Separable extensions (Lecture 14)

Df. 1) An irr. polynomial $f \in K[t]$ is separable over K if it has no multiple roots in $\overline{K}$, i.e. $f = c\prod(t-\alpha_j)$, where $\alpha_j \in \overline{K}$ are distinct

2) $f \in K[t]\setminus\{0\}$ is separable over K if its irr. factors are separable

3) $L:K$, $\alpha \in L \Rightarrow \alpha$ is separable over K if α is algebraic over K & μ_α^K is separable.

4) An algebraic extension $L:K$ is a separable extension if $\forall \alpha \in L$ is separable.

Exm $K = \mathbb{F}_p(t)$, $f(x) = x^p - t \in K[t]$, $\deg f = p > 1$

1) Show that f is irr. over K.

Indeed, t is irr. in $\mathbb{F}_p[t]$ (if $t = gh$, $g, h \in \mathbb{F}_p[t]$ $\Rightarrow 1 = \deg g + \deg h \Rightarrow \deg g = 0$ or $\deg h = 0$). Thus by Gauss' lemma t is irr. over $\mathbb{F}_p(t) \Rightarrow$ by Eisenstein's criterion we see that $f(x)$ is irreducible over K.

2) Now we show that is **not** separable.

Indeed, let $f(\alpha) = 0$, $\alpha \in \overline{K} \Rightarrow \alpha^p = t$ and

$$x^p - t = x^p - \alpha^p = x^p + (-1)^p\alpha^p = (x-\alpha)^p$$

(the last holds for $p > 2$; if $p = 2$, then $-\alpha = \alpha$ $\Rightarrow$ the same remains true)

Thus $\mathbb{F}(t^p) - \mathbb{F}(t)$ is inseparable ($\mu_t^{\mathbb{F}(t^p)} = x^p - t^p$)

L.1 $K-M-L$ alg. extensions & $K\subseteq M\subseteq L\subseteq \overline{K}$.
Suppose that $f\in K[t]\setminus K$ is separable over K. If $g\in M[t]\setminus M$ divides f, then g is separable over M.
In particular, if $\alpha\in L$ is separable over K
$\Rightarrow \alpha$ is separable over M
Also, if $K-L$ is separable $\Rightarrow M-L$ is separable

Pf. $g|f$ and let $g_0|f$ is irreducible factor of g over M. By corollary in Lecture 10 $\exists h\in K[t]$, h is irr. over K s.t. 1) $h|f$ in $K[t]$
2) $g_0|h$ in $M[t]$
Thus $f=g_0\varphi$, $\varphi\in M[t] \Rightarrow \deg f = \deg g_0 + \deg\varphi$ & f has $\deg f$ distinct roots in $\overline{K} \Rightarrow g_0$ has $\deg g_0$ distinct roots in $\overline{K} \Rightarrow$ this is true for any irreducible factor of g ($\&\ \overline{M}\cong\overline{K}$)
$\Rightarrow g$ is separable over M.

In particular, $\forall\alpha\in L$, α is separable, we have $\mu_\alpha^M \mid \mu_\alpha^K \Rightarrow \mu_\alpha^M$ is separable over M ($\Leftrightarrow$ α is separable over M) $\blacksquare$

So, $K-M-L \Rightarrow$ I) $K-L$ normal $\Rightarrow M-L$ normal
II) $K-L$ separable $\Rightarrow M-L$ separable
(clearly, $K-M$ normal & separable)
Later we prove that $K-L$ sep. $\Leftrightarrow$ $K-M$ & $M-L$ sep

L.2. 1) $K - L$ algebraic, $\alpha \in L$ & $\sigma : K \to \overline{K}$ be a homomorphism $\Rightarrow$ μ_α^K is separable over K iff $\sigma(\mu_\alpha^K)$ is separable over $\sigma(K)$

(thus separability is preserved under homomorphisms)

2) Let $L:K$ is a splitting field for $f \in K[t]$. If f is separable, then $L:K$ is separable.

(this is an exercise. Hint: use Thm. 1' below).

Thm 1. $K - L - \overline{K}$, $L = K(\alpha_1, \dots, \alpha_n)$, where $\alpha_j \in L$ and $\sigma_0 : K \to \overline{K}$ the inclusion map. Put $K_0 = K$, $K_i = K_{i-1}(\alpha_i)$

1) If α_i is separable over K_{i-1}, $i = 1, \dots, n$, then $\exists\ [L:K]$ ways to extend σ_0 to a hom. $\tau : L \to \overline{K}$

2) If α_i is not separable over K_{i-1} $\Rightarrow$ $\exists$ $< [L:K]$ ways to extend σ_0 to a hom. $\tau : L \to K$

Pf. Put $\sigma_i = \tau|_{K_i}$ $\Rightarrow$ τ corresponds to a sequence of hom. $\sigma_1, \dots, \sigma_n = \tau$ and each σ_i extends σ_{i-1}. We know that # ways to extend σ_{i-1} is # of distinct roots of $\sigma_{i-1}(\mu_{\alpha_i}^{K_{i-1}})$ in $\overline{K}$ $=$ # of distinct roots of $\mu_{\alpha_i}^{K_{i-1}}$ in $\overline{K}$ $\Rightarrow$ # ways to extend σ_{i-1} $\overset{=}{\leq}$ $[K_i : K_{i-1}]$ if α_i is separable over K_{i-1} and smaller otherwise. ∎

Thm 1'. Let $K - L = K(\alpha_1, \dots, \alpha_n)$ & define $K_i = K_{i-1}(\alpha_i)$ as above. Then the following equivalent

1) $\forall \alpha_i$ is separable over K_{i-1}, $1 \le i \le n$
2) $\forall \alpha_i$ ——— " ——— K, $1 \le i \le n$
3) $L:K$ is separable.

Pf. In veiw of Lemma 1 it is enough to prove that 1) $\Rightarrow$ 3). We know that # K-hom. $\tau: L \to \overline{K}$ is $[L:K]$. Take $\forall \beta \in L$ $\Rightarrow \beta$ is alg. over K and $L = K(\beta, \beta_2, \dots, \beta_m)$. As above put $K_0' = K$ & $K_j' = K_{j-1}'(\beta_j)$. We claim that β must be separable over K (otherwise # K-hom. $\tau: L \to \overline{K}$ is $< [L:K]$) We took any $\beta \Rightarrow L:K$ is separable ∎

Cor. 1. $L:K$ is finite. If it is a separable $\Rightarrow$ # K-hom. $\sigma: L \to \overline{K}$ is $[L:K]$ (and $< [L:K]$ otherwise)

Cor. 2. Let $K - L$ and L is a splitting field extension for f. Then $L:K$ is separable iff f is separable over K (exercise: use Lemma 2, part (2) above).

To prove that $K - M - L$:
$K - L$ is separable $\Leftrightarrow$ $K - M$ & $M - L$ are separable

it is useful to have in mind the primitive element theorem ($[L:K]<\infty$ & $L:K$ is separable $\Rightarrow$ $L:K$ is a simple ext.)
We will prove this theorem next time.