3.2 Separable extensions

<u>Def:</u> $\overline{K}$ alg. cl. of K

$f \in K[T]$

$f = u \prod_{i=1}^{n} (T - a_i)$ factorization in $\overline{K}[T]$

L/K arbitrary

(1) f is <u>separable</u> :⇔ $a_1, \ldots, a_n$ are pairwise distinct.

(2) An element $a \in L/K$ is <u>separable over K</u> if its minimal polynomial over K is separable.

(3) L/K is <u>separable</u> if every $a \in L$ is separable over K.

<u>Def:</u> $f = \sum_{i=0}^{n} c_i T^i \in K[T]$

The <u>formal derivative of f</u> is

$$f' = \sum_{i=1}^{n} i \cdot c_i \cdot T^{i-1}.$$

<u>Lemma 1:</u> If f is irreducible and <u>not</u> separable, then char $K = p > 0$ and

$$f = c_0 + c_p T^p + \ldots + c_{np} T^{np}.$$

proof: • Consider the factorization $f = u \prod_{i=1}^{n} (T - a_i)$ in $\overline{K}[T]$. By Leibniz' formula (exercise!),

$$f' = u \cdot \sum_{i=1}^{n} \prod_{j \neq i} (T - a_j)$$

in $\bar{K}[T]$. Since f has a multiple root, say $a = a_1 = a_2$, we have $f'(a) = 0$.

- Thus the minimal polynomial g of a over K divides both f' and f.

  Since f is irreducible, $f = u \cdot g$.

  Since $\deg f' \le \deg f - 1$ and $f' \in (g) = (f)$, we must have $f' = 0$.

- This is only possible if $\operatorname{char} K = p > 0$ and all coefficients $i \cdot c_i$

$$f' = \sum_{i=1}^{n} i \cdot c_i T^{i-1}$$

are zero, i.e. $c_i = 0$ if $p \nmid i$. $\square$

__Cor 2:__ If $\operatorname{char} K = 0$, then every irreducible polynomial is separable, and every algebraic extension L/K is separable. $\square$

__Def:__ L/K algebraic

The __separable degree of L/K__ is the number

$$[L:K]_s = \#\{\sigma : L \to \bar{K} \mid \sigma(a) = a \text{ for } a \in K\}$$

of K-linear embeddings
$$\begin{tikzcd} L \arrow[rr, "\sigma"] & & \bar{K} \\ & K \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}.$$

Lemma 3: L/K algebraic
$a \in L$
$f = \sum_{i=0}^{n} c_i T^i$ minimal polynomial of a over K
Then
$$[K(a):K]_s = \#\{b \in \bar{K} \mid f(b) = 0\}.$$

proof: • A K-linear hom. $\sigma: K(a) \longrightarrow \bar{K}$ is determined by the image $\sigma(a)$ of a.
Since σ leaves K fixed,
$$f(\sigma(a)) = \sum_{i=0}^{n} c_i \, \sigma(a)^i = \sigma\Big(\sum_{i=0}^{n} c_i \, a^i\Big) = \sigma(f(a)) = 0,$$
i.e. $\sigma(a) \in \bar{K}$ is a root of f.

• If conversely, $b \in \bar{K}$ is a root of f, then the minimal polynomial g of b over K divides f. Since f is irreducible and monic, $g = f$.
Since $ev_b : K[T] \longrightarrow \bar{K}$ has kernel $(g) = (f)$, we obtain a K-linear hom.
$$\begin{aligned} \sigma_b : \; K(a) &\xrightarrow{\sim} K[T]/(f) \xrightarrow{\overline{ev}_b} \bar{K} \\ a &\longmapsto [T] \longmapsto b \end{aligned}$$
that maps a to b. This yields a bijection
$$\left\{ \begin{tikzcd} K(a) \arrow[rr, "\sigma"] & & \bar{K} \\ & K \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd} \right\} \overset{1:1}{\longleftrightarrow} \{b \in \bar{K} \mid f(b) = 0\}.$$
$$\sigma \longmapsto \sigma(a)$$
$\square$

Cor 4: $\alpha \in \overline{K}$

Then $[K(\alpha):K]_s \leq [K(\alpha):K]$, and equality holds if and only if α is separable over K.

proof: Let f be the minimal polynomial of α. Then

$$[K(\alpha):K]_s \underset{(\text{Lemma } 3)}{=} \#\{b \in \overline{K} \mid f(b)=0\}$$

$$\leq \deg f = [K(\alpha):K],$$

and equality holds

$\iff$ all roots of f pairwise distinct

$\iff$ f separable

$\iff$ α separable over K. $\square$

$$\begin{tikzcd} L \arrow[d, dash] \\ E \arrow[d, dash] \\ K \end{tikzcd}$$

Lemma 5: $L/E/K$ finite

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

proof: Consider (fix $\overline{E} = \overline{L}$)

$$S = \left\{ \begin{tikzcd} E \arrow[rr, "\sigma_i"] & & \overline{E} \\ & K \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd} \right\}_{i \in I} \text{ and } T_i = \left\{ \begin{tikzcd} L \arrow[rr, "\tau_{ij}"] \arrow[dr, dash] & & \overline{L} \\ & E \arrow[ur, "\sigma_i"'] & \end{tikzcd} \right\}_{j \in J_i}.$$

Then $[E:K]_s = \# S$ and $[L:E]_s = \# T_i$ (any $i \in I$). Thus

$$[L:K]_s = \#\left\{ \begin{tikzcd} L \arrow[rr, "\tau_{ij}"] & & \overline{L} \\ & K \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd} \right\}_{\substack{i \in I \\ j \in J_i}} = \sum_{i \in I} \# T_i = \# T_i \cdot \# S$$

$$= [L:E]_s \cdot [E:K]_s$$

$\square$

Cor 6: $L = K(a_1 \dots a_n)/K$ finite

Then $[L:K]_s \leq [L:K]$, and "=" iff $a_1 \dots a_n$ are separable over K.

proof: Define $K_i := K(a_1 \dots a_i)$ and consider

$$K = K_0 \subset K_1 \subset \dots \subset K_n = L.$$

Since $K_{i+1} = K_i(a_{i+1})$, Cor. 4 implies $[K_{i+1}:K_i]_s \leq [K_{i+1}:K_i]$, with "=" iff a_{i+1} is separable over K_i, which is the case if a_{i+1} is separable over K.

By Lemma 5,

$$[L:K]_s = \prod_{i=0}^{n-1} [K_{i+1}:K_i]_s \leq \prod_{i=0}^{n-1} [K_{i+1}:K_i] = [L:K],$$

with "=" if $a_1 \dots a_n$ are separable over K. $\square$

Thm. 7: $L = K(a_1 \dots a_n)/K$ finite

Equiv: (1) L/K separable.

(2) $a_1 \dots a_n$ separable over K.

(3) $[L:K]_s = [L:K]$.

proof: (1) $\Rightarrow$ (2): clear.

(2) $\Rightarrow$ (3): Cor. 6.

(3) $\Rightarrow$ (1): Consider $a \in L$ and $K \subset K(a) \subset L$. Then

$$[L:K(a)]_s \cdot [K(a):K]_s = [L:K]_s = [L:K] = [L:K(a)] \cdot [K(a):K]$$

$$\begin{array}{c} L \\ | \\ K(a) \\ | \\ K \end{array}$$

By Cor. 6, $[-]_s \leq [-]$

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

$\Rightarrow$ a separable over K (by Cor. 4)

Thus L/K is separable. $\square$

<u>Cor. 8:</u> $L/E/K$ finite

Then L/K is separable iff

both L/E and E/K are separable.

$$\begin{tikzcd} L \arrow[d, dash, "\text{sep.}"'] \arrow[dd, dash, bend left, "\text{sep.}"] \\ E \arrow[d, dash, "\text{sep.}"'] \\ K \end{tikzcd}$$

<u>proof:</u> L/K is separable

$\iff$ $[L:E]_s \cdot [E:K]_s = [L:K]_s \underset{(\text{Thm. } 7)}{=} [L:K] = [L:E] \cdot [E:K]$.

$\iff$ $[L:E]_s = [L:E]$ and $[E:K]_s = [E:K]$
$\left(\begin{array}{c} [-]_s \leq [-] \\ \text{Cor. } 6 \end{array}\right)$

$\iff$ L/E and E/K both separable.
(Thm. 7) $\square$

<u>Def:</u> L/K arbitrary

The <u>separable closure of K in L</u> is

$$E = \{a \in L \mid a \text{ separable over } K\}.$$

The <u>separable closure of K</u> is the separable closure of K in $\overline{K}$.

Cor 9: L/K arbitrary

The separable closure of K in L is the largest subfield of L that is separable over K.

proof: Let $a, b \in E$. Then $K(a,b)/K$ is separable over K by Thm. 7, and thus

$a+b$, $a-b$, $a \cdot b$ and $\frac{a}{b}$ (if $b \neq 0$)

are separable over K and thus in E.

Thus E is a subfield of L. By definition, it is the largest subfield of L that is separable over K. $\square$

Exercise: $[L:K]_s = [E:K]$, and thus $[L:K]_s$ is a divisor of $[L:K]$ (if L/K is finite).

$$\begin{array}{c} L \\ | \\ E \\ | \\ K \end{array}$$

Thm. 10: (Theorem of the primitive element)

L/K finite separable

Then $L = K(a)$ for some $a \in L$.

(a is called a <u>primitive element for L/K</u>)

proof: · <u>K finite</u>: Later / exercise.

· <u>K infinite</u>: Since L/K is finite, $L = K(a_1, \ldots, a_n)$ for some $a_1, \ldots, a_n \in L$.

Find a primitive element by induction on n:

$\underline{n=1:}$ $L = K(a_1) \rightsquigarrow a_1$ is a prim. elt.

$\underline{n>1:}$ • $L = K(a_1, \dots, a_{n-1})(a_n)$. By IH, $K(a_1, \dots, a_{n-1}) = K(b)$ for some $b \in K(a_1, \dots, a_{n-1}) \Rightarrow L = K(a, b)$ for $a = a_n$.

$$\begin{array}{c} L = K(a,b) \\ | \\ K(a_1, \dots, a_{n-1}) \\ | \\ K \end{array}$$

• Let

$$m = [L:K] = [L:K]_s = \#\left\{ \begin{tikzcd}[column sep=small] L \arrow[rr, "\sigma_i"] \arrow[dr, dash] & & \bar{K} \arrow[dl, dash] \\ & K & \end{tikzcd} \right\}_{i=1,\dots,m}$$

Define

$$P(T) = \prod_{1 \le i < j \le n} \Big[\big(\sigma_i(a) T + \sigma_i(b)\big) - \big(\sigma_j(a) T + \sigma_j(b)\big) \Big].$$

Since K is infinite, $\exists c \in K$ s.t. $P(c) \neq 0$.

Thus $\sigma_1(ac+b), \dots, \sigma_n(ac+b)$ are pairwise distinct, i.e. $[K(ac+b):K]_s \geq m = [L:K]_s$

Since $ac+b \in L$, $L = K(ac+b)$,

i.e. $ac+b$ is a prim. elt. for L/K. $\square$

$\underline{\text{Rem:}}$ The proof works also for finite fields K with more than $\deg P(T) = \frac{m^2 - m}{2}$ elements (where $m = [L:K]$).