# 2 Algebraic field extensions

## 2.1 Algebraic extensions

**Def:**
- A field extension is an inclusion $K \hookrightarrow L$ of a field $K$ as a subfield of a field $L$. We write $L/K$.
- The degree of $L/K$ is

  $$[L:K] = \dim_K L$$

  of $L$ as a $K$-vector space.
- $L/K$ is finite if $[L:K] < \infty$.
- An element $a \in L$ is algebraic over $K$ if it satisfies a nontrivial equation of the form

  $$c_n a^n + \dots + c_1 a + c_0 = 0$$

  with $c_0 - c_n \in K$. Otherwise, $a$ is called transcendental over $K$.
- $L/K$ is algebraic if every $a \in L$ is algebraic over $K$.

Ex: • $a = \sqrt{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$ (since $a^2 - 2 = 0$).

• $K/K$ is algebraic ($\forall a \in K$, $1 \cdot a - a = 0$).

• $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is algebraic (cf. Lemma 2).

• $\mathbb{C}/\mathbb{R}$ is algebraic ($\forall z \in \mathbb{C}$, $z^2 - (z + \bar{z}) \cdot z + (z \cdot \bar{z}) = 0$)

• $\mathbb{R}/\mathbb{Q}$ is not (since $\pi$ is not alg. $/\mathbb{Q}$).

Def: $L/K$ field extension, $a \in L$

• The evaluation at $a$ is the unique determined $K$-linear map

$$ev_a : K[T] \longrightarrow L$$

with $ev_a(T) = a$. We write $f(a) = ev_a(f)$ for $f \in K[T]$ and have

$$f(a) = c_n a^n + \ldots + c_0 \in L$$

if $f = c_n T^n + \ldots + c_0$.

Since $K[T]$ is a PID, $\ker(ev_a) = (f)$ for some $f \in K[T]$. Since $K[T]^\times = K^\times$, there is a unique monic $f$ s.t. $\ker(ev_a) = (f)$, i.e. $f = 1 \cdot T^n + c_{n-1} T^{n-1} + \ldots + c_0$.

<u>Def:</u> $a \in L/K$

The <u>minimal polynomial of $a$ over $K$</u> is the unique monic $f \in K[T]$ such that $\ker(ev_a) = (f)$. We write $f = \mathrm{Mipo}_a$.

<u>Rem:</u>
- Let $f = \mathrm{Mipo}_a$. Since $f \in \ker(ev_a)$, $f(a) = ev_a(f) = 0$.
- If $g(a) = 0$, then $g \in \ker(ev_a) = (f)$, and thus $f \mid g$.
- Thus if $g$ is monic, irreducible and $g(a) = 0$, then $g = f = \mathrm{Mipo}_a$.
- Since $K[T]/(f) \simeq \mathrm{im}(ev_a) \subset L$ is an integral domain, $(f)$ is a prime ideal. Thus $f = 0$ or $f$ is prime and thus irreducible.

  ($K[T]$ PID $\Rightarrow$ UFD $\Rightarrow$ "prime = irreducible")
- The map
$$M_a : L \longrightarrow L$$
$$b \longmapsto ab$$
is $K$-linear. If $[L:K] < \infty$, then the minimal polynomial of $M_a$ equals $\mathrm{Mipo}_a$. (Exercise on List 2)

**Lemma 1:** $L/K$

$a \in L$

Then $a$ is algebraic over $K$

iff. $\ker(ev_a) \neq 0$.

**proof:** • Assume $\ker(ev_a) = (f) \neq 0$, i.e. $f = \sum c_i T^i \neq 0$.

Then

$$0 = ev_a(f) = \sum c_i \, ev_a(T)^i = \sum c_i a^i$$

is a non-trivial relation.

$\Rightarrow$ $a$ alg. over $K$.

• If $\ker(ev_a) = 0$, then $ev_a : K[T] \to L$

is injective.

$\Rightarrow$ $\{1, a, a^2, \ldots\} \subset L$ is

lin. indep. over $K$.

$\Rightarrow$ $a$ does not satisfy any

non-trivial relation over $K$.

$\Rightarrow$ $a$ is not alg. $/K$. $\square$

**Lemma 2:** $L/K$ finite

Then $L/K$ is algebraic

proof: Let $n = [L:K]$. Consider $a \in L$.

$\Rightarrow$ $\{1, a, \ldots, a^n\}$ lin. dependent over $K$

$\Rightarrow$ $\exists$ non-trivial relation

$$c_0 \cdot 1 + c_1 \cdot a^1 + \ldots + c_n \cdot a^n = 0.$$

$\Rightarrow$ $a$ alg. $/K$. $\square$

Lemma 3: $L/E$ & $E/K$ finite

Then $[L:K] = [L:E] \cdot [E:K]$.

$$n \cdot m \left( \begin{array}{l} L \\ |\ m \\ E \\ |\ n \\ K \end{array} \right.$$

proof: Choose bases $(x_1, \ldots, x_n)$ of $E$ over $K$ and $(y_1, \ldots, y_m)$ of $L$ over $E$ where $n = [E:K]$, $m = [L:E]$. $\Rightarrow$ $\forall a \in L$ $\exists!$ $r_1, \ldots, r_m \in E$ s.t.

$$a = r_1 y_1 + \ldots + r_m y_m$$

and $\exists!$ $b_{i,j} \in K$ $(i = 1 \ldots m, j = 1 \ldots n)$ s.t.

$$r_i = b_{i,1} x_1 + \ldots + b_{i,n} x_n$$

for $i = 1 \ldots m$.

Thus
$$a = \sum_{i,j} b_{i,j} x_j y_i .$$

Since the $b_{i,j}$ are unique, $(x_j y_i)_{\substack{i=1\ldots m \\ j=1\ldots n}}$ is a basis of $L/K$.

Thus $[L:K] = m \cdot n = [L:E] \cdot [E:K]$. $\square$

**Def:** $L/K$

$a_1, \ldots, a_n \in L$

- $K[a_1, \ldots, a_n]$ is the smallest subring of $L$ that contains $K$ and $a_1, \ldots, a_n$.
  It is called the <u>$K$-algebra generated by $a_1, \ldots, a_n$</u>.
- $K(a_1, \ldots, a_n)$ is the smallest subfield of $L$ that contains $K$ and $a_1, \ldots, a_n$.
  It is called the <u>field extension of $K$ generated by $a_1, \ldots, a_n$</u>.

**Rem:** There is always such a smallest subring / subfield.

We have

$$K[a_1, \ldots, a_n] = \bigcap_{\substack{K \subset E \subset L \\ E \text{ ring} \\ a_1, \ldots, a_n \in E}} E = \left\{ b \in L \;\middle|\; \begin{array}{l} b = f(a_1, \ldots, a_n) \text{ for} \\ \text{some } f \in K[T_1, \ldots, T_n] \end{array} \right\}$$

and

$$K(a_1, \ldots, a_n) = \bigcap_{\substack{K \subset E \subset L \\ E \text{ field} \\ a_1, \ldots, a_n \in E}} E = \left\{ b \in L \;\middle|\; \begin{array}{l} b = \dfrac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)} \text{ for} \\ \text{some } f, g \in K[T_1, \ldots, T_n] \\ \text{with } g(a_1, \ldots, a_n) \neq 0 \end{array} \right\}.$$

Thm. 4: $a \in L/K$

Equiv.: (1) $a$ is algebraic over $K$;

(2) $[K(a):K] < \infty$;

(3) $K(a)/K$ is algebraic;

(4) $K[a] = K(a)$.

proof: Clear for $a=0$. Assume $a \neq 0$.

(1)⇒(2): $a$ alg. $/K$

$\Rightarrow (f) = \ker(ev_a)$ max. ideal of $K[T]$

$\Rightarrow K[a] = \operatorname{im}(ev_a) \cong K[T]/(f)$ is a field

$\Rightarrow K[a] = K(a)$ and $ev_a : K[T] \to K(a)$ surjective

$\Rightarrow (1, a, \ldots, a^{n-1})$ is a basis of $K(a) = K[a]$ where $n = \deg f = \dim_K K[a] = [K(a):K]$

$\Rightarrow [K(a):K] < \infty$

Note: $[K(a):K] = \deg(\text{Mipo}_a)$

(2)⇒(3): Lemma 2

(3)⇒(4): $K(a)/K$ alg.

$\Rightarrow \forall b \in K[a] - \{0\}$, $f = \text{Mipo}_{b^{-1}} = T^n + c_{n-1}T^{n-1} + \ldots + c_0$ we have

$$b^{-n} + c_{n-1} b^{-n+1} + \ldots + c_1 b^{-1} + c_0 = 0$$

$\Rightarrow$ $(\cdot b^{n-1})$ $b^{-1} = -(c_{n-1} + \ldots + c_0 b^{n-1}) \in K[a]$

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

(4) $\Rightarrow$ (1): $K[a] = K(a)$

$\Rightarrow a^{-1} = \sum_{i=1}^{n} c_i a^{i-1}$ for some $c_i \in K$

$\Rightarrow \sum_{i=1}^{n} c_i a^{i} - 1 = 0$

$\Rightarrow a$ alg. $/K$. $\square$

**Cor 5:** If $a$ is algebraic over $K$, then $[K(a):K] = \deg(\mathrm{Mipo}_a)$. $\square$

**Cor. 6:** If $L/E$ and $E/K$ are algebraic, then $L/K$ is algebraic.

$$\begin{tikzcd} L \arrow[d, dash, "\text{alg}"] \arrow[dd, dash, bend right=60, "\text{alg}"'] \\ E \arrow[d, dash, "\text{alg}"] \\ K \end{tikzcd}$$

**proof:** Consider $a \in L$, and let $f = \sum c_i T^i$ be its minimal polynomial over $E$. Then $c_i \in E$ is algebraic over $K$ for all $i = 0 \ldots n$. Thus

$$\begin{tikzcd} K(c_0 \ldots c_n, a) \arrow[d, dash, "\text{finite}"] \\ K(c_0 \ldots c_n) \arrow[d, dash, "\text{finite}"] \\ \vdots \arrow[d, dash, "\text{finite}"] \\ K(c_0) \arrow[d, dash, "\text{finite}"] \\ K \end{tikzcd}$$

$K \subset K(c_0) \subset K(c_0, c_1) \subset \ldots \subset K(c_0 \ldots c_n) \subset K(c_0 \ldots c_n, a)$ is a series of finite field extensions by Thm. 4. By Lemma 3,

$$[K(c_0 \ldots c_n, a) : K] = [K(c_0 \ldots c_n, a) : K(c_0 \ldots c_n)] \cdots [K(c_0) : K],$$

which is finite. Thus $K(a)/K$ is finite, and $a$ algebraic over $K$ by Thm. 4. $\square$

Rem: There are infinite algebraic extensions, for example

$$\mathbb{Q}(\sqrt[2]{2}, \sqrt[3]{2}, \sqrt[4]{2}, \dots) / \mathbb{Q}.$$

Note that

$$\mathrm{Mipo}_{\sqrt[n]{2}} = T^n - 2$$

($T^n - 2$ is irreducible by the Eisenstein criterium, and $(\sqrt[n]{2})^n - 2 = 0$), thus $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$ and

$$[\mathbb{Q}(\sqrt[2]{2}, \sqrt[3]{2}, \dots) : \mathbb{Q}] = \infty.$$