§5.1 域的有限扩张

域：= 交换的除环. F为域

$P \subseteq F$ 称为子域 若P为F的非零子环且 $\forall a \in P$ 则 $a^{-1} \in P$.

域的同态，同构：= 作为环的同态，同构.

$\varphi: F \longrightarrow K$ 域的同态 则 $\varphi(1_F) = 1_K \Rightarrow \varphi$ 不是零映射

F的理想：$\{0\}, F$. $\Rightarrow \ker\varphi = \{0\} \Rightarrow \varphi$ 为单射

定义：若 $\varphi: F \longrightarrow K$ 为域的同态，则称K为F的扩域(通过φ).

此时 $\varphi(F)$ 为K的子域，常将F与$\varphi(F)$等同 从而视F为K的子域

回顾：$\mathbb{R} \subseteq \mathbb{C}$ 的含义？

$$\mathbb{C} = \{(a,b) \mid a, b \in \mathbb{R}\} \qquad \begin{aligned} +&: (a,b)+(c,d) := (a+c, b+d) \\ \cdot&: (a,b)(c,d) := (ac-bd, ad+bc) \end{aligned}$$

$\varphi: \mathbb{R} \longrightarrow \mathbb{C}$, $r \longrightarrow (r,0)$ 为单同态，通过φ将$\mathbb{R}$看作$\mathbb{C}$的子域.

设K为F的扩域. 则K为F-向量空间(数乘为乘法)，且域的乘法是

F-双线性映射 $\Rightarrow$ K为F-代数 且K为可除代数.

K为域 $F \subseteq K$ 为子域

$S \subseteq K$ 为子集

$$F(S) := \bigcap_{F \cup S \subseteq \tilde{F} \subseteq K,\ \tilde{F}\text{为子域}} \tilde{F}$$ 称为S在F上生成的域

特别地，$S \subseteq K$ 为子域 则称 $F(S) = S(F)$ 为域F, S的合成.

当 $|S| < +\infty$，称 $F(S)$ 是F的有限生成扩张

设 $S = \{\alpha_1, \cdots \alpha_n\}$. 则 $F(\alpha_1 \cdots \alpha_n) = \left\{ \dfrac{f(\alpha_1 \cdots \alpha_n)}{g(\alpha_1 \cdots \alpha_n)} \;\middle|\; \begin{array}{l} f, g \in F[X_1, \cdots X_n] \\ \text{且 } g(\alpha_1, \cdots \alpha_n) \neq 0 \end{array} \right\}$.

称 $F(\alpha_1)$ 为F的单扩张，α_1 为 $F(\alpha_1)$ 的本原元.

注：由定义易知：$F(\alpha_1, \alpha_2) = F(\alpha_1)(\alpha_2)$.

引入域扩张的目的？解方程.

命题1：设 $f \in F[X]$ 为不可约多项式，则 $\exists\ K/F$ 及 $\alpha \in K$ s.t. $f(\alpha) = 0$.

证：令 $I = \langle f \rangle$. $\because F[X]$ 为PID. $\therefore I$ 为极大理想 (§4.2)

$\Rightarrow K = F[X]/\langle f \rangle$ 为域.

定义映射: $\varphi: F \longrightarrow K$, $a \longrightarrow a+I$. 为域同态 $\Rightarrow K$ 为 F 的扩域

令 $\alpha = X+I$. 设 $f = \sum_{i=0}^{n} c_i X^i$, $c_i \in F$. 则

$$f(\alpha) = \sum_{i=0}^{n} (c_i+I)(X+I)^i = \sum_{i=0}^{n} c_i X^i + I = 0 \ (\because f \in I)$$

□

定义2: 设 $f \in F[X]$, $\deg f = n > 0$. 则 F 的扩域 K 称为 f 在 F 上的分裂域

如果 1) $f = \lambda(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n)$, $\lambda \in F$, $\alpha_1, \cdots \alpha_n \in K$.

2) $K = F(\alpha_1, \cdots \alpha_n)$.

定理0: 设 $f \in F[X]$, $\deg f > 0$. 则 f 在 F 上的分裂域存在.

证: (归纳法).

当 $\deg f = 1$ 时, $f = \lambda(X-\alpha_1)$, $\lambda, \alpha_1 \in F$. 令 $K = F$ 即可.

设 $\deg f = n-1$ 时定理成立.

$\because F[X]$ 为 PID $\therefore$ 存不可约多项式 $f_1 \in F[X]$, s.t. $f_1 | f$.

命题0 $\Rightarrow$ 存 K/F 及 $\alpha_1 \in K$ s.t. $f_1(\alpha_1) = 0$.

令 $F_1 = F(\alpha_1)$. $f_1 | f \Rightarrow f(\alpha_1) = 0 \Rightarrow f = (X-\alpha_1)g$

由带余除法可知: $g \in F_1[X]$ 且 $\deg g = n-1$.

由归纳假设, g 在 F_1 上的分裂域存在 设其中一个为 L.

则 $L = F_1(\alpha_2, \cdots \alpha_n)$, $g = \lambda(X-\alpha_2)\cdots(X-\alpha_n)$. $\alpha_2 \cdots \alpha_n \in L$, $\lambda \in F_1$.

$\Rightarrow L = F(\alpha_1, \alpha_2, \cdots \alpha_n)$, $f = \lambda(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n)$

$\because f \in F[X] \Rightarrow \lambda \in F$. $\therefore L$ 为 f 在 F 上的分裂域. □

例: $F = \mathbb{Q}$, $f = X^2-2$ 为 $\mathbb{Q}$ 上不可约多项式.

则 $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ 为 f 在 F 上的分裂域, 同时 $\mathbb{Q}[X]/\langle X^2-2 \rangle$ 也为 f 在 F 上的分裂域.

注: 设 K 为 f 在 F 上的分裂域. $F \subseteq L \subseteq K$ 为子域

则 K 为 f 在 L 上的分裂域.

K 为 F 的扩域, $\theta \in K$.

称 θ 在 F 上代数, 如果 $\exists f \in F[X]$ 使 s.t. $f(\theta) = 0$.

与F-代数类似，用$\mu_\theta(X)$表示θ的极小多项式.

K为可除F-代数 $\Rightarrow \mu_\theta(X)$为不可约多项式.

当θ在F上不是代数么，则称θ在F上是超越的.

命题1：设K/F为域扩张，$\theta \in K$.

1) 若θ在F上超越，则 $F(X) \cong F(\theta)$

2) 若θ在F上代数，则 $F(\theta)=F[\theta] \cong F[X]/\langle \mu_\theta \rangle$.

证：1) 定义映射 φ：$F(X) \longrightarrow F(\theta)$

$f(X) \longrightarrow f(\theta)$

θ在F上超越 $\Rightarrow g(\theta)=0 \Leftrightarrow g(X)=0$, $\forall\, g \in F[X]$

$\therefore \varphi$是良定义的，易验证φ为同构.

2) 定义：φ：$F[X] \longrightarrow F[\theta]$ 则φ为满同态.

$g(X) \longrightarrow g(\theta)$

$\ker\varphi = \langle \mu_\theta \rangle$. μ_θ不可约，$F[X]$为PID $\Rightarrow \langle \mu_\theta \rangle$为极大理想 (§4.2)

$\therefore F[X]/\langle \mu_\theta \rangle$为域 且 $F[X]/\langle \mu_\theta \rangle \cong F[\theta]$.

$\therefore F[\theta]$为域. $\Rightarrow \forall\, g(\theta) \in F[\theta] \setminus \{0\}$, $\frac{1}{g(\theta)} \in F[\theta]$

$\Rightarrow F(\theta)=F[\theta]$. □

记号：$[K:F] := \dim_F K$.

定理1：设K/F为域扩张，$\theta \in K$.

1) 若θ在F上代数，则 $[F(\theta):F]=\deg\mu_\theta$，且 $1, \theta, \cdots \theta^{\deg\mu_\theta-1}$为$F(\theta)$的一组F-基.

2) θ在F上代数 $\Leftrightarrow [F(\theta):F]<+\infty$.

证：1) 由命题1，$F(\theta)=F[\theta]$. 剩下的参见§4.4 命题3的证明.

2) ($\Rightarrow$) 由1)知. ($\Leftarrow$) 显然. □

定理2：设$F \subseteq K \subseteq L$为域扩张，则

1) $[L:F]<+\infty \Leftrightarrow [K:F]<+\infty$ 且 $[L:K]<+\infty$.

2) 当$[L:F]<+\infty$时有 $[L:F]=[L:K][K:F]$ (称为望远镜公式)

证：1) ($\Rightarrow$) ∵作为F-向量空间，K为L的子空间

$\therefore [K:F] \leq [L:F] < +\infty$.

设 $u_1, \cdots u_n \in L$为一组F-基，从而 $L=Fu_1 \oplus \cdots \oplus Fu_n$.

$F \subseteq K \Rightarrow L = Ku_1 + \cdots + Ku_n \Rightarrow [L:K] \le n$.

($\Leftarrow$) 设 $u_1, \cdots u_l \in L$ 为 L 作为一组 K-基, $v_1, \cdots v_m \in K$ 为 K 作为一组 F-基.

下证 $\{u_i v_j \mid \substack{i=1,\cdots l \\ j=1,\cdots m}\} \subseteq L$ 为 L 作为一组 F-基.

· 设 $\sum_{i=1}^{l}\sum_{j=1}^{m} c_{ij} u_i v_j = 0$, $c_{ij} \in F$. 则 $\sum_{i=1}^{l}\left(\sum_{j=1}^{m} c_{ij} v_j\right) u_i = 0$

$\sum_{j=1}^{m} c_{ij} v_j \in K$, $\forall 1 \le i \le l \Rightarrow \sum_{j=1}^{m} c_{ij} v_j = 0 \quad \forall 1 \le i \le l$

$\Rightarrow c_{ij} = 0, \forall 1 \le i \le l, 1 \le j \le m$

$\Rightarrow \{u_i v_j \mid \substack{i=1,\cdots l \\ j=1,\cdots m}\}$ F-线性无关.

$\forall a \in L$, $a = \sum_{i=1}^{l} a_i u_i$, $a_i \in K$.

$\forall 1 \le i \le l$, $a_i = \sum_{j=1}^{m} c_{ij} v_j \Rightarrow a = \sum_{i=1}^{l}\sum_{j=1}^{m} c_{ij} u_i v_j$

$\therefore \{u_i v_j \mid \substack{i=1,\cdots l \\ j=1,\cdots m}\}$ 为 L 作为一组 F-基.

$\therefore [L:F] = lm = [L:K][K:F] < +\infty$ □

令 $A := \{a \in K \mid a$ 在 F 上代数$\}$ 称为 F 在 K 中作代数闭包.

下证明: A 为 F 在 K 中作代数闭包. 则 $F \subseteq A$ 且 A 为 K 作子域.

证: $\forall a \in F$, 有 $x - a$ 以 a 为根 $\Rightarrow a \in A$.

设 $a, b \in A$. 则 b 在 $F(a)$ 上代数.

定理1 $\Rightarrow \begin{cases} [F(a):F] < +\infty \\ [F(a,b):F(a)] < +\infty \end{cases} \Rightarrow [F(a,b):F]$

$= [F(a,b):F(a)][F(a):F] < +\infty$.

$\because a-b, ab \in F(a,b)$.

$\therefore [F(a-b):F] < +\infty$, $[F(ab):F] < +\infty \Rightarrow a-b, ab \in A$

$\Rightarrow A$ 为子环.

设 $a \in A \setminus \{0\}$, 则 $F(a) = F(a^{-1}) \Rightarrow [F(a^{-1}):F] < +\infty \Rightarrow a^{-1} \in A$.

$\therefore A$ 为子域 □

$f \in F[X] \setminus F$. $n = \deg f$, K 为 f 在 F 上的分裂域.

则 $f = \lambda(X - \alpha_1)\cdots(X - \alpha_n)$, $\lambda \in F$. $\alpha_1 \cdots \alpha_n \in K$.

称 f (在 K 中) 无重根, 若 $\forall 1 \le i \ne j \le n$, $\alpha_i \ne \alpha_j$.

设 $\varphi: F_1 \to F_2$ 为域同构. $f = \sum_{i=0}^{l} c_i X^i \in F_1[X]$.

记 $\varphi(f) := \sum_{i=0}^{l} \varphi(c_i) X^i \in F_2[X]$.

引理1：设 $\varphi: F_1 \to F_2$ 为域同构，K_1/F_1，K_2/F_2 分别为域扩张。

$\alpha \in K_1$ 在 F_1 上代数，μ_α 为极小多项式。则

1) 于域同态 $\psi: F_1(\alpha) \to K_2$ s.t. $\psi|_{F_1} = \varphi \iff \varphi(\mu_\alpha)$ 在 K_2 中有根。

2) ψ 个数 $= \varphi(\mu_\alpha)$ 在 K_2 中相异根个数。

证：1) ($\Rightarrow$) $\mu_\alpha(\alpha) = 0 \Rightarrow \psi(\mu_\alpha(\alpha)) = 0 \Rightarrow \varphi(\mu_\alpha)(\psi(\alpha)) = 0$

$\Rightarrow \psi(\alpha)$ 为 $\varphi(\mu_\alpha)$ 在 K_2 中一根

($\Leftarrow$) 设 β 为 $\varphi(\mu_\alpha)$ 在 K_2 中一根。则考虑环同态

$$\overline{\varphi}_\beta: F_1[X] \longrightarrow K_2$$

$$\sum_{i=0}^{l} c_i X^i = f(X) \longrightarrow \varphi(f)(\beta) = \sum_{i=0}^{l} \varphi(c_i)\beta^i$$

则 $\langle \mu_\alpha \rangle \subseteq \ker \overline{\varphi}$。$F_1[X]$ 为 PID $\Rightarrow \langle \mu_\alpha \rangle$ 为极大理想

$\Rightarrow \langle \mu_\alpha \rangle = \ker \overline{\varphi}$。

$\therefore$ $\overline{\varphi}_\beta: F_1[X]/\langle \mu_\alpha \rangle \longrightarrow K_2$

$f(X) + \langle \mu_\alpha \rangle \longrightarrow \varphi(f)(\beta)$ 为域同态

由命题1 $\Rightarrow \exists\, \sigma: F_1(\alpha) \longrightarrow F_1[X]/\langle \mu_\alpha \rangle$ 为域同构。

$$f(\alpha) \longrightarrow f(X) + \langle \mu_\alpha \rangle$$

令 $\psi_\beta = \sigma \circ \overline{\varphi}_\beta$: $F_1(\alpha) \longrightarrow K_2$

$f(\alpha) \longrightarrow \varphi(f)(\beta)$ 为域同态

且 $\psi_\beta|_{F_1} = \varphi$。

2) 设 β 与 β' 为 $\varphi(\mu_\alpha)$ 在 K_2 中相异根，则 $\psi_\beta(\alpha) = \beta \neq \beta' = \psi_{\beta'}(\alpha)$

$\Rightarrow \psi_\beta$ 与 $\psi_{\beta'}$ 为相异的同态

反之，同态 ψ 由 $\psi(\alpha)$ 唯一确定 $\Rightarrow$ 若 $\psi \neq \psi'$ 则 $\psi(\alpha)$ 与 $\psi'(\alpha)$ 为 $\varphi(\mu_\alpha)$ 在 K_2 中相异的根。 □

定理3：设 $\varphi: F_1 \to F_2$ 为域同构，$f_1 \in F_1[X]$，$\deg f_1 = n > 0$。

令 $f_2 = \varphi(f_1)$，设 K_1，K_2 分别为 f_1，f_2 在 F_1 与 F_2 上的分裂域。则

1) 于同构 $\overline{\varphi}: K_1 \to K_2$ s.t. $\overline{\varphi}|_{F_1} = \varphi$

2) $\overline{\varphi}$ 个数 $k \leq [K_1 : F_1]$ 且当 $f_2(X)$ 无重根时 $k = [K_1 : F_1]$。

证：对 $[K_1:F_1]$ 作归纳.

当 $[K_1:F_1]=1$ 时 $f_1=\lambda(X-\alpha_1)\cdots(X-\alpha_n)$, $\lambda,\alpha_1,\cdots\alpha_n\in F_1$

$f_2=\varphi(f_1)=\varphi(\lambda)(X-\varphi(\alpha_1))\cdots(X-\varphi(\alpha_n))$

$\Rightarrow K_2=F_2(\varphi(\alpha_1),\cdots\varphi(\alpha_n))=F_2$.

此时 $\sigma=\varphi$ 是唯一的同构.

设对任对 $[K_1:F_1]\leq n-1$ 时成立. 设 $[K_1:F_1]=n>1$.

令 α_1 为 f_1 在 K_1 中的一个根且 $\alpha_1\notin F_1$. 则 $\deg\mu_{\alpha_1}>1$.

$\mu_{\alpha_1}\mid f_1\Rightarrow\varphi(\mu_{\alpha_1})\mid f_2\Rightarrow\varphi(\mu_{\alpha_1})$ 在 K_2 中有根.

引理1 $\Rightarrow$ 存同态 $\psi:F_1(\alpha_1)\longrightarrow K_2$ s.t. $\psi|_{F_1}=\varphi$.

设 $\psi_1,\cdots\psi_l$ 为满足条件的所有同态，则 $l=\varphi(\mu_{\alpha_1})$ 在 K_2 中相异根的个数

$\Rightarrow l\leq\deg\varphi(\mu_{\alpha_1})$.

注意到 K_1 为 f_1 在 $F_1(\alpha_1)$ 上的分裂域 $\Rightarrow$

K_2 为 f_2 在 $\psi_i(F_1(\alpha_1))$ 上的分裂域 $\forall\ 1\leq i\leq l$.

$\because [K_1:F_1(\alpha_1)]=\dfrac{[K_1:F_1]}{[F_1(\alpha_1):F_1]}=\dfrac{[K_1:F_1]}{\deg\mu_{\alpha_1}}<[K_1:F_1]=n$.

现有：$\psi_i:F_1(\alpha_1)\longrightarrow\psi_i(F_1(\alpha_1))$ 为同构

K_1 为 f_1 在 $F_1(\alpha_1)$ 上的分裂域，K_2 为 f_2 在 $\psi_i(F_1(\alpha_1))$ 上的分裂域且 $[K_1:F_1(\alpha_1)]<n$.

由归纳假设，$\exists$ 同构 $\sigma_i:K_1\longrightarrow K_2$ s.t. $\sigma_i|_{F_1(\alpha_1)}=\psi_i$

设 $\sigma_{i,1},\cdots\sigma_{i,k_i}:K_1\longrightarrow K_2$ 为不同的同构 s.t. $\sigma_{i,j}|_{F_1(\alpha_1)}=\psi_i$

则 $k_i\leq[K_1:F_1(\alpha_1)]$ 且 $f_2(X)$ 无重根时 $k_i=[K_1:F_1(\alpha_1)]$.

设 $1\leq i\neq i'\leq l$. 则 $\sigma_{i,j}|_{F_1(\alpha_1)}=\psi_i\neq\psi_{i'}=\sigma_{i',j'}|_{F_1(\alpha_1)}$

$\therefore$ $\sigma_{i,j}$, $i=1,\cdots l$, $j=1,\cdots k_i$ 为相异的同构.

设 $\tau:K_1\longrightarrow K_2$ 为同构 s.t. $\tau|_{F_1}=\varphi$. 则 $\tau|_{F_1(\alpha)}=\psi_{i_0}$ 对某个 $1\leq i_0\leq l$.

$\Rightarrow\tau=\sigma_{i_0,j_0}$ 对某 $1\leq j_0\leq k_{j_0}$

$\Rightarrow$ σ 的个数 $=\sum_{j=1}^{l}k_i\leq l[K_1:F_1(\alpha_1)]\leq\deg\mu_{\alpha_1}[K_1:F_1(\alpha_1)]=[K_1:F_1]$.

当 $f_2(X)$ 无重根时，$\varphi(\mu_{\alpha_1})$ 在 K_2 中有 $\deg\mu_{\alpha_1}$ 个相异的根

$\Rightarrow l=\deg\mu_{\alpha_1}$

$\forall\ 1\leq i\leq l$, $k_i=[K_1:F_1(\alpha_1)]$

$\Rightarrow$ σ 的个数 $=\deg\mu_{\alpha_1}[K_1:F_1(\alpha_1)]$

$=[K_1:F_1]$ □

$\Rightarrow l = \deg \mu_{\alpha_1}$
$\forall 1 \le i \le l,\ k_i = [K_1 : F_1(\alpha_1)]$
$\Rightarrow$ 互不相等 $= \deg \mu_{\alpha_1} = [K_1 : F_1(\alpha_1)]$
$= [K_1 : F_1]$ □

推论2：设 $f \in F[x]$, $\deg f > 0$, K_1, K_2 为 f 在 F 上的两个分裂域 则
$\exists$ 同构 $\psi : K_1 \to K_2$ s.t. $\psi|_F = id_F$

证：在定理3中令 $F_1 = F_2 = F$, $\varphi : F \to F$ 为恒等映射即可.

令 $Aut(K/F) := \{\psi : K \to K$ 为域同构 $| \psi|_F = id_F\}$.

$Aut(K/F)$ 在复合运算下构成群.

推论3：设 K 为 f 在 F 上的分裂域 则 $|Aut(K/F)| \le [K:F]$
且当 $f(x)$ 无重根时，$|Aut(K/F)| = [K:F]$.

考察 $[K:F]$.

命题2：设 $f \in F[x]$, $\deg f = n > 0$, K 为 f 在 F 上的分裂域 则
$[K:F] \le n!$

证：对 $\deg f$ 作归纳.
当 $\deg f = 1$ 时 $K = F$ 成立.
设 $\deg f = n-1$ 时命题成立. $f = \lambda(x-\alpha_1)\cdots(x-\alpha_n)$, $\lambda \in F$, $\alpha_1, \cdots \alpha_n \in K$.
令 $f = (x-\alpha_1)g$. 则 $g \in F(\alpha_1)[x]$ 且 $\alpha_2, \cdots \alpha_n$ 为 g 的所有根
由定义知：K 为 g 在 $F(\alpha_1)$ 上的分裂域. $\deg g = n-1$
利用归纳假设 $\Rightarrow [K : F(\alpha_1)] \le (n-1)!$
又：$[F(\alpha_1) : F] = \deg \mu_{\alpha_1} \le \deg f = n$
$\therefore [K:F] = [K : F(\alpha_1)][F(\alpha_1) : F] \le n!$ □

例：$F = \mathbb{Q}$, $f = (x^2-2)(x^2-3)$. $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ 为 f 在 F 上的分裂域.
$[K:F] = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \le 4$.
令 $\theta = \sqrt{2} + \sqrt{3}$. 则 $\mu_\theta = x^4 - 10x + 1$
$4 = [\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] \le [K:\mathbb{Q}] \le 4 \Rightarrow [K:\mathbb{Q}] = 4$
且 $K = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.
f 无重根 $\Rightarrow |Aut(K/F)| = 4 \Rightarrow Aut(K/F) \cong \mathbb{Z}/4\mathbb{Z}$ 或 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$\forall \psi \in Aut(K/F)$ 引理证明 $\Rightarrow \begin{cases} \psi(\sqrt{2})^2 - 2 = 0 \\ \psi(\sqrt{3})^2 - 3 = 0 \end{cases}$

$\Rightarrow \psi(\sqrt{2}) = \pm\sqrt{2},\ \psi(\sqrt{3}) = \pm\sqrt{3}$.

$\Rightarrow \psi^2 = id \Rightarrow Aut(K/F) = \mathbb{Z}_2 \times \mathbb{Z}_2$.

$Aut(K/F)$ 称为 f 在 F 上的伽罗瓦群.

称 K/F 为有限扩张, 若 $[K:F] < +\infty$.

定理 4: 设 K/F 为有限扩张, 则本原元存在 $\Leftrightarrow$ K 的中间域 E ($F \subseteq E \subseteq K$) 个数有限.

证: 若 F 为有限域 则 K 也为有限域. 则 $U(K) = \langle \theta \rangle \Rightarrow K = F(\theta)$.

设 $|F| = +\infty$.

($\Leftarrow$) 设 $\alpha, \beta \in K$. 则 $F \subseteq F(\alpha + c\beta) \subseteq K$. $\forall c \in F$.

$\because |F| = +\infty$. $\therefore \exists c_1 \neq c_2 \in F$ s.t. $F(\alpha + c_1\beta) = F(\alpha + c_2\beta) =: E$

$\because \alpha + c_1\beta, \alpha + c_2\beta \in E \Rightarrow \beta \in E,\ \alpha \in E \Rightarrow E = F(\alpha, \beta)$

$[K:F] < +\infty \Rightarrow K/F$ 为有限生成扩张. i.e. $\exists \alpha_1, \cdots \alpha_n \in K$ s.t. $K = F(\alpha_1, \cdots \alpha_n)$.

用归纳法知: $\exists c_1, \cdots c_n \in F$ s.t. $K = F(\sum_{i=1}^{n} c_i \alpha_i)$.

($\Rightarrow$) 设 $K = F(\theta)$. μ_θ 为 θ 在 F 上的极小多项式.

令 $S = \{ g \in K[X] \setminus K \mid g \text{ 首1 且 } g \mid \mu_\theta \}$.

设 E 为中间域, f_E 为 θ 在 E 上的极小多项式. 则 $f_E \mid \mu_\theta \Rightarrow f_E \in S$.

定义映射: $\varphi: \{ E \mid F \subseteq E \subseteq K \text{ 中间域} \} \longrightarrow S$

$E \longrightarrow f_E$

设 $f_E = X^m + \sum_{i=0}^{m-1} c_i X^i,\ c_i \in E$. 令 $\tilde{E} = F(c_0, \cdots c_{m-1})$. 则 f_E 在 $\tilde{E}$ 上不可约.

$[K:\tilde{E}] = \deg f_E = [K:E] \Rightarrow E = \tilde{E} \Rightarrow \varphi$ 为单射

$\therefore$ 中间域个数 $\leq |S| < +\infty$. □

K/F 称为代数扩张, 若 $\forall a \in K$, a 在 F 上代数.

由定理1 $\Rightarrow$ 若 $[K:F] < +\infty$ 则 K/F 为代数扩张, 反之不然.

例: $S = \{ e^{\frac{2\pi\sqrt{-1}}{n}} \mid n > 0 \}$ 则 $\mathbb{Q}(S)/\mathbb{Q}$ 是代数扩张.

但 $[\mathbb{Q}(S):\mathbb{Q}] = +\infty$.

另一方面. 若 K/F 是有限生成代数扩张, 则 $[K:F] < +\infty$.

(设 $K = F(\alpha_1, \cdots \alpha_n)$. 则 α_i 在 $F(\alpha_1, \cdots \alpha_{i-1})$ 上代数.

$\Rightarrow [K:F] = \prod_{i=1}^{n} [F(\alpha_1, \cdots \alpha_i) : F(\alpha_1, \cdots \alpha_{i-1})] < +\infty$.)

命题3: 1) 设 K/F, L/K 为代数扩张. 则 L/F 也为代数扩张.

2) 设 K_1/F, K_2/F 为代数扩张且 K_1, K_2 为 L 的子域. 则 $K_1(K_2)/F$ 为代数扩张.

证: 1) $\forall a \in L$, a 在 K 上代数 $\Rightarrow \exists f(x) \in K[X] \setminus \{0\}$ s.t. $f(a)=0$

记 $f(X) = X^n + \sum_{i=0}^{n-1} c_i X^i$, $c_i \in K$. 则

$[F(a, c_0, c_1, \cdots c_{n-1}) : F(c_0, c_1, \cdots c_{n-1})] \leq n$.

另外: c_i 在 F 上代数 $\forall 0 \leq i \leq n-1 \Rightarrow [F(c_0, \cdots c_{n-1}) : F] < +\infty$

$\Rightarrow [F(a, c_0, c_1, \cdots c_{n-1}) : F] < +\infty$

$\Rightarrow [F(a) : F] < +\infty \Rightarrow a$ 在 F 上代数

2) 令 $\widetilde{F}$ 为 F 在 L 中的代数闭包. 则 $\widetilde{F}/F$ 为代数闭包且 $K_1, K_2 \subseteq \widetilde{F}$.

$\Rightarrow K_1(K_2) \subseteq \widetilde{F} \Rightarrow K_1(K_2)/F$ 为代数扩张. □

域的特征: $\varphi: \mathbb{Z} \to F$, $n \to n \cdot 1$, $\ker\varphi = m\mathbb{Z}$, $m=0$ 或 $m>1$

$\mathbb{Z}/m\mathbb{Z}$ 为整环 $\Rightarrow m=0$ 或 m 为素数, m 称为 F 的特征, 记作 $\mathrm{char}F$.

$\bigcap_{\widetilde{F} \subseteq F \text{ 子域}} \widetilde{F}$ 称为 F 的素域. 同构或 $\mathbb{Z}/p\mathbb{Z}$. p 为素数.

$f \in F[X]$ 称为可分的, 若 $f \neq F$ 且 f 的所有不可约因子均无重根, 否则称 f 不可分

K/F 为域扩张, $\alpha \in K$ 在 F 上代数. 称 α 在 F 上可分, 若 μ_α 是可分的

K/F 称为可分扩张, 若 K/F 为代数扩张且 $\forall \alpha \in K$, α 在 F 上可分.

F 称为完全域, 若 $\forall f \in F[X] \setminus F$, f 可分.

命题4: $f \in F[X] \setminus F$.

1) f 无重根 $\Leftrightarrow \gcd(f, f') = 1$

2) 若 $\mathrm{char}F = 0$ 则 F 是完全域.

3) 设 $\mathrm{char}F = p > 0$, f 不可约. 则 f 是不可分 $\Leftrightarrow \exists g \in F[X]$ s.t. $f = g(X^p)$

证: 1) 设 K 为 f 在 F 上的分裂域. $f = \lambda(X-\alpha_1)\cdots(X-\alpha_n)$ $\lambda \in F$, $\alpha_1, \cdots \alpha_n \in K$.

($\Rightarrow$) f 无重根 $\Rightarrow \alpha_i \neq \alpha_j$ $\forall 1 \leq i \neq j \leq n$.

$\Rightarrow f'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j) \neq 0$ $\forall 1 \leq i \leq n$

$\Rightarrow f$ 与 f' 无公因子 $\Rightarrow \gcd(f, f') = 1$.

($\Leftarrow$) 设 $f=\lambda(X-\alpha_1)^2 g \quad g\in K[X]$

则 $f'=2\lambda(X-\alpha_1)g+\lambda(X-\alpha)^2 g' \Rightarrow X-\alpha \mid f'$

$\Rightarrow X-\alpha$ 为 f 与 f' 公因子 $\Rightarrow \gcd(f,f')\neq 1$

2) 设 $g\in F[X]\setminus F$ 且 g 不可约.

$\gcd(g,g')\neq 1 \Rightarrow g\mid g'$, $\deg g'=\deg g-1$ $\Rightarrow g'=0 \Rightarrow g\in F$ 矛盾.

$\therefore \gcd(g,g')=1 \Rightarrow g$ 无重根, i.e. g 是可分的.

3) ($\Rightarrow$) f 不可约 $\Rightarrow f$ 有重根 $\Rightarrow \gcd(f,f')\neq 1 \Rightarrow f\mid f'$, $\deg f'=\deg f-1$ $\Rightarrow f'=0$

设 $f=\sum_{i=0}^{n} c_i X^i$ 则 $f'=\sum_{i=0}^{n} i c_i X^{i-1}=0 \Rightarrow c_i\neq 0$ 则 $i=0\in F$ i.e. $p\mid i$

$\Rightarrow f=\sum_{i=0}^{m} c_{ip} X^{ip}$. 令 $g=\sum_{i=0}^{m} c_{ip} X^i$. 则 $f=g(X^p)$.

($\Leftarrow$) $f=g(X^p) \Rightarrow f'=0 \Rightarrow \gcd(f,f')=f\neq 1 \Rightarrow f$ 有重根 $\Rightarrow f$ 不可分. □

定理5: 设 $\mathrm{char}F=p>0$. 则 F 是完全的 $\Leftrightarrow F=F^p\left(:=\{c^p \mid c\in F\}\right)$.

证: ($\Rightarrow$) 设 $F^p \subsetneq F$. 令 $a\in F\setminus F^p$. 则 X^p-a 在 F^p 上是不可约的

由命题4, X^p-a 不是可分的 $\Rightarrow F$ 不是完全域.

($\Leftarrow$) 设 F 不是完全域, $\exists f\in F[X]\setminus F$. 不可约. 且 f 不是可分的.

命题4 $\Rightarrow f=g(X^p)$. $g\in F[X]$. 设 $g=\sum_{i=0}^{l} c_i X^i$.

如果 $\forall 1\le i\le l$. 有 $c_i=\bar{c}_i^{\,p}$, $\bar{c}_i\in F$, 则 $f=\left(\sum_{i=0}^{l}\bar{c}_i X^i\right)^p$ 与 f 不可约矛盾.

$\therefore \exists c_i$ s.t. $c_i\notin F^p$, i.e. $F\neq F^p$. □

定理6: (本原元定理) 设 K/F 为有限可分扩张. 则 K/F 为单扩张.

证: 当 F 为有限域时成立. 下设 $|F|=+\infty$.

$[K:F]<+\infty \Rightarrow K=F(\alpha_1,\cdots\alpha_n)$. $\alpha_1,\cdots\alpha_n\in K$.

先证 $n=2$ 的情形. 设 $K=F(\alpha,\beta)$. μ_α, μ_β 为极小多项式.

设 L 为 μ_α 在 F 上的分裂域. L' 为 μ_β 在 L 上的分裂域.

$\forall \lambda\in F$. $\beta\in F(\alpha+\lambda\beta) \Rightarrow \alpha\in F(\alpha+\lambda\beta) \Rightarrow F(\alpha+\lambda\beta)=F(\alpha,\beta)$

$\therefore$ 仅需证 $\exists \lambda\in F$ s.t. $\beta\in F(\alpha+\lambda\beta)$.

$\mu_\alpha(-\lambda X+\alpha+\lambda\beta)$ 与 $\mu_\beta(X)$ 有公共根 β.

将 $\mu_\alpha(-\lambda X+\alpha+\lambda\beta)$ 与 $\mu_\beta(X)$ 看作 $F(\alpha+\lambda\beta)[X]$ 中元素.

令 $g_\lambda=gcd(\mu_\alpha(-\lambda X+\alpha+\lambda\beta),\mu_\beta(X))\in F(\alpha+\lambda\beta)[X]$.

则 $g_\lambda(\beta)=0\Rightarrow \deg g\geq 1$.

设 $\deg g_\lambda>1$. $\because \beta$ 可分 $\therefore \mu_\beta$ 为可分多项式 $\Rightarrow \mu_\beta$ 在 Σ 中无重根

$\Rightarrow g$ 在 Σ 中无重根 $(g\mid\mu_\beta)\Rightarrow \exists \beta'\in\Sigma$ s.t. $g(\beta')=0$ 且 $\beta'\neq\beta$.

$\Rightarrow \mu_\alpha(-\lambda\beta'+\alpha+\lambda\beta)=0\Rightarrow -\lambda\beta'+\alpha+\lambda\beta=\alpha'\in\Sigma$

$\Rightarrow \lambda=\dfrac{\alpha'-\alpha}{\beta-\beta'}$

$\because |F|=+\infty$ 而 $\alpha,\alpha',\beta,\beta'$ 分别为 μ_α,μ_β 的根,只有有限种可能.

$\therefore \exists \lambda\in F$ s.t. $\lambda\neq\dfrac{\alpha'-\alpha}{\beta-\beta'}$, 对 $\forall \alpha',\beta'\in\Sigma$, $\mu_\alpha(\alpha')=0,\mu_\beta(\beta')=0$ 且 $\beta'\neq\beta$.

此时 $\deg g_\lambda=1\Rightarrow g_\lambda=a(X-\beta)\in F(\alpha+\lambda\beta)[X]\Rightarrow \beta\in F(\alpha+\lambda\beta)$.

当 $n>2$ 时利用归纳法. 口.