4-23-25 (WEEK 10) Shun/翔海 (@shun4midx)

SEPARABLE EXTENSIONS

RECALL

Given $f(x)\in K[x]$, L/K, L'/K: splitting fields for $f(x)$ over K, $\sigma: L \xrightarrow{\sim} L'$ which fixes K,
If $f(x)=(x-\alpha_1)^{n_1}\cdots(x-\alpha_s)^{n_s}$ with $\alpha_i\in L$, then $f(x)=(x-\sigma(\alpha_1))^{n_1}\cdots(x-\sigma(\alpha_s))^{n_s}$

If $n_i=1$, then α_i is called a simple root in $L \Rightarrow \sigma(\alpha_i)$ is also a simple root in L'
If $n_i>1$, then α_i is called a multiple root in $L\Rightarrow\sigma(\alpha_i)$ is also a multiple root in L'

DEFINITION

- A polynomial $f(x)\in K[x]$ is said to be separable over K if its factors have no multiple root in a splitting field L over K
- If $f(x)=a_nx^n+\ldots+a_0$, then $f'(x)=na_nx^{n-1}+\ldots+a_1$

CRITERION

Let $f(x)$ be a monic poly of positive degree in $K[x]$.
Then, all roots of $f(x)$ in a splitting field are simple $\Leftrightarrow \underbrace{(f,f')}_{\text{gcd}}=1$

Proof

"$\Rightarrow$": We can write $f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$, $\alpha_1,\ldots,\alpha_n$ distinct
Then, $f'(x)=\sum_{i=1}^{n}(x-\alpha_1)\cdots\widehat{(x-\alpha_i)}\cdots(x-\alpha_n)\Rightarrow (x-\alpha_i)\nmid f'(x)\ \forall i$
$\therefore (f(x),f'(x))=1$ ✓

"$\Leftarrow$": Suppose $f(x)$ has a multiple root α, so $f(x)=(x-\alpha)^kg(x)$, $k>1$
Then, $f'(x)=k(x-\alpha)^{k-1}g(x)+(x-\alpha)^kg'(x)\Rightarrow(x-\alpha)\mid f'(x)\Rightarrow(x-\alpha)\mid(f',f)$ —✗—

REMARK

TFAE

(1) α is a multiple root of f
(2) α is a common root of $f(x)$ and $f'(x)$
(3) $m_{\alpha,K}\mid f(x)$ and $m_{\alpha,K}\mid f'(x)$

PROPOSITION 1

Any irr poly $f(x)$ is not separable over K iff $\operatorname{char}K=p>0$ and $f(x)=g(x^p)$ for some $g\in K[x]$

separable $\not\Rightarrow$ irr

Proof

"$\Rightarrow$": Let L be a splitting field for f over K and $\alpha\in L$ be a multiple root of $f(x)$. Then, $m_{\alpha,K}\mid f$, $m_{\alpha,K}\mid f'$
$\because f$ is irr $\therefore f\sim m_{\alpha,K}$, i.e. $\deg m_{\alpha,K}=\deg f$

Now, $\begin{cases} m_{\alpha,K}\mid f' \\ \deg m_{\alpha,K}>\deg f' \end{cases}\Rightarrow f'\equiv 0$

If $\operatorname{char}K=0$, then $f=c\in K$ —✗—
$\therefore$ We must have $\operatorname{char}K=p>0$. Let $f(x)=b_0+b_1x+\ldots+b_mx^m$
Here, $f'(x)\equiv 0\Rightarrow ib_i=0\ \forall i=1,\ldots,m$, if $b_i\neq0$, then $p\mid i$
That is, $f(x)=b_0+b_px^p+b_{2p}x^{2p}+\ldots+b_{np}x^{np}=g(x^p)$, where $g(x)=b_0+b_px+b_{2p}x^2+\ldots+b_{np}x^n$ ✓

"$\Leftarrow$": $f'(x)\equiv0\Rightarrow$ if $m_{\alpha,K}\mid f$, then $m_{\alpha,K}\mid f'\Rightarrow\alpha$ is a multiple root of $f(x)$

REMARK

f is irr $\Rightarrow g$ is irr and not all b_i are in K^p

Proof

- If $g=g_1g_2$, then $f(x)=g(x^p)=g_1(x^p)g_2(x^p)$ —✗—
- If $\forall i$, $b_i=a_i^p$ for some $a_i\in K$, then $f(x)=a_0^p+a_p^px^p+\ldots+a_{np}^px^{np}=(a_0+a_px+\ldots+a_{np}x^n)^p$ —✗— $(x+y)^p=x^p+y^p$

Shun/翔海 (@shun4midx)

DEFINITION

- A field of char p is said to be perfect if $K=K^p$
- A field of char 0 is also said to be perfect

COROLLARY

K is perfect $\Leftrightarrow$ every polynomial in $K[x]$ is separable

Proof

"$\Rightarrow$": By prop 1, if char $K=0$, then all irr poly are separable
if char $K=p$, then $K=K^p \Rightarrow \nexists\, g$ in prop 1 $\Rightarrow$ all irr poly are separable

"$\Leftarrow$": If char $K=p>0$ and $K^p \subsetneq K$, then take $b\in K\setminus K^p \Rightarrow x^p-b$ is inseparable over K
↳ Proof x^p-b is irr: $x^p-b=g(x)h(x)$ in $K[x]$ with monic $g(x)$ and $1\leq \deg g=k\leq p-1$
Let L be a splitting field for x^p-b over K and $\alpha\in L$ with $\alpha^p=b$
Then, $x^p-\alpha^p=(x-\alpha)^p$ and $g(x)=(x-\alpha)^k$ in $L[x] \Rightarrow \alpha^k\in K$. As $\alpha^p\in K$, thus $\alpha\in K \Rightarrow b=\alpha^p\in K^p$ $\times$

PROPOSITION 2

Let char $K=p$ and $\phi: K\longrightarrow K$, $\alpha\longmapsto\alpha^p$ be the Frobenius monomorphism. If $K/\overset{\mathbb{Z}/p\mathbb{Z}}{\mathbb{F}_p}$ is algebraic, then ϕ is an automorphism, i.e. $K=K^p$

In particular, any finite field is perfect

DEFINITION

- $\alpha\in L$ is said to be separable over K if $m_{\alpha,K}$ is separable
- L/K is separable if $\forall\alpha\in L$, α is separable over K

PROPOSITION 3

Let $[L:K]=d$ and $\tau: K\to L'$ be a nontrivial homo. If L/K is separable and $\forall\alpha\in L$, $\bar{\tau}(m_{\alpha,K})$ splits over L', then $\exists$ exactly d extensions $\sigma: L\to L'$ of τ. Otherwise, $\exists\, r<d$ such extensions.

Proof sketch

- $m_{\alpha,K}$ is separable $\Rightarrow \bar{\tau}(m_{\alpha,K})$ is separable
- By induction on d, $d=1\Rightarrow \sigma=\tau$.
  $d>1$: $\alpha\in L\setminus K \Rightarrow \exists$ exactly $[K(\alpha):K]$ extensions $\tau_1: K(\alpha)\to L'$
  (Otherwise, pick α s.t. it's inseparable. Then, $\exists <[K(\alpha):K]$ extensions)
- L/K is separable $\Rightarrow L/K(\alpha)$ is separable ($\forall\beta\in L$, $m_{\beta,K(\alpha)} \mid m_{\beta,K}$)
  $\Rightarrow$ By induction hypothesis, $\exists$ exactly $[L:L(\alpha)]$ extensions σ of τ_1, so in total, $\exists$ exactly $\overset{\tau_1\to\sigma}{[L:K(\alpha)]}\overset{\tau\to\tau_1}{[K(\alpha):K]}$ exts of τ.
  (otherwise, $\leq$)

PROPOSITION 4

If $K(\alpha_1,\dots,\alpha_n)/K$ is alg and L is a splitting field for $f(x)=m_{\alpha_1,K}\dots m_{\alpha_n,K}$ over K, then $\forall\beta\in K(\alpha_1,\dots,\alpha_n)$, $m_{\beta,K}$ also splits over L

Proof

$\because m_{\beta,K}\in K[x]\subseteq L[x]$ $\therefore$ We can take $\Sigma\ni r$, a root of $m_{\beta,K}$, as a splitting field of $m_{\beta,K}$ over L

We also write $L=K(R)$, where $R=$ the set of all roots of $f(x)$

So,

$$\begin{tikzcd}
K(R) \arrow[r, "\exists\,\cong"', "\sigma"] & K(R,r) \\
K(\beta) \arrow[u] \arrow[r, "\tau_1", "\sim"'] & K(r) \arrow[u] \\
& K \arrow[ul] \arrow[u]
\end{tikzcd}$$

splitting field for $f(x)$ over $K(\beta)$ → $K(R)$

a splitting field for $f(x)=\bar{\tau}_1(f(x))$ over $K(r)$ → $K(R,r)$

Now, $[K(R):K]=[K(R):K(\beta)][K(\beta):K]$
$=[K(R,r):K(r)][K(r):K]$
$=[K(R,r):K]$

$\therefore K(R)=K(R,r)$, i.e. $r\in K(R)$ $\square$

PROPOSITION 5

Given $K(\alpha_1,\dots,\alpha_n)/K$, if α_i is separable over $K(\alpha_1,\dots,\alpha_{i-1})=K_{i-1}$, then $K(\alpha_1,\dots,\alpha_n)/K$ is separable

Proof

Let L be a splitting field of $f(x)=m_{\alpha_1,K}\cdots m_{\alpha_n,K}$ over K. Observe that $\exists\ [\underbrace{K(\alpha_1)}_{=K_1}:K]$ extensions $\tau_1: K(\alpha_1)\longrightarrow L$ of $id: K\to K$ and $\exists\ [K(\alpha_1,\alpha_2):K(\alpha_1)]$ extensions $\tau_2: K(\alpha_1,\alpha_2)\longrightarrow L$ of $\tau_1: K_1\to L$

Continue, then $\exists\ [K(\alpha_1,\dots,\alpha_n):K_{n-1}]$ extensions $\tau_n: K_n\to L$ of $\tau_{n-1}: K_{n-1}\to L$

$\therefore$ In total, $\exists\ [K(\alpha_1,\dots,\alpha_n):K_{n-1}]\cdots[K_1:K]=[K_n:K]$ extensions $\sigma: K_n\to L$

By prop 4, $\forall\beta\in K(\alpha_1,\dots,\alpha_n)$, $m_{\beta,K}$ splits over L. $\therefore$ By prop 3, $K(\alpha_1,\dots,\alpha_n)/K$ is separable

COROLLARY

M/K is separable $\Leftrightarrow$ M/L, L/K are separable

Proof

"$\Rightarrow$": OK

"$\Leftarrow$": $\forall\alpha\in M$, α is separable for some $\underbrace{K(a_1,\dots,a_m)}_{\text{coef of } m_{\alpha,L}}\leq L$

By prop 5, $K(a_1,\dots,a_m)/K$ is separable $\square$