抽象代数学

1. 不可约多项式的零点

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

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

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

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

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

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

证明: "$\Longrightarrow$" 在 $\mathbb{E}[x]$ 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 $\mathbb{E}[x]$ 中), 若 $(f(x),f'(x))=1$ 在 $\mathbb{F}[x]$ 中, 则存在 $u(x),v(x)\in\mathbb{F}[x]$, $u(x)f(x)+v(x)f'(x)=1$

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

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

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

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

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

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

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

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

与 $f(x)$ 不可约矛盾！

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

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

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

证明：设 α_1,α_2 是 $f(x)$ 的两个不同的根，$\alpha_1,\alpha_2\in\mathbb{E}$.

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

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

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

这说明 α_2 的重数 $\geq k$，同理 α_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

$\mathrm{char}\,\mathbb{F}=p$

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 ϕ 是单射，则 ϕ 满）

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

$g(x^p) = C_s^p x^{ps} + \cdots + C_1^p x^p + C_0^p = (C_s x^s + \cdots + C_1 x + C_0)^p$

$\Rightarrow g(x^p)$ 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 $\mathbb{F}^p = \mathbb{F}$（$\mathrm{char}\,\mathbb{F} = p$），或 $\mathrm{char}\,\mathbb{F} = 0$

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 $\Leftrightarrow$

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

$$x^p - a \begin{cases} (x-b)^p & a \in \mathbb{F}^p \quad a = b^p,\ b \in \mathbb{F} \\ x^p - a \text{ 不可约} & a \notin \mathbb{F}^p \Rightarrow \text{不可分} \end{cases}$$

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

定义 设$\mathbb{F}\subseteq\mathbb{E}$代数扩张，$\alpha\in\mathbb{E}$，$\alpha$的极小多项式$p(x)\in\mathbb{F}[x]$，若$p(x)$可分，则$\alpha$是$\mathbb{F}$上可分元。若$\forall\beta\in\mathbb{E}$，$\beta$均是$\mathbb{F}$上可分元，则$\mathbb{E}$是$\mathbb{F}$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$\mathbb{F}\subseteq\mathbb{E}$，$\mathbb{E}$是$\mathbb{F}$的有限可分扩张.

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

Case-2 $\mathbb{F}$是无限域，需证$\forall\alpha,\beta$可分元$\in\mathbb{E}$，则存在$c\in\mathbb{E}$ $\mathbb{F}(\alpha,\beta)=\mathbb{F}(c)$ 证明类似于$\mathrm{char}\mathbb{F}=0$情形.

~~定理 设$\mathbb{F}\subseteq\mathbb{E}$，$f(x)\in\mathbb{F}[x]$，$\deg f(x)>0$，$\mathbb{E}$是$f(x)$在$\mathbb{F}$上分裂域，则$\mathbb{E}$是$\mathbb{F}$的有限可分扩张$\Longleftrightarrow|\mathrm{Aut}_{\mathbb{F}}\mathbb{E}|=[\mathbb{E}:\mathbb{F}]$~~

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

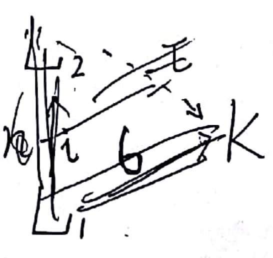
则K是可分扩张$\Leftrightarrow\alpha_1,\cdots,\alpha_r$是$\mathbb{F}$上可分元

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

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

~~嵌入：且$L_2\subseteq K$，~~

~~令$g_i(x)$是α_i的在L_1上极小多项式~~



~~K是$\prod_{i=1}^{t}g_i(x)$的分裂域~~

定义 设$\mathbb{F}$是一个域，$K,\mathbb{E}$是$\mathbb{F}$的扩域，令

$$Em_{\mathbb{F}}(K,\mathbb{E}) := \{\sigma: K\to \mathbb{E} \text{ 域单嵌入} \mid \sigma|_{\mathbb{F}} = id\}$$

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

(a) 若$K=\mathbb{F}(\alpha)$ 则$|Em_{\mathbb{F}}(K,\overline{\mathbb{F}})| = P_{\mathbb{F}}(x)$的全部互异根个数（记作$n_{p(x)}$）. $\overline{\mathbb{F}}$是$\mathbb{F}$的代数闭包.

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

α在$\mathbb{L}$上极小多项式$P_{\mathbb{L}}(x)$

$$|Em_{\mathbb{F}}(K,\overline{\mathbb{F}})| = |Em_{\mathbb{F}}(\mathbb{L},\overline{\mathbb{F}})|\cdot n_{P_{\mathbb{L}}(x)}.$$

证明：(b) 定义 $R: Em_{\mathbb{F}}(K,\overline{\mathbb{F}}) \longrightarrow Em_{\mathbb{F}}(\mathbb{L},\overline{\mathbb{F}})$，$\sigma \longmapsto \sigma|_{\mathbb{L}}=\sigma'$ 是自然限制.

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

命题 设$\mathbb{F}\subseteq K$有限域扩张，则$|Em_{\mathbb{F}}(K,\overline{\mathbb{F}})|\le[K:\mathbb{F}]$

等号成立$\Leftrightarrow K$是$\mathbb{F}$的有限可分扩张.

证明：~~(1)设K是F的有限可分扩张~~ 关于$[K:\mathbb{F}]$作归纳

选择$\alpha\in K$，中间域$\mathbb{L}$，使得$K=\mathbb{L}(\alpha)$，$\mathbb{F}\subseteq \mathbb{L}\subseteq K=\mathbb{L}(\alpha)$，$\alpha\notin \mathbb{L}$

则由引理 $|Em_{\mathbb{F}}(K,\overline{\mathbb{F}})|=|Em_{\mathbb{F}}(\mathbb{L},\overline{\mathbb{F}})|\cdot n_{P_{\mathbb{L}}(x)}$.