5 Non-Galois extensions

5.1 Inseparable extensions

Ex: $\mathbb{F}_p(x) / \mathbb{F}_p(x^p)$ is a typical example of an inseparable extension.

Prop 1: K of $\operatorname{char} K = p > 0$
$a \in \bar{K}$
f minimal polynomial of a over K
Then there is an $u \geq 0$ such that
(1) every root of f has multiplicity p^u;
(2) a^{p^u} is separable over K;
(3) $[K(a):K] = p^u \cdot [K(a):K]_s$.

proof: • Let $a = a_1, \dots, a_r \in \bar{K}$ be the pairwise distinct roots of f and $e_1, \dots, e_r$ their multiplicities, i.e. $f = \prod_{i=1}^{r} (T - a_i)^{e_i}$ in $\bar{K}[T]$.

• Since f is irreducible, it is the minpo of each a_i. Thus we have isomorphisms

$$\sigma_i : K(a) \xrightarrow{\sim} K[T]/(f) \xrightarrow{\sim} K(a_i) \subseteq \bar{K},$$
$$a \longmapsto [T] \longleftarrow a_i$$

which extend to isom. $\bar{\sigma}_i : \bar{K} \to \bar{K}$ by Lemma 2.2.7.

- Since $\bar{\sigma}_i(A) = A$, we have

$$\prod_{i=1}^{r} (T - a_i)^{e_i} = f = \bar{\sigma}_j(f) = \prod_{i=1}^{r} (T - \bar{\sigma}_j(a_i))^{e_i}$$

which implies that $e_j = e_i$ for all $j = 1 - r$.

Thus all roots have the same multiplicity

$e = e_1 = \cdots = e_r$.

- By Lemma 3.2.1, $f = \sum c_{ip} T^{ip}$ if f is not separable. Thus $f(T) = g(T^p)$ for $g = \sum c_{ip} T^i$, and
  - $\deg f = p \cdot \deg g$
  - a_i^p is a root of g for all $i = 1 - r$

Repeating this argument, we find an $n \geq 0$ and a separable $h \in K[T]$ s.t.

- $f(T) = h(T^{p^n})$
- $\deg f = p^n \cdot \deg h$
- $a_i^{p^n}$ is a root of h for all $i = 1 - r$.

We will show that this n satisfies (1)–(3).

- h irreducible: If $h = h_1 \cdot h_2$, then

$$f = h(T^{p^n}) = h_1(T^{p^n}) \cdot h_2(T^{p^n})$$

$\Rightarrow h_1(T^{p^n}) \in K^\times$ or $h_2(T^{p^n}) \in K^\times$

$\Rightarrow h_1 \in K^\times$ or $h_2 \in K^\times \Rightarrow h$ irreducible.

$K(a)$ · $K[T]/(h) \cong K(a^{p^u})$ $\quad (h(a^{p^u}) = 0)$,

$\deg f$ ($| p^u$ $K(a^{p^u})$ $| \deg h$ K)

$\Rightarrow [K(a):K] = p^u \cdot [K(a^{p^u}):K]$ $\quad (\deg f = p^u \cdot \deg h)$

$\Rightarrow [K(a):K(a^{p^u})] = p^u$.

· a is a root of $T^{p^u} - a^{p^u} \in K(a^{p^u})[T]$, and

$T^{p^u} - a^{p^u} = (T-a)^{p^u} \mid f$ $\quad$ (in $\bar{K}[T]$)

$\Rightarrow e \geq p^u$.

· h separable $\Rightarrow$ h has $s = \deg h$ pairwise distinct roots. Thus f has $r \geq s$ distinct roots. Since ($a_1^{p^u}, \dots, a_r^{p^u}$ might not be distinct)

$$p^u \cdot s = p^u \cdot \deg h = \deg f = e \cdot r,$$

this implies that $e = p^u$ and $r = s$.

Thus (1) & (2).

· $[K(a):K]_s = \#\{\text{roots of } f\} = r$ $\quad$ (Lemma 3.2.3)

$\Rightarrow [K(a):K] = p^u \cdot \deg h = p^u \cdot r = p^u \cdot [K(a):K]_s$.

Thus (3). □

Def: L/K finite

The <u>inseparable degree of L over K</u> is

$$[L:K]_i = \frac{[L:K]}{[L:K]_s}.$$

Cor 2: L/K finite, $\mathrm{char}\, K = p > 0$

Then $[L:K]_i = p^u$ for some $u \geq 0$.

(by Cor. 3 below)

proof: $L = K_r = K(a_1, \dots, a_r)$

$K_{r-1} = K(a_1, \dots, a_{r-1})$

$\vdots$

$K_1 = K(a_1)$

$K_0 = K$

$\Rightarrow [L:K]_i = \prod_{i=1}^{r} [K_i : K_{i-1}]_i$

$= \prod_{i=1}^{r} p^{u_i}$ (some $u_i \geq 0$)

(Prop 1)

$= p^{\sum u_i}$.

□

Cor 3: $K \subset E \subset L$ finite

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

proof:

$$[L:K]_i = \frac{[L:K]}{[L:K]_s}$$

$$= \frac{[L:E]\cdot[E:K]}{[L:E]_s \cdot [E:K]_s} = [L:E]_i \cdot [E:K]_i.$$

(Lemmas 2.1.3 & 3.2.5)

□

Def: L/K algebraic, $\mathrm{char}\, K = p > 0$

An element $a \in L$ is <u>purely inseparable over K</u>

if $a^{p^u} \in K$ for some $u \geq 0$.

The extension L/K is <u>purely inseparable</u>

if every $a \in L$ is purely inseparable over K.

Thm 4: $L = K(a_1, \dots, a_r)$ / K algebraic

Equiv: (1) L/K is purely inseparable.

(2) $a_1, \dots, a_r$ are purely inseparable over K.

(3) $[L:K]_s = 1$.

(4) The minimal polynomial of every $a \in L$ over K is of the form $T^{p^{n_a}} - a^{p^{n_a}}$ for some $n_a \geq 0$.

proof: (1) $\Rightarrow$ (2): This follows from the definition. ∎

(2) $\Rightarrow$ (3): $a_1, \dots, a_r$ purely inseparable over K.

Then the minimal polynomial f_i of a_i over K is a divisor of $T^{p^{n_i}} - a_i^{p^{n_i}}$ for some $n_i \geq 0$.

$\Rightarrow$ a_i is the only root of f_i.

$\Rightarrow$ Every homomorphism $\sigma: L \to \bar{L}$ (over K) sends a_i to $\sigma(a_i) = a_i$.

$\Rightarrow$ $[L:K]_s = \#\{\sigma: L \to \bar{L} \text{ over } K\} = 1$. ∎

(3) $\Rightarrow$ (4): Let $a \in L$. Then $[K(a):K]_s \leq [L:K]_s = 1$

$\Rightarrow$ a is the only root of its minimal polynomial f over K

$\Rightarrow$ By Prop. 1, there is an $n = n_a \geq 0$ s.t.

$$\deg f = [K(a):K] = p^n \cdot [K(a):K]_s = p^n.$$

Thus $f = (T-a)^{p^n} = T^{p^n} - a^{p^n}$. ∎

(4) $\Rightarrow$ (1): Immediate from the definition. □

Cor 5: L/K algebraic

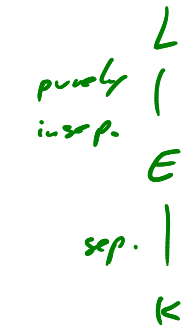
E separable closure of K in L

Then E/K is separable of degree

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

and L/E is purely inseparable of degree

$$[L:E] = [L:K]_i.$$



proof: . This is clear in char. 0. Assume that $\operatorname{char} K = p > 0$.

. By definition, E/K is separable.

. By Prop. 1, $\forall \alpha \in L \ \exists n \geq 0$ s.t. α^{p^n} is separable over K.

$\Rightarrow \alpha^{p^n} \in E \Rightarrow \alpha$ is purely inseparable over E.

Thus L/E is purely inseparable.

. $[E:K]_s = [E:K]$ (E/K separable),

$[L,E]_s = 1$ (Thm. 4)

$\Rightarrow [L:K]_s = [L:E]_s \cdot [E:K]_s = 1 \cdot [E:K]$

and $[L:K]_i = \dfrac{[L:K]}{[L:K]_s} = \dfrac{[L:E]\cdot[E:K]}{1\cdot[E:K]} = [L:E].$ □

Def: A field K is *perfect* if every algebraic extension L/K is separable.

Ex: . every field of char. 0,
. every algebraically closed field,
. every finite field, and
. every algebraic extension of a perfect field is perfect.

. If $\operatorname{char} K = p > 0$, then $\operatorname{Frac}(K[T])$ is *not* perfect.