L20 课上笔记

在L20均假设所在域 char=0.

注意. char=0 ⇒ infinite field, 但 infinite field 可以 char=p (char 只有0或p)

例1: $\mathbb{F}_p \times \mathbb{F}_p \times \cdots \mathbb{F}_p \times \cdots$ 无限次直积

例2: $\mathbb{F}_p(x)=\{\frac{f}{g}: f,g\in\mathbb{F}_p[x], g\neq 0\}$, 多项式环上的分式域

char 的定义是 minimal n s.t. $\underbrace{1+1+\cdots 1}_{n\text{-times}}=0$, $\mathbb{F}_p\subseteq\mathbb{F}_p(x)$ ∴ $char(\mathbb{F}_p(x))=p$

在 char=0, char=p 的 finite field 中: irreducible ⇒ separable, (参考 P121); it's not necessarily holds if $char(\mathbb{F})=p$, $\mathbb{F}$ infinite in 例1

corollary: algebraic extension E/F is finite normal ⇔ E是 splitting field of f(x) over $\mathbb{F}$, $f\in\mathbb{F}[x]$

"⇐" L19最后证了 splitting field over $\mathbb{F}$, 必然是$\mathbb{F}$的 finite normal 扩张

"⇒" E/F finite ⇔ E/F is algebraic extension

设 $E=\mathbb{F}(a_1,a_2,\cdots a_n)$

$m_{a_i\mathbb{F}}$ is irr in $\mathbb{F}[x]$, 由于 E/F normal, $m_{a_i\mathbb{F}}$ 所有 root 均在E中

$f(x)=m_{a_1\mathbb{F}}\times m_{a_2\mathbb{F}}\times\cdots m_{a_n\mathbb{F}}$

∴ E is splitting field of f(x) over $\mathbb{F}$, (易证)

例3: $f(x)=x^3-2\in\mathbb{Q}[x]$, root: $a, a\omega, a\omega^2$

$\mathbb{Q}(a)$ is algebraic, 但 $m_{a\mathbb{Q}}=f(x)$ 含有其它不在$\mathbb{F}=\mathbb{Q}$中的 root

∴ $\mathbb{Q}(a)$ is algebraic extension, 但做不到 normal

fix: $\sigma(L)=L$, 不是 pointwise

lem1: field $\mathbb{F}\subseteq L\subseteq E$, L is a field fixed by $Gal(E/\mathbb{F})$ ⇔ $Gal(E/L)\triangleleft Gal(E/\mathbb{F})$

"⇒" $\sigma\in Gal(E/\mathbb{F})$ $\sigma: E\to E$ $\sigma(a)=a$ $\forall a\in\mathbb{F}$

$\sigma(L)=L$, ∴ σ induces an automorphism of L;

$Gal(E/F)$ act on L natraully, 且 the kernel of this action is $Gal(E/L)$

∴ $Gal(E/L)\triangleleft Gal(E/\mathbb{F})$

recall: group action: G act on H, 右乘

$\varphi: G\to\hat{G}$

$g\to\hat{g}: H\to H$

$h\to hg$

act on: 先通过一个任意 map, 把群G转换为H上的映射, 如G与$\hat{G}$, 再用这个以G生成的映射$\hat{G}$对H作用

⇒ 此处类比写成:

$\varphi: Gal(E/F)\to Gal(E/F)$

$\sigma\to\varphi(\sigma)=\sigma|_L: L\to L$

$l\mapsto\varphi(\sigma)(l)=l$

φ只要是 map 即可, φ: group → 某个 group action, 不用 homo 之类

$\ker\varphi=\{\sigma\in Gal(E/\mathbb{F}): \varphi(\sigma)=\sigma|_L=id\}\triangleleft Gal(E/\mathbb{F})$ 易证成立的

⇐ 设 $Gal(E/L) \lhd Gal(E/F)$

记 $Gal(E/L) =: H$, $\sigma \in Gal(E/F)$ then:

$E^{\sigma H \sigma^{-1}} = \sigma(E^H) = \sigma(L)$; $E^{\sigma H \sigma^{-1}} = E^H = L$ since $H \lhd Gal(E/F)$ --- (*)

即 $\sigma(L) = L \ \forall \sigma \in Gal(E/F)$

(*) ... 《抽》P127 Thm2. 设 K/F is finite Galois extension ($\Leftrightarrow$ finite separable & normal)

‖

def: K中每个元素α, $m_{\alpha,F}$ is separable, 即只有一重根

(1): K/F的中间域集$\{L: K \supseteq L \supseteq F\}$与$Gal(K/F)$的子群集$\{H: H \leq Gal(K/F)\}$之间存在一一映射

first: ①: $K \supseteq L \supseteq F$, $K^{Gal(K/L)} = L$

②: $H \leq Gal(K/F)$, $H \subseteq Gal(K/K^H)$, 在K/F finite 时, H是$Gal(K/K^H)$的闭子群, 所以换成"="

设 $\sigma \in Gal(K/K^H)$, σ fix K^H pointwise

即 $\forall x \in K^H$, x fixed by H, then x should be fixed by σ $\Rightarrow \sigma \in H$ 这是有前提的

考虑: $\varphi^{-1}: \{L\} \to Gal(K/L)$ +②; 这也可以说明$Gal(K/L)$的每个子群均有$Gal(K/L)$的形式 ...(**)

$\varphi: K^H \leftarrow H$

K^H is closed under "+","×"; $K^H \leq K$, 且存在unity. $\forall x \neq 0$ $x^{-1} \in K^H$ ∴ K^H is field

$\forall L \leq K$, let $H = Gal(K/L)$, $K^H = L$ by ①, ∴ φ surjective. 这一条在infinite Galois扩张也成立

设 $H_1 \neq H_2$, 由②知 $H = Gal(K/K^H)$, then $K^{H_1} \neq K^{H_2}$ ∴ φ injective 这条只在finite…成立

$\Rightarrow$ $\{L: K \supseteq L \supseteq F\}$ 与 $\{H: H \leq Gal(K/F)\}$ 间存在一一映射 $H \to K^H$

(2): $H \lhd Gal(K/F) \Leftrightarrow K^H/F$ is normal extension (finite前提下)

lem: $F \subseteq L \subseteq K$, L is fixed by $Gal(K/F) \Leftrightarrow Gal(K/L) \lhd Gal(K/F)$

(1)(**)说明 $H \leq Gal(K/F)$, 则H具有$Gal(K/L)$形式.

故(2)等价于 $Gal(K/L) \lhd Gal(K/F) \Leftrightarrow L/F$ is normal extension $\Leftrightarrow L$ is fixed by $Gal(K/F)$

在HW12 T3证过这个 ⇕ "L/F is splitting extension since "finite""

(3): $\forall \sigma \in Gal(K/F)$, $K^{\sigma H \sigma^{-1}} = \sigma(K^H)$

设 $x \in K^{\sigma H \sigma^{-1}} = \{z \in K: \sigma h \sigma^{-1}(z) = z\}$; $\sigma H \sigma^{-1}(x) = x$ 即 $\sigma h \sigma^{-1}(x) = x \ \forall h \in H$

∴ $\sigma^{-1} \sigma h \sigma^{-1}(x) = \sigma^{-1}(x)$, $\sigma^{-1}(x) \in K^H$ and $x \in \sigma(K^H)$ $\Rightarrow$ LHS $\subseteq$ RHS

设 $x \in \sigma(K^H) = \{z \in \sigma(K): H(\sigma^{-1}(z)) = \sigma^{-1}(z)\}$; $H \cdot \sigma^{-1}(x) = \sigma^{-1}(x)$

∴ $\sigma H \sigma^{-1}(x) = \sigma \cdot \sigma^{-1}(x) = x$; then $x \in K^{\sigma H \sigma^{-1}}$ $\Rightarrow$ LHS $\supseteq$ RHS

以上定理和lemma的证明顺序是(1),(3) → lemma → (2); (1)(3)不存在因果关系

Rmk: (2): 在finite extension前提下: L/F is normal extension $\Leftrightarrow L/F$ is splitting extension

$\overset{HW12}{\Leftrightarrow}$ L fixed by $Gal(K/F)$ set-wise

$\overset{lem}{\Leftrightarrow}$ $Gal(K/L) \lhd Gal(K/F)$

《选》P117. Th2.8 E/F is finite normal extension, L/E 是任意 extension
then any F automorphism of L stablizes E, 即 $\sigma(E)=E$

$F \xrightarrow{f \text{ splitting}} E \to L$

proof: E/F finite normal $\Leftrightarrow$ E is splitting of $f(x)$ over F, $f\in F[x]$

σ is F-auto of L; $\sigma: L\to L$
$\sigma(a)=a\ \forall a\in F$

$\therefore \sigma(f)=f\ \forall f\in F[x]$, σ permutes root of $f(x)$

$E=F(a_1,\dots a_n)$ a_i为$f(x)$的root

$\sigma(F)=F$, $\sigma(a_1,\dots a_n)=(a_1,\dots a_n)$ $\therefore \sigma(E)=E$

P123. Prop 3.14. 设K/F is finite, $K=F(a_1,a_2\dots a_n)$, $g_i(x)=m_{a_i,F}\ \forall i$; $g=\prod_{i=1}^n g_i(x)$, E is splitting field of g over F

then: K/F is separable $\Leftrightarrow$ $|F\text{-embedding of } K \text{ to } E|=[K:F]$

F; $a_1\dots a_n$: $F \to K$; split g: $F \to E$

proof: 设$K_i=F(a_1,\dots a_i)$; $|F\text{-embedding of } K_i \text{ to } E|=n_i$

实际上有 $n_i\le[K_i:F]\ \forall i$, "=" holds iff K_i/F separable

induction: $i=1$时 obv

σ是F-embedding of K_{i-1} to E, $\sigma: K_{i-1}=F(a_1,\dots a_{i-1})\to E$, $\sigma(a)=a\ \forall a\in F$

在σ基础上, let $\tau: K_i=F(a_1\dots a_{i-1},a_i)\to E$, $\tau(a)=a$, $\forall a\in F$

from Th2.8, $g_j(x)\in F[x]$, σ,τ fix F pointwise $\therefore$ permute $\prod_{j=1}^i g_j(x)$ 的root

设$\prod_{j=1}^i g_j(x)$解集为$\{a_1,\dots a_i,\beta_1\dots\beta_t,\gamma_1\dots\gamma_m\}$, $\prod_{j=1}^{i-1} g_j(x)$解集为$\{a_1,\dots a_{i-1},\beta_1,\dots\beta_t\}$

注意: 数学归纳法中使用了$\sigma\to\tau$的lift automorphism; 即: $\tau|_{K_{i-1}}=\sigma$

$\therefore \tau(a_1\dots a_{i-1})=\sigma(a_1\dots a_{i-1})$ 有 n_{i-1}种可能; since τ permutes $\prod_{j=1}^i g_j(x)$ 的 root

$\tau(a_i)=$ $g_i(x)$ root 的其中一个, 有 n_i'种

(*): $n_i'\le g_i(x)$根的个数 $=\deg g_i(x)=[K_i:K_{i-1}]$

$\therefore n_i=n_{i-1}\times n_i'\le[K_{i-1}:F]\times[K_i:K_{i-1}]=[K_i:F]$, induction成立 ... ①

iff K/F separable:

(*)写"≤"原因:
- 多重根 $\Leftarrow$ $\forall a\in K$: $m_{a,F}$ separable; $m_{a,F}=(x-a_1)(x-a_2)\cdots(x-a_n)$ $a_i\ne a_j$
- other roots not in F $\Leftarrow$ splitting field 必 normal, $a\in K$, $\therefore$ 其它root也在K

这里解决的是重根, 本题的g_i irr, $\therefore g_i$所有root均在K中 ... ②

①+② K/F is finite algebraic extension, E/F is splitting extension of $\prod_{i=1}^n m_{a_i,F}$

则$[F\text{-embedding of } K \text{ to } E]\le[K:F]$, iff K/F separable, 取等号

prop5: $f(x)\in F[x]$, E is splitting field of $f(x)$ over F, then $|Aut(E/F)|\le[E:F]$

iff $f(x)$ separable, $|Aut(E/F)|=[E:F]$

proof: $E=F(a_1,a_2\dots a_n)$, a_i是$f(x)$的root; 和上面的定理一样使用 induction 和 lift automorphism,

其中"≤"因为重根, (f的根均在E中)