① 19 March 2024

Recall: §7. Separability

Definition. K a field.

(i) irreducible $f \in K[t]$ is separable over K if it has no multiple roots.

(ii) $f \in K[t] \setminus K$ is separable if all of its irreducible factors in $K[t]$ are separable.

(iii) $L:K$ an extension: say $\alpha \in L$ is separable over K when α is algebraic over K and $m_\alpha(K)$ is separable

(iv) $L:K$ is separable when $\alpha \in L$ is separable over K for all α.

Example Let $K = \mathbb{F}_p(y)$ with y transcendental over $\mathbb{F}_p$.

$t^p - y = (t - y^{1/p})^p$

Then $t^p - y$ is not separable over $\mathbb{F}_p(y)$

$\Rightarrow \mathbb{F}_p(y^{\frac{1}{p}}) : \mathbb{F}_p(y)$ is not a separable extension.

"inseparable".

Proposition 4.11 Let $L:K$ be an extension with $K \subseteq L$. Suppose $g \in L[t]$ is irreducible over L, and $g \mid f$ in $L[t]$, where $f \in K[t] \setminus \{0\}$. Then g divides a factor of f that is irreducible over K.

Thus, there exists an irreducible $h \in K[t]$ having the property that $h \mid f$ in $K[t]$, and $g \mid h$ in $L[t]$.

Proof. Assume $K \subseteq L \subseteq \overline{L}$.

Since g irreducible over L, have $\deg(g) \geq 1$.

$\Rightarrow \exists\, \alpha \in \overline{L}$ s.t. $g(\alpha) = 0 \Rightarrow f(\alpha) = 0$, so α algebraic over K, and $\underset{h}{\underset{\shortparallel}{m_\alpha(K)}} \mid f$.

Then h is irreducible over K and $h \mid f$. $\square$

But $h(\alpha)=0$, so $m_\alpha(L) \mid h$

and $g(\alpha)=0$, so $m_\alpha(L) \mid g$, say $g = \lambda m_\alpha(L)$, some $\lambda \in L^\times$. (remember: g is irreducible!)

Hence $g \mid h$ in $L[t]$, as required. $\square$

Proposition 7.1 Suppose $L:M:K$ is a tower of algebraic field extensions. Assume that $K \subseteq M \subseteq L \subseteq \bar{K}$, and $f \in K[t] \setminus K$ is separable over K.

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

- If $g \in M[t] \setminus M$ satisfies $g \mid f$, then g is separable over M
- If $\alpha \in L$ is separable over K, then α is separable over M
- If $L:K$ is separable, then so is $L:M$.

Proof. (of Prop^n 7.1). Assume $f \in K[t] \setminus K$ separable $/K$. Suppose $g \in M[t]$ and $g \mid f$, and let $g_0 \in M[t]$ be an irreducible factor of g. Then $g_0 \mid f$, so Prop^n 4.11 we have $g_0 \mid f_0$ for some irreducible factor of f over K. Then

$$f_0 = g_0 h_0,$$

for some $h_0 \in M[t]$.

Since f_0 is separable, it has $\deg f_0$ distinct roots over $\bar{K}$, and $\deg f_0 = \deg g_0 + \deg h_0$, so by UFD property for $\bar{K}[t]$, we have ~~that~~ g_0 and h_0 must have $\deg g_0$ distinct roots, and $\deg h_0$ distinct roots over $\bar{K}$, respectively. Thus g_0 is separable over $M[t]$. Hence all irred. factors of g are separable over M $\Rightarrow$ g separable over M. $\square$

Suppose $\alpha \in L$ is separable over K. Then α is algebraic over K, and $m_\alpha(K)$ is separable. But $m_\alpha(M) \mid m_\alpha(K)$, so $m_\alpha(M)$ has distinct roots over $\overline{K}$, so is separable.

Then α is separable over M. $\square$

If $L:K$ is separable, then each $\alpha \in L$ is separable over K. By preceding result, each $\alpha \in L$ is also separable over M. Thus $L:M$ is separable. $\square$

Note: <u>Qn 2 HW9.</u>

<u>Proposition 7.2.</u> Suppose $L : M$ is algebraic. Let $\alpha \in L$ and $\sigma : M \longrightarrow \overline{M}$ be a homomorphism. Then $\sigma(m_\alpha(M))$ is separable $\Leftrightarrow$ $m_\alpha(M)$ is separable over M.

$$\begin{tikzcd}
& L \arrow[dl, dash] \arrow[dr, dash] & \\
M \arrow[dr, dash] & & M' \arrow[dl, dash] \\
& K &
\end{tikzcd}$$

Theorem 7.3 Let $L : K$ be finite with $K \subseteq L \subseteq \overline{K}$, so that $L = K(\alpha_1, \dots, \alpha_n)$ for some $\alpha_1, \dots, \alpha_n \in L$. Put $K_0 = K$, and for $1 \leq i \leq n$, set

$$K_i = K_{i-1}(\alpha_i).$$

$$\begin{array}{c} L \\ \| \\ K_n \\ | \\ \vdots \\ | \\ K_1 \\ | \\ K_0 \end{array}$$

Finally, let $\sigma_0 : K \hookrightarrow \overline{K}$ be inclusion mapping.

(i) If α_i is separable over K_{i-1} for $1 \leq i \leq n$, then there are $[L : K]$ ways to extend σ_0 to a homomorphism $\tau : L \longrightarrow \overline{K}$.

(ii) If α_i is not separable over K_{i-1} for some index i, then there are <u>fewer</u> than $[L : K]$ ways to extend σ_0 to a homomorphism $\tau : L \to \overline{K}$.

Proof: First observe if $\tau : L \to \bar{K}$ is a homomorphism extending σ_0, we can put $\sigma_i := \tau|_{K_i}$. Then

$\sigma_i : K_i \to \bar{K}$ is a homomorphism extending σ_{i-1}.

Thus, every homomorphism $\tau : L \to \bar{K}$ corresponds to a sequence of homomorphisms $\sigma_1, \dots, \sigma_n$, where $\sigma_n = \tau$, and $\sigma_i : K_i \to \bar{K}$ extends σ_{i-1} $(1 \leq i \leq n)$

Let j satisfy $1 \leq j \leq n$, and suppose for $1 \leq i < j$ there are homomorphisms $\sigma_i : K_i \to \bar{K}$ having property σ_i extends σ_{i-1}. By Corollary 3.3, the number of ways of extending σ_{j-1} to $\sigma_j : K_j \to \bar{K}$ is equal to the number of distinct roots of $\sigma_{j-1}(m_{\alpha_j}(K_{j-1}))$ ~~that~~

lie in $\overline{K}$.

By Corollary 4.7, this number is equal to the number of distinct roots of $m_{\alpha_j}(K_{j-1})$ that lie in $\overline{K}$. (Note that $\overline{K_j} = \overline{K}$ for all j).

So the number of ways to extend σ_{j-1} to σ_j is equal to $\deg m_{\alpha_j}(K_{j-1}) = [K_j : K_{j-1}]$ if α_j is separable, and is smaller (for sure!) if α_j is not separable.

Then the total number of ways to extend σ_0 to τ is

- $= \underbrace{[K_n : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_2 : K_1]}_{[K_1:K_0]} = \underline{\underline{[L:K]}}$ if each α_j is separable over K_{j-1}
- $< \underbrace{[K_n : K_{n-1}] \cdots [K_2 : K_1]}_{[K_1:K_0]} = [L;K]$ ~~otherwise~~

Theorem 7.4 Let $L:K$ be a finite extension with $L = K(\alpha_1, \dots, \alpha_n)$. Set $K_0 = K$, and for $1 \leq i \leq n$, inductively define $K_i = K_{i-1}(\alpha_i)$. TFAE:

(i) the element α_i is separable over K_{i-1} $(1 \leq i \leq n)$

(ii) the element α_i is separable over K $(1 \leq i \leq n)$

(iii) the extension $L:K$ is separable.

Proof: Suppose $K \subseteq L \subseteq \overline{K}$.

(i) $\Rightarrow$ (iii) Assume (i). Thm 7.3 shows that the number of K-homomorphisms $\tau : L \to \overline{K}$ is equal to $[L:K]$. Let $\beta_1 \in L$. Since $[L:K] < \infty$, so β_1 is algebraic over K, so $L = K(\beta_1, \beta_2, \dots, \beta_m)$, some $\beta_2, \dots, \beta_m \in L$.

Put $K_0' = K$, and $K_j' = K(\beta_1, \dots, \beta_j) = K_{j-1}'(\beta_j)$ $1 \leq j \leq m$.

Then the number of K-homomorphisms $\tau' : K_m' \to \bar{K}$ is $[L:K]$ since $K_m' = L$, so β_1 must be separable over K (since otherwise there are fewer than $[L:K]$ such K-homomorphisms).

Since β_1 is separable over K for all $\beta_1 \in L$,

hence $L : K$ is separable.

This proves (i) $\Rightarrow$ (iii) $\square$

(iii) $\Rightarrow$ (ii) ✓ (defn of separable extn) $\square$

(ii) $\Rightarrow$ (i) Proposition 7.1. $\square$