可分多项式与完备域

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

$$f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+a_1$$

为 $f(x)$ 的**形式微商**.

注. 这里只是形式的定义，没有用到极限，但很多性质与分析中相同.

注. 不一定有 $\deg f'(x)=\deg f(x)-1$，因为 na_n 可能为零. 当 $\mathrm{Ch}F=0$ 时，上式成立.

性质 1. 对任意 $a\in F$，有 $a'=0$，但反之不一定，只有当 $\mathrm{Ch}F=0$ 时条件充要.

例 1. 设 p 为素数，$f(x)=x^p-\alpha\in\mathbb{Z}_p(\alpha)[x]$，其中 α 是 $\mathbb{Z}_p$ 上的超越元，则 $f'(x)=px^{p-1}=0$.

性质 2. $x'=1$.

性质 3. $(cf(x))'=cf'(x),\ \forall c\in F$.

性质 4. $(f(x)+g(x))'=f'(x)+g'(x)$.

性质 5. $(f(x)g(x))'=f'(x)g(x)+f(x)g'(x)$.

性质 6. $\deg f'(x)\leqslant\deg f(x)$.

引理 1. 设 K 是 $f(x)\in F[x]$ 的分裂域，$\alpha\in K$ 是 $f(x)$ 的一个 k 重根，则

1. 当 $\mathrm{Ch}F\nmid k$ 时，α 是 $f'(x)$ 的 $k-1$ 重根.
2. 当 $\mathrm{Ch}F\mid k$ 时，α 至少是 $f'(x)$ 的 k 重根.

证明. 在 $K[x]$ 中，记 $f(x)=(x-\alpha)^kg(x)$，$g(\alpha)\neq 0$. 则由微商的乘法法则，有

$$f'(x)=(x-\alpha)^{k-1}\left[kg(x)+(x-\alpha)g'(x)\right].$$

当 $\mathrm{Ch}F\nmid k$ 时，$kg(\alpha)\neq 0$，故 α 是 $f'(x)$ 的 $k-1$ 重根.
当 $\mathrm{Ch}F\mid k$ 时，$kg(\alpha)=0$ 且 $(\alpha-\alpha)g'(\alpha)=0$，故 α 至少是 $f'(x)$ 的 k 重根. □

注. α 是 $f(x)$ 的单根能推出 α 不是 $f'(x)$ 的根，因为任何特征都不能整除 1. 那反过来呢？

注. 设 $f(x)$ 在分裂域中的所有根 α_i，$i=1,2,\cdots,s$ 分别是 $f(x)$ 的 k_i 重根，且 $\mathrm{Ch}F\mid k_i$，则由上述引理，α_i 至少是 $f'(\alpha)$ 的 k_i 重根，这与“$\deg f'(x)\leqslant\deg f(x)$”是否矛盾？

定理 1. 设 K 是 $f(x)\in F[x]$ 的分裂域，则 $f(x)$ 在 K 中无重根当且仅当 $(f(x),f'(x))=1$.

证明. $f(x)$ 有重根 $\iff$ $f(x)$ 与 $f'(x)$ 有公根 $\iff$ $f(x)$ 与 $f'(x)$ 有次数大于等于 1 的公因式 $\iff$ $(f(x),f'(x))\neq 1$. □

定理 2. 设不可约多项式 $p(x)\in F[x]$，则 $p(x)$ 在其分裂域 K 中无重根当且仅当 $p'(x)\neq 0$.

证明. $p(x)$ 无重根 $\iff$ $(p(x),p'(x))=1$ $\iff$ $(p(x),p'(x))\neq p(x)$ $\iff$ $p(x)\nmid p'(x)$ $\iff$ $p'(x)\neq 0$. □

例 2. 设 p 是素数，α 是 $\mathbb{Z}_p$ 上的超越元. 多项式 $x^p-\alpha\in\mathbb{Z}_p(\alpha)[x]$ 有重根，因为 $(x^p-\alpha)'=px^{p-1}=0$.

推论 1. 若 $\mathrm{Ch}F=0$，则 $F[x]$ 中任一不可约多项式在分裂域中都无重根.

证明. 因为 $\deg p'(x)=\deg p(x)-1\geqslant 0$，故 $p'(x)\neq 0$，即 $p(x)$ 无重根. □

定义 2 (可分多项式)**.** 设 F 是域，若 $f(x)\in F[x]$ 的每个不可约因式在分裂域中都无重根，则称 $f(x)$ 是 F 上的**可分多项式**.

注. 可分多项式与基域 F 有关，因为在不同的基域下，不可约因式会改变.

由上述定义可以简化一些命题的叙述.

命题 1. 设 $f(x)\in F[x]$ 的分裂域为 E，则 E 的 F-自同构的个数不超过 $[E:F]$，等号成立当且仅当 $f(x)$ 是 F 上的可分多项式.

命题 2. 不可约多项式 $p(x)\in F[x]$ 在 F 上可分当且仅当 $p'(x)\neq 0$.

命题 3. 若 $\mathrm{Ch}F=0$，则 $F[x]$ 中任一多项式均可分.

引理 2. 设 $\mathrm{Ch}F=p\neq 0$，$f(x)\in F[x]$ 不可约，则 $f(x)$ 在 F 上不可分当且仅当存在不可约多项式 $g(x)\in F[x]$ 使 $f(x)=g(x^p)$.

证明. “$\Leftarrow$”: 记 $g(x)=\sum\limits_{i=0}^{n}a_ix^i$，则 $f(x)=\sum\limits_{i=0}^{n}a_i(x^p)^i=\sum\limits_{i=0}^{n}a_ix^{pi}$，则 $f'(x)=\sum\limits_{i=0}^{n}pia_ix^{pi-1}=0$. 由于 $f(x)$ 不可约，故 $f(x)$ 不可分.

”$\Rightarrow$”: 记 $f(x)=\sum\limits_{j=0}^{n}a_jx^j$，因为 $f(x)$ 不可分不可约，故

$$f'(x)=\sum_{j=0}^{n}ja_jx^{j-1}=0\Rightarrow ja_j=0.$$

若 $a_j \neq 0$,则 $p \mid j$,即只有 $a_0, a_p, a_{2p}, \cdots, a_{mp}$ 可能不为零,其中 m 满足 $n = mp+r, 0 \leqslant r < p$. 所以

$$f(x) = \sum_{i=0}^{m} a_{ip} x^{ip} = \sum_{i=0}^{m} a_{ip} (x^p)^i.$$

令 $g(x) = \sum\limits_{i=0}^{m} a_{ip} x^i$，则 $f(x) = g(x^p)$.

反设 $g(x)$ 可约，有 $g(x) = g_1(x)g_2(x)$，则 $f(x) = g(x^p) = g_1(x^p)g_2(x^p)$，这与 $f(x)$ 不可约矛盾，故 $g(x)$ 不可约. □

定理 3. 设 $\mathrm{Ch}F = p \neq 0$，$f(x)$ 是 $F[x]$ 中不可分不可约多项式，K 是 $f(x) \in F[x]$ 的分裂域，则在 $K[x]$ 中，

$$f(x) = c(x-\alpha_1)^{p^e}(x-\alpha_2)^{p^e}\cdots(x-\alpha_r)^{p^e},\ \alpha_i \neq \alpha_j, \forall i \neq j,\ e \in \mathbb{N}.$$

且有 $F[x]$ 中可分的不可约多项式

$$h(x) = c(x-\alpha^{p^e})(x-\alpha_2^{p^e})\cdots(x-\alpha_r^{p^e})$$

使 $f(x) = h(x^{p^e})$.

证明. 因为 $f(x)$ 不可分，由引理2，存在不可约多项式 $g_1(x) \in F[x]$ 使得 $f(x) = g_1(x^p)$.

若 $g_1(x)$ 可分，取 $h(x) = g_1(x)$. 否则，由引理2，存在不可约多项式 $g_2(x) \in F[x]$ 使 $g(x) = g_2(x^p)$，则 $f(x) = g_1(x^p) = g_2(x^{p^2})$. 以此类推，由于

$$\deg f(x) > \deg g_1(x) > \deg g_2(x) > \cdots,$$

经有限步后总能得到可分的不可约多项式 $g_e(x)$ 使 $f(x) = g_e(x^{p^e})$，取 $h(x) = g_e(x)$.

因为 $h(x)$ 可分，故在其分裂域中，

$$h(x) = c(x-\beta_1)(x-\beta_2)\cdots(x-\beta_r), \qquad \beta_i \neq \beta_j, \forall i \neq j.$$

于是 $f(x) = c(x^{p^e}-\beta_1)(x^{p^e}-\beta_2)\cdots(x^{p^e}-\beta_r)$.

记 α_i 是 $x^{p^e}-\beta_i$ 在分裂域中的一个根，则 $\alpha_i^{p^e}-\beta_i = 0$，$\beta_i = \alpha_i^{p^e}$. 于是

$$x^{p^e}-\beta_i = x^{p^e}-\alpha_i^{p^e} = (x-\alpha)^{p^e},$$

故

$$f(x) = c(x-\alpha_1)^{p^e}(x-\alpha_2)^{p^e}\cdots(x-\alpha_r)^{p^e},\ e \in \mathbb{N}.$$

对任意 $i \neq j$，若 $\alpha_i = \alpha_j$，则 $\alpha_i^{p^e} = \alpha_j^{p^e}$，与 $\beta_i \neq \beta_j$ 矛盾. □

注. $f(x) = c(x-\alpha_1)^{p^e}(x-\alpha_2)^{p^e}\cdots(x-\alpha_r)^{p^e} = c\left[(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_r)\right]^{p^e}$.

注. 称 $f(x)$ 不同根的个数 r 为 $f(x)$ 的**简约次数**，记为 $\mathrm{red}f(x)$. 有 $\mathrm{red}f(x) = \deg h(x)$.

注. $\deg f(x) = \mathrm{red}f(x) \cdot p^e$，即 $p^e = \dfrac{\deg f(x)}{\mathrm{red}f(x)}$.

注. 不可约多项式 $f(x) \in F[x]$ 可分当且仅当 $\deg f(x) = \mathrm{red}f(x)$.

定义 3 (完备域)**.** 设 F 是域，若 $F[x]$ 中任一多项式都是可分多项式，则称 F 为**完备域**.

注. 由可分多项式的定义，完备域只需任一不可约多项式可分即可. 由推论*1*，特征为 0 的域都是完备域.

定理 4. 设 F 是域，$\mathrm{Ch}F = p \neq 0$，则 F 是完备域的充要条件是

$$F^p = F, \qquad F^p = \{a^p \mid a \in F\}.$$

证明. ”$\Leftarrow$”: 反设 $F[x]$ 中存在不可分不可约多项式 $f(x)$，由引理2，存在不可约多项式 $g(x) \in F[x]$ 使 $f(x) = g(x^p)$. 记 $g(x) = \sum_{i=0}^{n} a_i x^i$，$b_i^p = a_i$，则

$$f(x) = \sum_{i=0}^{n} a_i (x^p)^i = \sum_{i=0}^{n} b_i^p x^{pi} = \left(\sum_{i=0}^{n} b_i x^i\right)^p.$$

这与 $f(x)$ 不可约矛盾.

“$\Rightarrow$”：即证对任意 $b \in F$，存在 $a \in F$ 使得 $b = a^p$. 令 $f(x) = x^p - b \in F[x]$，则 $f'(x) = px^{p-1} = 0$，$f(x)$ 有重根，而 F 是完备域，故 $f(x)$ 在 F 中可约.

设 $f(x) = g(x)h(x)$，$0 < \deg g(x), \deg h(x) < p$，$g(x), h(x) \in F[x]$. 记 θ 是 $f(x) = x^p - b$ 在扩域中的一个根，则 $\theta^p - b = 0$，$b = \theta^p$. 于是

$$f(x) = x^p - b = x^p - \theta^p = (x - \theta)^p.$$

故在 $f(x) \in F[x]$ 的分裂域中，记 $\deg g(x) = r$，则 $g(x) = (x - \theta)^r \in F[x]$，故 $\theta^r \in F$. 又 $\theta^p = b \in F$，p 是素数，于是 $(r, p) = 1$. 存在 u, v 使得 $ur + vp = 1$. 于是

$$\theta = \theta^{ur+vp} = (\theta^r)^u (\theta^p)^v \in F.$$

令 $a = \theta$ 便完成证明. □

注. 定理的条件即为 F 中任一元素可在自身 F 中开 p 次方.

注. 事实上，特征为素数 p 的域 F 上，若 $a \in F$ 能开 p 次方，则 p 次方根是唯一的. 因为对 $b_1^p = b_2^p = a$，有 $b_1^p - b_2^p = (b_1 - b_2)^p = 0$，于是 $b_1 = b_2$.

定理 5. 有限域是完备域.

证明. 不妨设 $\mathrm{Ch}F=p\neq 0$，令 $\sigma:F\to F,\ a\mapsto a^p$，可以证明 σ 是良定义的且是单射. 而 F 有限，故 σ 也是满射. 故 $\sigma(F)=F$，即 $F^p=F$，故 F 是完备域. $\square$

注. 事实上，对任意 $a,b\in F$，有

$$\sigma(a+b)=(a+b)^p=a^p+b^p=\sigma(a)+\sigma(b),$$

$$\sigma(ab)=(ab)^p=a^pb^p=\sigma(a)\sigma(b),$$

于是 σ 是 F-自同构，称为 ***Frobenius* 自同构**.

定理 6. 完备域 F 的代数扩张 K 是完备域.

证明. 不妨设 $\mathrm{Ch}F=p\neq 0$，即证对任意 $\alpha\in K$，存在 $\beta\in K$ 使得 $\beta^p=\alpha$. 令 $\sigma:K\to K,\ a\mapsto a^p$，可以证明 σ 是单同态. 记 $E=F(\alpha)$，则 $\sigma\big|_E:E\to\sigma(E)$ 是同构. 有

$$E\cong\sigma(E)=E^p\subset E.$$

下证 $\sigma(E)=E$. 因为

$$\sigma(E)=\sigma(F(\alpha))=\sigma(F)(\sigma(\alpha))=F^p(\sigma(\alpha))=F(\sigma(\alpha)),$$

于是 $F\subset\sigma(E)\subset E$. 由于 α 是 F 上的代数元，故 $[E:F]$ 的有限扩张. 有

$$[E:F]=[E:\sigma(E)]\,[\sigma(E):F]\,.$$

又 $E\cong\sigma(E)$，故 $[E:F]=[\sigma(E):F]$，于是 $[E:\sigma(E)]=1$，故 $E=\sigma(E)$. $\square$