4.5 Kummer and Artin-Schreier extensions

<u>Def:</u> A <u>field extension</u> L/K is called a <u>Kummer extension</u> (<u>of degree n</u>) if $\#\mu_n(K)=n$ and L/K is cyclic of degree n.

<u>Thm 1:</u> K field with $\#\mu_n(K)=n$

(1) If L/K is a Kummer extension of degree n, then there is an $a\in L$ with minimal polynomial T^n-b for some $b\in K$ and $L=K(a)$. ("$a=\sqrt[n]{b}$")

(2) If $a\in\bar{K}$ is a root of T^n-b for some $b\in K$, then $K(a)/K$ is a Kummer extension of degree d where $d\mid n$, $c=a^d\in K$ and T^d-c is the minimal polynomial of a over K.

<u>proof:</u> (1) $\mu_n(K)=\langle\zeta_n\rangle$, $Gal(L/K)=\langle\sigma\rangle$

$\Rightarrow N_{L/K}(\zeta_n^{-1})=(\zeta_n^{-1})^n=1$ since $\zeta_n\in K$.

By Thm. 4.4.5 (Hilbert 90), $\exists a\in L$ s.t. $\zeta_n^{-1}=\frac{a}{\sigma(a)}$, i.e. $\sigma(a)=\zeta_n a$.

$\Rightarrow \sigma^i(a)=\zeta_n\sigma^{i-1}(a)=\ldots=\zeta_n^i a$.

Since $a,\zeta_n a,\ldots,\zeta_n^{n-1}a$ are pairwise distinct,

$[K(a):K] \geq n$, i.e. $L = K(a)$. Since

$$\sigma(a^n) = \sigma(a)^n = (\zeta_n a)^n = a^n,$$

$b = a^n \in L^{\langle\sigma\rangle} = K$.

$\Rightarrow$ a is a root of $T^n - b$.

Since $\deg(T^n - b) = [K(a):K]$, $T^n - b$ is the minimal polynomial of a over K.

(2). If a is a root of $f = T^n - b$, then $\zeta_n^i a$ is a root of f for $i = 0 \ldots n-1$.

Thus $f = \prod_{i=1}^{n} (T - \zeta_n^i a)$ decomposes over $K(a)$, i.e. $K(a)$ is the splitting field of f over K $\Rightarrow$ $K(a)/K$ is normal.

Since f is separable, $K(a)/K$ is Galois.

- Let $G = Gal(K(a)/K)$. Then

$$\begin{aligned} \varepsilon: G &\longrightarrow \mu_n(K) \\ \sigma &\longmapsto \zeta_n^i \text{ s.t. } \sigma(a) = \zeta_n^i a \end{aligned}$$

is an injective group homomorphism.

Thus $G = \langle\sigma\rangle$ is cyclic of order $d \mid n$, and $\varepsilon(\sigma) = \zeta_n^i$ for a primitive d-th root of unity ζ_n^i.

$\Rightarrow$ $\sigma(a^d) = \sigma(a)^d = (\zeta_n^i a)^d = a^d$

$\Rightarrow \quad c = a^d \in K(a)^{\langle\sigma\rangle} = K(a)^G = K.$

$\Rightarrow \quad a$ is a root of $g = T^d - c$

Since $\deg g = \# G = [K(a):K]$,
g is the minimal polynomial of a. $\square$

<u>Def:</u> A field extension L/K is an <u>Artin-Schreier extension</u> (<u>of degree p</u>) if $\operatorname{char} K = p$ and if L/K is cyclic of degree p.

<u>Rem:</u> If $\operatorname{char} K = p$, then $\mu_p(K) = \{1\}$.

<u>Thm 2:</u> Let $\operatorname{char} K = p$

(1) If L/K is an Artin-Schreier extension, then there is an $a \in L$ with minimal polynomial $f = T^p - T - b$ over K and $L = K(a)$.

(2) Let $f = T^p - T - b \in K[T]$. Then f is either irreducible or decomposes into linear factors in $K[T]$. If f is irreducible and $a \in \bar{K}$ a root of f, then $K(a)/K$ is an Artin-Schreier extension.

<u>proof:</u> (1) $G = \operatorname{Gal}(L/K) = \langle\sigma\rangle$. Since

$\operatorname{Tr}_{L/K}(-1) = p \cdot (-1) = 0$,

Thm. 4.4.6 ("additive Hilbert 90") shows

that there is an $a \in L$ such that $-1 (= a - \sigma(a))$,
i.e. $\sigma(a) = a + 1$. Thus

$$\sigma^i(a) = \sigma^{i-1}(a) + 1 = \dots = a + i.$$

Since $a, a+1, \dots, a+(p-1)$ are pairwise disinct,
$[K(a):K] \geq p$, which shows that $L = K(a)$. Since

$$\sigma(a^p - a) = \sigma(a)^p - \sigma(a) = (a+1)^p - (a+1) = a^p + 1^p - a - 1 = a^p - a,$$

$b = a^p - a \in L^{\langle\sigma\rangle} = K$. Thus a is a root of
$T^p - T - b$. Since $\deg(T^p - T - b) = p = [K(a):K]$,
$T^p - T - b$ is irreducible and the minimal polynomial
of a.

(2) Let $a \in \bar{K}$ be a root of $f = T^p - T - b$. Then for $i \in \mathbb{F}_p$,

$$f(a+i) = (a+i)^p - (a+i) - b = a^p + \underbrace{i^p}_{(= i \text{ since } \mathbb{F}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z})} - a - i - b = a^p - a - b = 0.$$

$\Rightarrow$ $a, a+1, \dots, a+(p-1)$ are p pairwise distinct
roots of f

$\Rightarrow$ f is separable and splits over $L = K(a)$

Thus if $a \in K$, then f splits over $K = K(a)$.

<u>claim:</u> If $a \notin K$, then f is irreducible over K.

Let $f = gh$ in $K[T]$. Then $g = z \prod_{i \in I} (T - (a+i))$ in $L[T]$
for some $z \in K^\times$, $I \subset \mathbb{F}_p$, and $g = \sum_{i=0}^{d} c_i T^i \in K[T]$
where $d = \# I$ and $c_d = z$.

Then

$$\underbrace{c_{d-1}/\tilde{c}}_{\in K} = -\sum_{i\in I}(a+i) = \underbrace{-da}_{\in L} - \underbrace{\sum_{i\in I} i}_{\in \mathbb{F}_p \subset K},$$

which is in K if and only if $d=0$ or $d=p$. Thus one of g and h is a unit, which proves the claim. ↯

- If f is irreducible over K, then $L = K(a)$ is the splitting field of the separable polynomial f. $\Rightarrow$ L/K is Galois. Since

$$\begin{aligned} \sigma: K(a) &\xrightarrow{\sim} K[T]/(f) \xrightarrow{\sim} K(a+1) = K(a) \\ a &\longmapsto T \longmapsto a+1 \end{aligned}$$

is of order $p = [L:K]$, $\mathrm{Gal}(L/K) = \langle \sigma \rangle$ is cyclic. $\square$