21 March 2024

Recall: **Theorem 7.4.** Let $L:K$ be finite with $L = K(\alpha_1, \dots, \alpha_n)$.

Put $K_0 = K$, and $K_i = K_{i-1}(\alpha_i)$ $(1 \le i \le n)$.

TFAE:

(i) α_i is separable over K_{i-1} for $1 \le i \le n$

(ii) α_i is separable over K for $1 \le i \le n$

(iii) $L : K$ is separable.

Corollary 7.5. Suppose $L:K$ is finite. If $L:K$ is separable, then the number of K-homomorphsims $\sigma : L \to \bar{K}$ is $[L:K]$, and otherwise there are $< [L:K]$ K-homomorphisms.

Proof: Thm 7.3 + Thm 7.4. //

Corollary 7.6 Suppose $f \in K[t] \setminus K$ and $L : K$ is a splitting field extension for f. Then

$L:K$ is separable $\iff$ f is separable over K.

More generally, if $L : K$ is a splitting field extension for $S \subseteq K[t] \setminus K$.

Then

$L : K$ is separable $\iff$ f is separable over K for all $f \in S$.

Proof. Assume $K \subseteq L$.

(i) $L:K$ a splitting field extension for $f \in K[t] \setminus K$.

($\Rightarrow$) f separable over K $\xRightarrow[\text{HW9, Qn 3 (a)}]{}$ $L:K$ separable

($\Leftarrow$) If $L:K$ separable splitting field extension for $f \in K[t] \setminus K$

Then f has algebraic roots over K, and $L:K$ separable, so every root of f is separable over $K \Rightarrow f$ separable. □

(ii) $L:K$ a splitting field extension for $S \subseteq K[t] \setminus K$,

and

($\Rightarrow$) each $f \in S$ is separable over K

$\Longrightarrow$ (HW9, Qn 3(b)) $L:K$ separable.

($\Leftarrow$) If $L:K$ is a splitting field extension for $S \subseteq K[t] \setminus K$ and $L:K$ separable $\Rightarrow$ for each $f \in S$, the roots of f are separable $/K$, so f separable $/K$. □

Theorem 7.7. Suppose $L : M : K$ is a tower of algebraic extensions. Then

$$L : K \text{ separable} \iff L : M \text{ and } M : K \text{ are both separable.}$$

Proof. HW 11, Qn 1 (using primitive element ~~theorem~~)

Theorem 9.1. (Primitive element theorem)

Let $L : K$ be finite and separable with $K \subseteq L$.

Then $L : K$ is a simple extension.

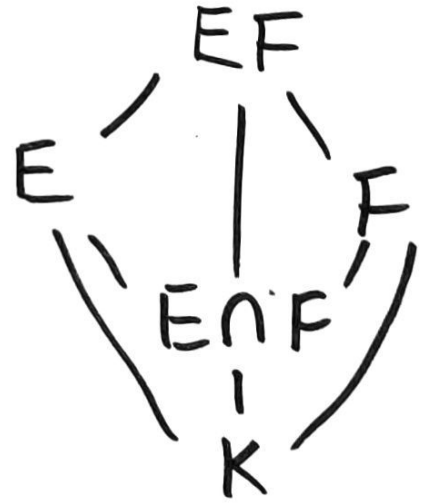
(i.e. there exists $\alpha \in L$ with $L = K(\alpha)$).

Theorem 7.8 Suppose $E:K$ & $F:K$ are finite extensions with $E \subseteq L$ and $F \subseteq L$, where L a field. Then:

(a) $E:K$ separable $\Rightarrow$ $EF:F$ is separable

(b) $E:K$ & $F:K$ both separable

$\Rightarrow$ $EF:K$ and $E \cap F:K$ is separable.



Proof: HW11, Qn2.

§8. Inseparable polynomials, differentiation & Frobenius.

Definition 25: A polynomial $f \in K[t]$ **inseparable** over K if f is **not** separable over K, so f has an irreducible factor $g \in K[t]$ having the property that g has fewer than $\deg g$ distinct roots over $\bar{K}$.

Definition 27. We define **derivative operator** D

$$D : K[t] \longrightarrow K[t]$$

$$\sum_{k=0}^{n} a_k t^k = \sum_{k=1}^{n} k a_k t^{k-1} \qquad (a_k \in K)$$

Properties: For each $f, g \in K[t]$, we have

⑦ $$D(f+g) = Df + Dg$$

$$D(\alpha f) = \alpha\, Df \quad \text{for all } \alpha \in K.$$

Also, $$D(t^m t^n) = (m+n)\,t^{m+n-1} = (Dt^m)t^n + (Dt^n)t^m,$$

so by linearity, $$D(fg) = (Df)g + (Dg)f.$$

<u>Theorem 8.1.</u> Let $f \in K[t] \setminus K$, and let $L : K$ be a splitting field extension for f. Assume $K \subseteq L$.

TFAE:

(i) f has a repeated root over L

(ii) there is an element $\alpha \in L$ such that
$$f(\alpha) = 0 = (Df)(\alpha).$$

(iii) There is some $g \in K[t]$ such that
$\deg g \geq 1$ and $g \mid f$ and $g \mid Df$.

Proof: Qn 1 from HW10. //

Theorem 8.2. Suppose that $f \in K[t]$ is irreducible over K. Then f is inseparable if and only if $\text{char}(K) = p > 0$, and $f \in K[t^p]$, and thus $f = a_0 + a_1 t^p + \dots + a_m t^{mp}$, some $a_i \in K$.

Proof. Let $f \in K[t]$ be irred.

($\Rightarrow$) Suppose f is inseparable over K, and

$$f = a_0 + a_1 t + \dots + a_n t^n, \text{ some } a_i \in K.$$

Then there is a $g \in K[t]$ s.t. $\deg g \geq 1$ and $g \mid f$ and $g \mid Df$.

Thus $f = gh$, some $h \in K[t]$.

But f is irreducible and g is not a unit, so

② h must be a unit (i.e. $h \in K^\times$).

But $g \mid Df$, so $f \mid Df$. Since $\deg f > \deg Df$, we find that $Df = 0$.

Thus

$$0 = Df = a_1 + 2a_2 t + \dots + n a_n t^{n-1},$$

and hence $a_1 = 0,\ 2a_2 = 0, \dots,\ n a_n = 0$.

Then if $\mathrm{char}(K) = 0$, this implies $a_1 = a_2 = \dots = a_n = 0$, so $f \in K$ (i.e. f is constant. ※). So

f is inseparable $\Rightarrow \mathrm{char}(K) = p > 0$. □

But if $\mathrm{char}(K) = p$, and $1 \cdot a_1 = 0,\ 2a_2 = 0, \dots, n a_n = 0$, then a_i can be non-zero only when $p \mid i$.

Hence $f = b_0 + b_1 t^p + b_2 t^{2p} + \dots + b_m t^{mp}$,

where $b_i \in K$, so $f \in K[t^p]$. □

($\Leftarrow$) If $\mathrm{char}(K) = p > 0$ and $f \in K[t^p]$, then $Df = 0$, and by Theorem 8.1, whenever α satisfies $f(\alpha) = 0$ we have $Df(\alpha) = 0$, so f is inseparable over K. □ //

$(a+b)^p = a^p + b^p$ in $\mathrm{char}(K) = p$.

$(a+b+c)^p = a^p + b^p + c^p$.

$= (a+b)^p + c^p =$

$(a_0 + a_1 t + \cdots + a_n t^n)^p = a_0^p + a_1^p t^p + \cdots + a_n^p t^{np}$

$a \in \mathbb{F}_p \Rightarrow a^p = a$

$t \in \mathbb{F}_p(t)$, $\boxed{t^p \neq t}$

The Frobenius map

Definition 28. Suppose $\text{char}(K) = p > 0$. The **Frobenius map**

$$\phi : K \longrightarrow K$$
$$\alpha \longmapsto \alpha^p.$$

(in $\mathbb{F}_p$, $\phi = id$).

Define $\text{Fix}_\phi(K) = \{ \alpha \in K : \phi(\alpha) = \alpha \}$.

$\alpha^p = \alpha$

Theorem 8.4. Suppose $\text{char}(K) = p > 0$, and let F be the prime subfield of K. Let $\phi : K \longrightarrow K$ denote Frobenius. Then ϕ is an injective homomorphism, and $\text{Fix}_\phi(K) = F$.

(12) Proof. One has $\phi(1) = 1$, and when $\alpha, \beta \in K$, then $\phi(\alpha\beta) = (\alpha\beta)^p = \phi(\alpha)\phi(\beta)$, and

$$\phi(\alpha+\beta) = \alpha^p + \beta^p = \phi(\alpha) + \phi(\beta).$$

So ϕ is a homomorphism, so injective, since K is a field. □

Have $F = \{ c \cdot 1_K : c \in \mathbb{Z} \text{ and } 1 \le c \le p \}$,

and $\phi(c \cdot 1_K) = c\,\phi(1_K) = c \cdot 1_K$.

Thus $c \cdot 1_K \in \mathrm{Fix}_\phi(K)$ for $1 \le c \le p$,

so $F \subseteq \mathrm{Fix}_\phi(K)$.

Also, every element α of F satisfies

$$\alpha^p = \phi(\alpha) = \alpha,$$

and hence is a root of $t^p - t$, since this has at most p roots, the fixed field contains no elements

other than those lying in F.

So $F = \mathrm{Fix}_{\phi}(K)$. //