proof. E_a is a non-zero ring homomorphism, so E_a is injective.

- We need to prove that E_a is surjective.

$a^n + a_{n-1}a^{n-1} + \cdots + \lambda_1 a + \lambda_0 = 0$

$a(a^{n-1} + \cdots + \lambda_1) = 1$

Proof cont'd:

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2+2b^2}$$

- Recall that
$$K(a) = \left\{ \frac{f(a)}{g(a)} : \ f,g \in K[x], \ g(a) \neq 0 \right\} \subset L.$$
- Need to show that if $g \in K[x]$, $g(a) \neq 0$, then $1/g(a) \in K[a]$.
- Since $p(x)$ is irreducible and $g(a) \neq 0$, g and p are co-prime.
- Since $K[x]$ is a PID, there exist $f(x), h(x) \in K[x]$ such that
$$f(x)g(x) + h(x)p(x) = 1.$$
- It follows that $f(a)g(a) = 1$ so $1/g(a) = f(a) \in K[a]$.

End of Monday.

Q.E.D.