L8: Simple extension
{ splitting field

α,β algebraic over $\mathbb{F}$

Lem1: char $\mathbb{F}=0$, $E=\mathbb{F}(\alpha,\beta)$, then $\exists\gamma$ s.t. $\gamma\in E$, $E=\mathbb{F}(\gamma)$

即 char $\mathbb{F}=0$ 时，$\mathbb{F}(\alpha,\beta)$ 可以用 $\mathbb{F}(\gamma)$, $\gamma\in\mathbb{F}(\alpha,\beta)$ 代替，∴是 simple extension

proof: 设 $f(x)=m_{\alpha,\mathbb{F}}$, $g(x)=m_{\beta,\mathbb{F}}$, $\gamma=\alpha+c\beta$, some $c\in\mathbb{F}$

设 $h(x)=f(\gamma-cx)$, $h(\beta)=f(\gamma-c\beta)=f(\alpha)=0$

$c\in\mathbb{F}\subseteq\mathbb{F}(\gamma)$, $\gamma\in\mathbb{F}(\gamma)$ ∴ $h(x)=f(\gamma-cx)\in\mathbb{F}(\gamma)[x]$，$f$ irr over $\mathbb{F}$, ∴ h 也 irr over $\mathbb{F}$

由上，$h(\beta)=g(\beta)=0$

h,g irreducible over $\mathbb{F}$, char$(\mathbb{F})=0$, ∴ h,g 均 separable 且有单因子

∴ $\gcd(h(x),g(x))=(x-\beta_1)(x-\beta_2)\cdots(x-\beta_r)$, β_i 为共同 root. $\beta_i\neq\beta_j$ ($i\neq j$)

① β 是唯一 common root 是在 h,g 的分裂域上的 gcd

$\exists s(x),t(x)$: $sh+tg=x-\beta$ ∴ s 和 $t\in\mathbb{K}[x]$，$\mathbb{K}$ = splitting field of h & g over $\mathbb{F}$

(分裂域[x])

∴ $x-\beta\in\mathbb{F}(\gamma)[x]$; $\beta\in\mathbb{F}(\gamma)$, $\alpha=\gamma-c\beta\in\mathbb{F}(\gamma)$; 即 $\mathbb{F}(\alpha,\beta)\subseteq\mathbb{F}(\gamma)$, thus $\mathbb{F}(\gamma)=\mathbb{F}(\alpha,\beta)$

②: 若还有其它 root,（考虑2个）β' 和 β

$0=h(\beta')=f(\gamma-c\beta')=f(\alpha+c(\beta-\beta'))=0$

记: $\alpha'=\alpha+c(\beta-\beta')$ $\quad c=\dfrac{\alpha'-\alpha}{\beta-\beta'}\in\mathbb{F}$, α' 是 f 的根

记 $\deg f=m$, $\deg g=n$, α' 最多 m 种, β' 最多 n 种 ∴ c 取值情况有限

$\mathbb{F}$ infinite ∴ 可以通过取其它的 c，让情况② → ①

如果 $h(x),g(x)$ 还有其它公因式 $x-\beta'$，可以写成: $c=\frac{\alpha'-\alpha}{\beta-\beta'}$. α' 为 f 的根, β' 为 g 的根

Th1: char$(\mathbb{F})=0$, $\forall$ finite extension of $\mathbb{F}$ is simple extension

finite ⇒ $E=\mathbb{F}(\alpha_1,\alpha_2,\cdots\alpha_n)$, α_i alge over $\mathbb{F}$

∴ $E=\mathbb{F}(\alpha_1+c_2\alpha_2+\cdots c_n\alpha_n)$

Th2: $\mathbb{F}$ is finite field, $\forall$ finite extension of $\mathbb{F}$ is simple extension

Th1+Th2: 有限扩张（⇒代数扩张）一定是单扩张

proof: $\mathbb{F}=\mathbb{F}_{p^d}$, $E=\mathbb{F}_{p^n}$ $\quad d\mid n$ $\quad$ Q: $d\mid n$ 为什么, HW10, T10(1), 还不会

$E^*=\langle\alpha\rangle$, then $E=\mathbb{F}(\alpha)$

例1: $\mathbb{Q}(\sqrt[3]{2},w)$ $\quad w=\frac{-1+\sqrt{3}i}{2}$, $\quad\mathbb{Q}(\sqrt[3]{2},w)=\mathbb{Q}(\sqrt[3]{2}+w)$

$[\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{2}w,\sqrt[3]{2}w^2):\mathbb{Q}]=6$, 我一开始以为是3. $x^3-2=0$.

Method 1: $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$, $[\mathbb{Q}(w):\mathbb{Q}]=2$. 互质 ∴ $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]\times[\mathbb{Q}(w):\mathbb{Q}]=[\mathbb{Q}(\sqrt[3]{2},w):\mathbb{Q}]$

2: $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}(w)]$ 和 $[\mathbb{Q}(w):\mathbb{Q}(\sqrt[3]{2})]$ 都不好求.

先弄成 simple extension, 求 $[\mathbb{Q}(w+\sqrt[3]{2}):\mathbb{Q}]=\deg(m_{w+\sqrt[3]{2},\mathbb{Q}})$

$\{a+bt : a, b \in \mathbb{F}_p\}$ $\mathbb{F} = \left\{ \frac{a_1+b_1 t}{a_2+b_2 t} : a_i, b_i \in \mathbb{F}_p, a_2+b_2 t \neq 0 \right\}$

Example 2. *Let $R = \mathbb{F}_p[t]$ and let F be the fraction field of R denoted by $\mathbb{F}_p(t)$. Then* char $F = p$ *and* $|F| = \infty$. [*Let $f(x) = x^p - t \in F[x]$. Suppose α is a root of $f(x)$. Then $f(x) = (x-\alpha)^p$.*]

Claim: $f(x)$ is irreducible in $F[x]$. 条件即 $t = a^p$?

Suppose $f(x) = g(x)h(x)$, $1 \leqslant \deg g < \deg f$. Then $g(x) \mid f(x) = (x-\alpha)^p$, and $g(x) = (x-\alpha)^m = \dots x + (-\alpha)^m$. Thus $\alpha^m \in F$. Since $F = \mathbb{F}_p(t)$. Now $t = \alpha^p$ since $\gcd(p, m) = 1$ we have $\alpha \in F$. Contradiction.

为啥? why not

char ≠ 0. field 有限. 只针对数域?

"F"这种字体是默认数域吗

可分多项式:

- $f(x) \in F[x]$. K is splitting field for $f(x)$ over F; $f(x) = \prod_{i=1}^{m} a(x-a_i)^{k_i}$, $a \neq 0$, $a_i \neq a_j$ ($i \neq j$); 则:
  $x - a_i$ 是 f 的 k_i 重因式, $k_i = 1$ 称为单因式, a_i 是 k_i 重根

《教》P120, lem3.2: $f(x) \in F[x]$, a 是 $f(x)=0$ 的 k 重根, $f'(x)$ 为导数

(1) $\mathrm{char}(F) \nmid k$, $f'(x)=0$ 以 a 为 $k-1$ 重根

(2) $\mathrm{char}(F) \mid k$, $f'(x)=0$ 中, a 至少是 k 重根,

prop3.3: $f(x) \in F[x]$, $f(x)=0$ 有重根 $\Leftrightarrow \gcd(f(x), f'(x)) \neq 1$

prop3.4: $f(x) \in F[x]$ irreducible, $f(x)$ 无重根 $\Leftrightarrow f'(x) \neq 0$ (指不恒 $=0$)

$\Rightarrow$ 设 $f'(x) = 0$, $(f'(x), f(x)) = f(x)$

$\Leftarrow$ 设有重根, $\gcd(f', f) \neq 1$,

f irreducible, f 因子只有 1 和 f $\therefore \gcd(f', f) = f$

$f(x) \mid f'(x)$ 与 $\deg(f') < \deg(f)$ 矛盾 设 $f' \neq 0$

▲prop3.5: $\mathrm{char}(F) = 0$, f irr in $F[x]$; then: f 在 K 上无重根

在 F 上不可分, x^2+1 在 $\mathbb{C}$ 上 reducible, 在 $\mathbb{R}$ 上 irr

def: F is field, $f(x) \in F[x]$ irreducible; K is splitting field of $f(x)$ over F;
若 $f(x)$ 在 $K[x]$ 中所有因式均为单因式, f 是 F 上的可分多项式.

P127 prop3.7+3.8 f irr in $F[x]$, f 在 F 上可分. 真假?

对 F finite 或 infinite 讨论