唯一析因环上多项式环

本节总假定 R 是 UFD. 约定对任意 $a \in R$，有 $a \mid 0$，最大公因子 $(a, 0) = a$.

定义 1 (容度). 设 $0 \neq f(x) = \sum_{k=0}^{n} a_k x^k \in R[x]$，称 $(a_0, a_1, \cdots, a_n)$ 为 $f(x)$ 的**容度**，记作 $c(f(x))$.

注. 容度在相伴意义下唯一.

定义 2 (本原多项式). 设 $0 \neq f(x) \in R[x]$，若 $c(f(x)) \sim 1$，则称 $f(x)$ 为**本原多项式**.

引理 1. 设 $R[x]$ 是唯一析因环 R 上的多项式环，记 S 为 $R[x]$ 中本原多项式的集合，则

1. 对任意非零多项式 $f(x) \in R[x]$，存在 $f_1(x) \in S$ 使得

$$f(x) = c(f) f_1(x).$$

且分解在相伴意义下唯一.

2. 次数大于零的不可约多项式是本原多项式.

3. (Gauss 引理) 本原多项式的积仍为本原多项式.

证明. 1. 设 $f(x) = \sum_{k=0}^{n} a_k x^k \neq 0$，记 $d = c(f) = (a_0, a_1, \cdots, a_n)$，于是对任意 $k = 0, 1, \cdots, n$，存在 a'_k 使得 $a_k = d a'_k$，且 $(a'_0, a'_1, \cdots, a'_n) \sim 1$，于是多项式 $f_1(x) = \sum_{k=0}^{n} a'_k x^k \in S$，且满足 $f(x) = c(f) f_1(x)$.

设另有 $d' \in R^*, f_2(x) \in S$ 使得 $f(x) = d' f_2(x)$，则 $c(f_2) \sim 1$，于是 $d' c(f_2) \sim c(f) = d$，即 $d' \sim d$. 于是存在 $u \in U$ 使得 $d' = ud$，则 $d' f_2(x) = u d f_2(x) = d f_1(x)$，于是由消去律，有 $f_1(x) \sim f_2(x)$. 故分解在相伴意义下是唯一的.

2. 设 $f(x) \in R[x]$ 不可约且 $\deg f(x) > 0$，则由结论 1，存在 $f_1(x) \in S$ 使得 $f(x) = c(f) f_1(x)$，由于 $f(x)$ 不可约，于是 $c(f) \in U$，则 $c(f) \sim 1$，故 $f(x) \in S$.

3. 设 $f(x) = \sum_{k=0}^{n} a_k x^k$，$g(x) = \sum_{k=0}^{m} b_k x^k$，则

$$h(x) = f(x) g(x) = \sum_{k=0}^{m+n} c_k x^k, \quad c_k = \sum_{i+j=k} a_i b_j.$$

假设 $h(x) \notin S$，则存在素元素 $p \in R$ 使得 $p \mid c_k$，对任意 $k = 0, 1, \cdots, m+n$. 而 $f(x), g(x) \in S$，于是存在 r, s 使得

$$p \mid a_i,\ i = 0, 1, \cdots, r-1,\ p \nmid a_r,$$

$$p \mid b_j,\ j = 0, 1, \cdots, s-1,\ p \nmid b_s,$$

对于第 $r+s$ 项，有

$$c_{r+s} = \sum_{i+j=r+s} a_i b_j = a_r b_s + \sum_{\substack{i<r \\ i+j=r+s}} a_i b_j + \sum_{\substack{j<s \\ i+j=r+s}} a_i b_j,$$

由于

$$p \mid c_{r+s} \quad p \left| \sum_{\substack{i<r \\ i+j=r+s}} a_i b_j, \quad p \right| \sum_{\substack{j<s \\ i+j=r+s}} a_i b_j,$$

推出 $p \mid a_r b_s$，这就导出矛盾. 故 $h(x) \in S$. □

注. 本原多项式未必是不可约多项式，例如 $x^2 - 1 \in \mathbb{Z}[x]$ 是可约的本原多项式. *Gauss* 引理的证明与高等代数中几乎完全一致.

引理 2. 设 F 是唯一析因环 R 的分式域，于是 $R[x] \subset F[x]$. 设 S 是 $R[x]$ 中本原多项式的集合，记 $R[x]$ 中的相伴关系为 $\overset{R}{\sim}$，$F[x]$ 中的相伴关系为 $\overset{F}{\sim}$，则

1. 对任意非零多项式 $f(x) \in F[x]$，存在 $g(x) \in S$ 使得 $f(x) \overset{F}{\sim} g(x)$ 且 $g(x)$ 在 $\overset{R}{\sim}$ 下唯一.
2. 设 $f_1(x), f_2(x) \in F[x]$，$g(x), g_1(x), g_2(x) \in S$ 且

$$f_1(x) \overset{F}{\sim} g_1(x), \quad f_2(x) \overset{F}{\sim} g_2(x), \quad f_1(x) f_2(x) \overset{F}{\sim} g(x),$$

   则 $g_1(x) g_2(x) \overset{R}{\sim} g(x)$.

3. 设 $f(x) \in R[x]$，$\deg f(x) \geqslant 1$ 且 $f(x)$ 在 $R[x]$ 中不可约，则 $f(x)$ 在 $F[x]$ 中也不可约.

证明. 1. 设 $f(x) = \sum_{k=0}^{n} d_k x^k \in F[x]$，即 $d_k \in F$，则存在 $a_k, b_k \in R$ 且 $b_k \neq 0$ 使得 $d_k = \frac{a_k}{b_k}$. 令 $b = b_0 b_1 \cdots b_n$，则

$$d_k b = a_k \prod_{i \neq k} b_i \in R, \quad k = 0, 1, \cdots, n,$$

再令 $d = (d_0 b, d_1 b, \cdots, d_n b)$，则有 $c_k = \frac{d_k b}{d} \in R$ 且 $(c_0, c_1, \cdots, c_n) \overset{R}{\sim} 1$. 而

$$f(x) = \frac{d}{b} \sum_{k=0}^{n} c_k x^k = \frac{d}{b} g(x),$$

其中，$0 \neq \frac{d}{b} \in F$，$g(x) = \sum_{k=0}^{n} c_k x^k \in R[x]$，又 $(c_0, c_1, \cdots, c_n) \overset{R}{\sim} 1$，于是 $g(x) \in S$，有 $f(x) \overset{F}{\sim} g(x)$.

设 $f(x) \overset{F}{\sim} g_1(x)$，$g_1(x) \in S$. 因为 $f(x) \overset{F}{\sim} g(x)$，于是由传递性，$g_1(x) \overset{F}{\sim} g(x)$，存在 $u \in F^*$ 使得 $g_1(x) = ug(x)$. 存在 $p, q \in R$ 使得 $u = \dfrac{p}{q}$，于是令 $\tilde{f}(x) = pg(x) = qg_1(x) \in R$，由引理1的结论 1 可知 $g_1(x) \overset{R}{\sim} g(x)$.

2. 由于相伴是同余关系，于是

$$f_1(x)f_2(x) \overset{F}{\sim} g_1(x)g_2(x) \overset{F}{\sim} g(x).$$

由于本原多项式的积仍是本原多项式，于是 $g_1(x)g_2(x) \in S$. 由结论 1，$g_1(x)g_2(x) \overset{R}{\sim} g(x)$.

3. 反设 $f(x)$ 在 $F(x)$ 中可约，由于 F^* 中元素都是单位，即 $f(x)$ 的平凡真因子，于是存在 $f_1(x)$，$f_2(x)$ 使得 $f(x) = f_1(x)f_2(x)$ 且 $\deg f_1(x), \deg f_2(x) \geqslant 1$. 由结论 1，存在 $g_1(x), g_2(x) \in S$ 使得 $f_1(x) \overset{F}{\sim} g_1(x)$，$f_2(x) \overset{F}{\sim} g_2(x)$. 由相伴关系是同余关系，有

$$f(x) = f_1(x)f_2(x) \overset{F}{\sim} g_1(x)g_2(x).$$

由于 $f(x)$ 是 $R[x]$ 上的不可约多项式，由引理1的结论 2 得 $f(x) \in S$. 再由本引理的结论 2，因为 $f_1(x), f_2(x) \in F$，$f(x), g_1(x), g_2(x) \in S$ 且

$$f_1(x) \overset{F}{\sim} g_1(x), \quad f_2(x) \overset{F}{\sim} g_2(x), \quad f_1(x)f_2(x) \overset{F}{\sim} f(x),$$

于是有 $g_1(x)g_2(x) \overset{R}{\sim} f(x)$，这与条件 $f(x)$ 在 R 上不可约矛盾. □

定理 1. 唯一析因环上的一元多项式环是唯一析因环.

证明. 设 $f(x)$ 是唯一析因环 R 中的多项式环，不妨设 $\deg f(x) > 0$. 由引理1的结论 1，存在 $d \in R, g(x) \in S$ 使得 $f(x) = dg(x)$. 因为 R 是 UFD，于是存在不可约元 $p_1, p_2, \cdots, p_t$ 使得 $d = p_1p_2 \cdots p_t$. 这些 p_i 在 $R[x]$ 中也不可约.

因为 $d \in R$，于是 $\deg f(x) = \deg g(x)$. 设 F 是 R 的分式域，则 $g(x) \in F[x]$ 有分解

$$g(x) = g_1(x)g_2(x) \cdots g_r(x).$$

其中 $g_i(x)$ 为 $F[x]$ 中不可约多项式. 由引理2的结论 1，存在 $p_i(x) \in S$ 使得 $g_i(x) \overset{F}{\sim} p_i(x)$，于是

$$g(x) \overset{F}{\sim} p_1(x)p_2(x) \cdots p_r(x).$$

又因为 $g(x), p_i(x) \in S$，于是

$$g(x) \overset{R}{\sim} p_1(x)p_2(x) \cdots p_r(x).$$

不妨设 $g(x) = p_1(x)p_2(x) \cdots p_r(x)$，由于 $p_i(x)$ 在 $F[x]$ 中不可约且 $p_i \in S$，于是 $p_i(x)$ 在 $R[x]$ 中也不可约. 于是 $f(x)$ 有分解

$$f(x) = p_1p_2 \cdots p_tp_1(x)p_2(x) \cdots p_r(x).$$

满足有限析因条件.

设 $f(x)$ 还有分解

$$f(x)=q_1q_2\cdots q_{t'}q_1(x)q_2(x)\cdots q_s(x),$$

其中 q_i 是 R 中不可约元，$q_j(x)$ 是 $R[x]$ 中不可约多项式且 $\deg q_j(x)>0$，由引理1的结论 2 有 $q_j(x)\in S$，由引理1的结论 3，有 $q_1q_2\cdots q_{t'}\in S$. 由引理1的结论 1，有

$$p_1p_2\cdots p_t\overset{R}{\sim}q_1q_2\cdots q_{t'},$$

$$p_1(x)p_2(x)\cdots p_r(x)\overset{R}{\sim}q_1(x)q_2(x)\cdots q_s(x).$$

不妨设 $p_1p_2\cdots p_t=q_1q_2\cdots q_{t'}$. 由于 R 是 UFD，于是 $t=t'$ 且存在 $\pi_1\in S_t$ 使得 $p_i=q_{\pi_1(i)}$. 由引理2的结论 3 知，$p_i(x),q_i(x)$ 均为 $F[x]$ 中的不可约多项式. 而 $F[x]$ 是 Euclid 环，进而是 UFD，于是 $r=s$ 且存在 $\pi_2\in S_r$ 使得 $p_i(x)=q_{\pi_2(i)}(x)$. 又由引理2的结论 1 可得 $p_i(x)\overset{R}{\sim}q_{\pi_2(i)}(x)$，于是在相伴意义下分解唯一，故 $R[x]$ 是唯一析因环. □

推论 1. 唯一析因环上 n 元多项式环是唯一析因环.

证明. 对 n 作归纳法. 有 $R[x_1,x_2,\cdots,x_n]=R[x_1,x_2,\cdots,x_{n-1}][x_n]$ 归结为一元多项式环. □

定理 2 (Eisenstein 判别法)**.** 设 F 是唯一析因环 R 的分式域，$f(x)=\sum_{k=0}^{n}a_kx^k\in R[x]$，$n>1$ 且 $a_n\neq0$. 若有素元素 $p\in R$ 满足

1. $p\nmid a_n$;
2. $p\mid a_k,\ k=0,1,\cdots,n-1$;
3. $p^2\nmid a_0$,

则 $f(x)$ 是 $F[x]$ 中不可约元素.

证明. 由引理2的结论 3，只需证明 $f(x)$ 在 $R[x]$ 中不可约即可. 反设 $f(x)=g(x)h(x)$，其中 $g(x)=\sum_{k=0}^{r}b_kx^k$，$h(x)=\sum_{k=0}^{s}c_kx^k$ 是次数大于零的 $R[x]$ 中多项式，则

$$r+s=n,\quad a_k=\sum_{i+j=k}b_ic_j,\quad p\mid a_0,\quad p^2\nmid a_0.$$

设 $p\mid b_0$，$p\nmid c_0$. 又 $p\nmid a_n$，故 $p\nmid b_r$ 且 $p\nmid c_s$. 于是存在 t，使得 $p\mid b_i,\ i=0,1,\cdots,t-1$ 但 $p\nmid b_t$. 而

$$a_t=\sum_{i+j=t}b_ic_j=b_tc_0+\sum_{\substack{i<t\\i+j=t}}b_ic_j.$$

由于 $p\left|\sum_{\substack{i<t\\i+j=t}}b_ic_j\right.$ 但 $p\nmid b_tc_0$，于是 $p\nmid a_t$. 这与条件 2 矛盾. □

例 1. 设 p 是素数，则 $f(x)=x^{p-1}+x^{p-2}+\cdots+1\in\mathbb{Q}[x]$ 是不可约多项式.

证明. 令 $g(x)=f(x+1)$，则

$$g(x)=\frac{(x+1)^p-1}{(x+1)-1}=\sum_{k=1}^{p}\binom{p}{k}x^{k-1}.$$

其中最高项系数为 1，$p\mid\binom{p}{k},\ k=1,2,\cdots,p-1$，常数项为 p 满足 $p^2\nmid p$. 于是由 Eisenstein 判别法可知 $g(x)$ 在 $\mathbb{Q}[x]$ 上不可约，进而 $f(x)$ 不可约. □