# 抽象代数学

## 1. 不可约多项式的零点

定义 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in F[x]$.

令 $f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+a_1\in F[x]$, 称为 $f(x)$ 的导函数 (derivative)

设 $E$ 是 $f(x)$ 在 $F$ 上分裂域. 在 $E[x]$ 中,

$$f(x)=c\prod_{i=1}^{s}(x-\alpha_i)^{k_i},\quad c,\alpha_1,\cdots,\alpha_s\in E,\ c\neq 0,\ \alpha_i\neq\alpha_j$$

$x-\alpha_i$ 是 $f(x)$ 的 $k_i$ 重因式, $\alpha_i$ 是 $f(x)=0$ 的 $k_i$ 重根.

定理 设 $F$ 是域, $f(x)\in F[x]$, 则 $f(x)=0$ 有重根 $\Leftrightarrow$ $(f(x),f'(x))\neq 1$

证明: "$\Rightarrow$" 在 $E[x]$ 中, 设 $f(x)=(x-\alpha)^2g(x)$, $f'(x)=(x-\alpha)^2g'(x)+2(x-\alpha)g(x)=(x-\alpha)[(x-\alpha)g'(x)+2g(x)]\Rightarrow f'(\alpha)=0$

即 $x-\alpha\mid f(x)$, $x-\alpha\mid f'(x)$ (在 $E[x]$ 中), 若 $(f(x),f'(x))=1$ 在 $F[x]$ 中, 则存在 $u(x),v(x)\in F[x]$, $u(x)f(x)+v(x)f'(x)=1$

$u(x)f(x)+v(x)f'(x)\in F[x]\subseteq E[x]$, 但是它被 $x-\alpha$ 整除 (矛盾)

"$\Leftarrow$" 若 $(f(x),f'(x))\neq 1$, 存在 $d(x)\mid f(x)$, $d(x)\mid f'(x)$ (在 $F[x]$ 中)

由 扫描全能王 扫描创建

在 $\mathbb{E}[x]$ 中，$\exists \alpha \in \mathbb{E}$，$x-\alpha \mid d(x) \Rightarrow f(\alpha)=f'(\alpha)=0$

$f(x)=(x-\alpha)q(x) \Rightarrow f'(x)=(x-\alpha)q'(x)+q(x) \Rightarrow q(\alpha)=0$

即 $(x-\alpha) \mid q(x) \Rightarrow (x-\alpha)^2 \mid f(x)$.

推论 设 $\mathbb{F}$ 是域，$f(x) \in \mathbb{F}[x]$ 不可约

(1) $\mathrm{char}\,\mathbb{F}=0$，则 $f(x)$ 无重根.

(2) $\mathrm{char}\,\mathbb{F}=p \neq 0$，则 $f(x)$ 有重根 $\Leftrightarrow \exists g(x) \in \mathbb{F}[x]$, $f(x)=g(x^p)$

证明：(1) $f(x)$ 无重根 $\Leftrightarrow (f(x), f'(x))=1$

若 $f(x)$ 有重根，则 $f(x) \mid f'(x)$，$\deg f'(x) < \deg f(x) \Rightarrow f'(x)=0$

设 $f(x)=\sum_{i=0}^{n} a_i x^i$ $\quad f'(x)=0 \Leftrightarrow i a_i = 0 \quad i=1,\cdots,n$

因为 $\mathrm{char}\,\mathbb{F}=0 \quad i a_i = 0 \Rightarrow a_i = 0 \quad i=1,\cdots,n \Rightarrow f(x)=a_0$

与 $f(x)$ 不可约矛盾！

(2) $f(x)$ 有重根 $\xLeftrightarrow[\text{讨论}]{\text{如上}} i a_i = 0 \quad i=1,\cdots,n$ 若 $p \nmid i$，$a_i=0$；若 $p \mid i$，$i a_i = 0$

$\Leftrightarrow f(x)=g(x^p) \quad \exists g(x) \in \mathbb{F}[x]$

定理 设 $\mathbb{F}$ 域，$f(x) \in \mathbb{F}[x]$，$\xrightarrow[\deg f(x)>0]{f(x)\text{不可约}}$ $\mathbb{E}$ 是 $f(x)$ 在 $\mathbb{F}$ 上分裂域，则在 $\mathbb{E}[x]$ 中，$f(x)=c\prod_{i=1}^{\ell}(x-\alpha_i)^k$，$\alpha_i \neq \alpha_j \in \mathbb{E}$，$c \neq 0 \in \mathbb{F}$.

证明：设 $\alpha_1, \alpha_2$ 是 $f(x)$ 的两个不同的根，$\alpha_1, \alpha_2 \in \mathbb{E}$.

由 扫描全能王 扫描创建

在 $\mathbb{E}[x]$ 中，设 $f(x)=(x-\alpha_1)^{k}g(x)$，$g(\alpha_1)\neq 0$，$g(x)\in\mathbb{E}[x]$

$\exists \sigma\in Aut_{\mathbb{F}}\mathbb{E}$，$\sigma(\alpha_1)=\alpha_2$ 则有

$$\sigma(f(x))=f(x)=(x-\alpha_2)^{k}\sigma(g(x))$$

这说明 $\alpha_2$ 的重数 $\geq k$，同理 $\alpha_1$ 的重数 $\geq \alpha_2$ 的重数.

$\Rightarrow$ 所有根的重数相同.

2. 可分多项式

定义 设 $\mathbb{F}$ 域，$f(x)\in\mathbb{F}[x]$ 不可约，$\mathbb{E}$ 为 $f(x)$ 在 $\mathbb{F}$ 上分裂域，若 $f(x)$ 在 $\mathbb{E}[x]$ 中所有因式均是一重因式.

则称 $f(x)$ 是 $\mathbb{F}$ 上可分多项式. 否则称为不可分多项式

命题(1) 特征 $=0$ 的域上不可约多项式是可分的.

(2) 有限域上不可约多项式均可分.

证明：由1中推论.(1) 成立

(2) 设 $\mathbb{F}$ 是有限域，$f(x)\in\mathbb{F}[x]$ 不可约

$Char\,\mathbb{F}=p$

若存在 $g(x)$，$f(x)=g(x^p)$，写 $g(x)=b_s x^s+b_{s-1}x^{s-1}+\cdots+b_1x+b_0$ $\in\mathbb{F}[x]$

考虑 $\mathbb{F}\xrightarrow{\phi}\mathbb{F}$，$x\longmapsto x^p$ 这是一个域同构.(它是域同态，且有逆.

(或直接检查 $\phi$ 是单射，则 $\phi$ 满)

$\mathbb{F}\xrightarrow{\phi^{-1}}\mathbb{F}$，$x\longmapsto x^{p^{n-1}}$ $n=[\mathbb{F}:\mathbb{Z}_p]$，$\forall b_i$，$\exists c_i\in\mathbb{F}$，$b_i=c_i^p$

由 扫描全能王 扫描创建

$g(x^p) = c_s^p x^{ps} + \cdots + c_1^p x^p + c_0^p = (c_s x^s + \cdots + c_1 x + c_0)^p$

$\Rightarrow g(x^p)$可约，与$f(x)$不可约矛盾. 因此，不存在$g(x) \in \mathbb{F}[x]$，

$f(x) = g(x^p) \Rightarrow f(x)$无重根.

定义 设$\mathbb{F}$是一个域，$\mathbb{F}^p = \{a^p \mid a \in \mathbb{F}\}$，若$\mathbb{F}^p = \mathbb{F}$，或$\mathrm{char}\mathbb{F}=0$（$\mathrm{char}\mathbb{F}=p$）

则$\mathbb{F}$称为完全域(perfect field)

定理 完全域上不可约多项式是可分的.

证明：类似于以上命题.

不可分多项式的例子：

设$\mathrm{char}\mathbb{F} = p \neq 0$，$f(x) \in \mathbb{F}[x]$不可约，则$f(x)$不可分$\Leftrightarrow$

$\exists g(x) \in \mathbb{F}[x]$，$f(x) = g(x^p)$. $\quad \forall a \in \mathbb{F}$

$x^p - a$ 〈 $(x-b)^p$ $\quad a \in \mathbb{F}^p$ $a = b^p$, $b \in \mathbb{F}$

$x^p - a$不可约 $\quad a \notin \mathbb{F}^p \Rightarrow$ 不可分

（若可约，则在分裂域中$\exists b$, $b^p = a$ $\quad x^p - a = (x-b)^p = f_1(x) f_2(x)$ $\quad f_1(x) = (x-b)^k \in \mathbb{F}[x]$ $k<p$ 矛盾！）

例 $\mathbb{F} = \mathbb{Z}_p(t)$ $\mathbb{Z}_p$上有理函数域，$f(x) = x^p - t \in \mathbb{F}[x]$

① $f(x)$不可约，若$t = \left(\frac{g(t)}{h(t)}\right)^p \in \mathbb{F}^p \Rightarrow h(t) = 0$ 矛盾！

② $f(x)$不可分，$f'(x) = 0$

3. 可分扩张与不可分扩张.

由 扫描全能王 扫描创建

定义 设$F\subseteq E$代数扩张，$\alpha\in E$，$\alpha$的极小多项式$p(x)\in F[x]$，若$p(x)$可分，则$\alpha$是$F$上可分元. 若$\forall\beta\in E$，$\beta$均是$F$上可分元，则$E$是$F$的可分扩张(separable extension)

否则，是不可分扩张(inseparable extension)

定理 有限可分扩张是单扩张

证明：设$F\subseteq E$，$E$是$F$的有限可分扩张.

Case-1 $F$是有限域，则$E$也是有限域，$E^*$是循环群，生成元为$\alpha$，则$E=F(\alpha)$.

逻辑问题！要保证c也是可分元才可以，事实上由$c\in E$可得c可分

Case-2 $F$是无限域，需证$\forall\alpha,\beta$可分元$\in E$，则存在$c\in E$

$F(\alpha,\beta)=F(c)$ 证明类似于$\mathrm{char}F=0$情形.

~~定理 设$F\subseteq E$，$f(x)\in F[x]$，$\deg f(x)>0$，$E$是$f(x)$在$F$上分裂域，则$E$是$F$的有限可分扩张$\Leftrightarrow|Aut_F E|=[E:F]$~~

定理 设$F\subseteq K$是有限维扩张，令$K=F(\alpha_1,\alpha_2,\cdots,\alpha_r)$

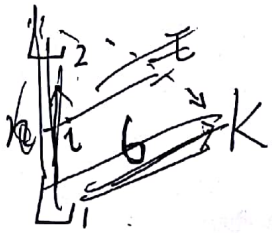
则$K$是可分扩张$\Leftrightarrow\alpha_1,\cdots,\alpha_r$是$F$上可分元

引理 ~~设$L_1\subseteq L_2$有限域扩张，$[L_2:L_1]=n$，$L_1\Rightarrow K$域~~

$L_2=L_1(\alpha_1,\cdots,\alpha_t)$

~~证：且$L_2=K$，~~

令$g_i(x)$是$\alpha_i$的在$L_1$上极小多项式




~~$K$是$\prod_{i=1}^{t}g_i(x)$的分裂域~~

由 扫描全能王 扫描创建

定义 设$F$是一个域，$K,\Omega$是$F$的扩域，令

$$Em_F(K,\Omega)=\{\sigma:K\to\Omega \text{ 域单嵌入} \mid \sigma|_F=id\}$$

引理 设$K$是$F$的代数扩域，$\alpha\in K$，在$F$上极小多项式$p_\alpha(x)$

(a) 若$K=F(\alpha)$则$|Em_F(K,\Omega)|=p_\alpha(x)$的全部互异根个数(记作$n_{p(x)}$). $\Omega$是$F$的代数闭包. α是可分元⇒次数与根个数相等

(b) 设$F\subseteq L\subseteq K$，$K=L(\alpha)$，则

$$|Em_F(K,\Omega)|=|Em_F(L,\Omega)|\cdot n_{p_L(x)}$$

($\alpha$在$L$上极小多项式$p_L(x)$)

证明：(b) 定义$R: Em_F(K,\Omega)\longrightarrow Em_F(L,\Omega)$是自然限制.

$$\sigma\longmapsto \sigma|_L=\sigma'$$

给定$\sigma'\in Em_F(L,\Omega)$，因为$K=L(\alpha)$，只需定义$\sigma'(\alpha)$就可以扩展$\sigma'$到$\sigma:K\to\Omega$，$\alpha$是$p_L(x)$的根，$\sigma'(\alpha)$是$\sigma'(p_L(x))=p_L(x)$的根. $R^{-1}(\sigma')=\{\sigma:K\to\Omega \mid \sigma|_L=\sigma'\}$元素个数$=n_{p_L(x)}$.

命题 设$F\subseteq K$有限域扩张，则$|Em_F(K,\Omega)|\le[K:F]$

等号成立$\Leftrightarrow$ $K$是$F$的有限可分扩张. 相等⇒ K是可分扩张

证明：~~(⇒设$K$是$F$的有限可分扩张~~ 关于$[K:F]$作归纳

选择$\alpha\in K$，中间域$L\neq K$，使得$K=L(\alpha)$，$F\subseteq L\subseteq K=L(\alpha)$. $\alpha\notin L$

则由引理 $|Em_F(K,\Omega)|=|Em_F(L,\Omega)|\cdot n_{p_L(x)}$.

由 扫描全能王 扫描创建

(1) 若 $K$ 是 $F$ 的有限可分扩张，则 $L$ 也是 $F$ 的有限可分扩张. 由归纳假设 $|Em_F(L,\overline{F})| = [L:F]$

$\alpha$ 在 $L$ 上可分（因为 $\alpha$ 在 $L$ 上极小多项式整除 $P_F(x)$），$K = L(\alpha)$

$\Rightarrow |Em_F(K,\overline{F})| = [L:F]\cdot[K:L] = [K:F]$

(2) 若 $K$ 不是 $F$ 上可分扩张，存在 $\beta \in K$，$\beta$ 不是 $F$ 上可分元，若 $K = F(\beta)$，由引理(a). $\beta$ 的极小多项式 $q_F(x)$

$$|Em_F(K,\overline{F})| \neq \deg q_F(x) = [K:F]$$

若 $K \neq F(\beta)$，存在中间域 $L$，$\beta \in L$，$L$ 不是 $F$ 的可分扩张

通过归纳，$|Em_F(L,\overline{F})| < [L:F]$. $L(\alpha) = K$.

$\Rightarrow |Em_F(K,\overline{F})| < [L:F]\cdot[K:L] = [K:F]$

定理的证明："$\Rightarrow$" 显然.

"$\Leftarrow$" $K = F(\alpha_1, \alpha_2, \cdots, \alpha_r) = K_r \supseteq K_{r-1} = F(\alpha_1, \cdots, \alpha_{r-1}) \supseteq \cdots \supseteq F(\alpha_1) = K_1$

则 $K_{i+1} = K_i(\alpha_{i+1})$ $\alpha_{i+1}$ 是 $F$ 上可分元 $\Rightarrow$ 是 $K_i$ 上可分元.

$$|Em_F(K,\overline{F})| = |Em_F(K_{r-1},\overline{F})|\cdot[K_r:K_{r-1}] = \cdots$$

$$= [K:F]$$

由命题，它是可分扩张.

由 扫描全能王 扫描创建