

Goal: We aim to show that in a tower $E/K/F$,

E/K sep. + K/F sep. $\Rightarrow E/F$ sep.

The "natural" way to study this is via embeddings.

Defn E/F finite. The separable degree, $[E:F]_s$,

is the number of distinct embeddings $E \hookrightarrow \bar{F}$ fixing F .

Thm: $E \supseteq K \supseteq F$, E/F finite. Then

$$[E:F]_s = [E:K]_s \cdot [K:F]_s.$$

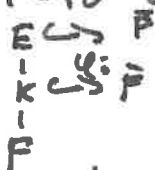
Pf: Set $[K:F]_s =: m$, $[E:K]_s =: n$.

Let ψ_1, \dots, ψ_m be the embeddings of $K \hookrightarrow \bar{F}$ over F ,

$\varphi_1, \dots, \varphi_n$ the embeddings of $E \hookrightarrow \bar{F}$ over K .

Let Ω_0 be a splitting field over F containing \bar{F} .

Fix a ψ_i .



Claim: The number of embeddings of E into \bar{F} over F restricting to ψ_i over K is n .

Pf: Use our extⁿ theorem (13.4, Th^m 27 in D-F) to extend ψ_i to $\tilde{\psi}_i: \Omega_0 \rightarrow \Omega_0$.

This is possible as Ω_0 is a splitting field of $f \in F[X]$ so it's also a splitting field of f over K and $\psi_i(K)$.

Clearly, $\tilde{\psi}_i: \Omega_0 \hookrightarrow \Omega_0$ is injective.

Look at Defn $\tilde{\psi}_i^{-1} \circ \psi_i: E \rightarrow \bar{F}$.

Now $\mathbb{F}_1 \subseteq K = \text{id}_K$: if $x \in K$, $\tau(x) = \varphi_i(x)$

by assumption $\Rightarrow \varphi_i(\tau(x)) = \varphi_i(x)$

Thus, $\varphi_i \circ \tau$ is an embedding of E fixing K

$\Rightarrow \varphi_i \circ \tau = \tau_j$ for some j .

Therefore, $\tau = \varphi_i^{-1} \circ \tau_j$ for some j ,

so there are exactly n possible τ . \square

We now count embeddings $\tau: E \hookrightarrow \bar{F}$:

For each $i = 1, \dots, m$, there are exactly n extending φ_i , giving mn total.

Thus, $[E:F]_s = mn = [E:K]_s \cdot [K:F]_s$. \square

Theorem 2: If $E = F(\alpha)$, $\alpha \in E$ a root of an irred. poly. $f \in F[x]$. Then $[E:F]_s$ is the # of distinct roots of f .

Since $[E:F] = \deg(f)$, we have

$[E:F]_s \leq [E:F]$, with equality iff f is separable.

Prf: Assume WLOG f is monic. Let $n = \deg(f)$,

write $f(x) = \prod_{i=1}^n (x - \alpha_i)$.

By Thm 3.1, $\forall i$, \exists embedding

$\varphi_i: F(\alpha) \hookrightarrow \bar{F}$ with $\varphi_i(\alpha) = \alpha_i$. \square

Moreover, if $\varphi: F(\alpha) \hookrightarrow \bar{F}$ is any embedding,
 it sends α to some α_i , so $\varphi = \varphi_i$ for some i .

Also, $\varphi_i = \varphi_j \Leftrightarrow \alpha_i = \alpha_j$. Thus, $[E:F]_s = \# \text{ distinct } \varphi_i$
 $= \# \text{ distinct } \alpha_j$ \square

Th^m 3: For any finite extension E/F ,

$$[E:F]_s \leq [E:F].$$

PF: We just did the case of a simple extension α Th^m 2

Generally: say $E = F(\alpha_1, \dots, \alpha_n)$. Do a tower
 of simple ext^s $F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2) \subseteq \dots \subseteq E$

Now each $[F(\alpha_1, \dots, \alpha_k) : F(\alpha_1, \dots, \alpha_{k-1})]_s \leq [F(\alpha_1, \dots, \alpha_k) : F(\alpha_1, \dots, \alpha_{k-1})]$
 Multiplying these inequalities gives the result \square

Finally, we obtain: define E/F is separable $\Leftrightarrow [E:F]_s = [E:F]$

Th^m 4: $E \supseteq K \supseteq F$ finite ext^s. Then

$$E/F \text{ sep.} \Leftrightarrow E/K \text{ and } K/F \text{ sq.}$$

PF: we write $[E:K]_s [K:F]_s = [E:F]_s \leq [E:F]$

Thus, $[E:F]_s = [E:F] \Leftrightarrow$ both $[E:K]_s = [E:K]$
 and $[K:F]_s = [K:F]$ \square

For completeness, we connect to the book's defn of separable:

Th^m E/F finite. Then E/F is sep. (w/ above defn) iff every $\alpha \in E$ is a root of a sep. poly in $F[x]$.

PA If E/F sep., then Th^m 4

$\Rightarrow F(\alpha)/F$ is sep. $\forall \alpha \in E$, and Th^m 2
 $\Rightarrow \alpha$ is a root of a separable poly.

Conversely, suppose all $\alpha \in E$ are roots of sep. polys.

To show E/F is separable, we induct on degree.

If $n=1$, $E=F$, and it's clear. $n := [E:F]$.

If $n > 1$, assume true \forall exts of degree $< n$.

For $\alpha \in E \setminus F$, let $K = F(\alpha)$.

As α is a root of a sep. poly. $/F$, Th^m 2

$\Rightarrow F(\alpha)/F$ is sep. To use Th^m 4, we

have to show E/K is sep. Every elt of E

is a root of a sep. poly $/F$, hence over K too.

As $[E:K] < [E:F]$, by the induction hypothesis

E/K is separable, as required. 14