## 0.1 唯一析因环的多项式环

**定义 0.1 (容度)**

设 $R$ 为唯一析因环,$f(x)=\sum_{k=0}^{n} a_k x^k \in R[x]$. 若 $f(x)\neq 0$, 则称 $a_0,a_1,\cdots,a_n$ 的最大公因子为 $f(x)$ 的**容度**, 记为 $c(f(x))$ 或 $c(f)$.

注 由引理????知 $f(x)$ 的容度 $c(f)$ 在相伴意义下是唯一的. 由引理????易知 $c(df(x))=d\cdot c(f(x)),\forall d\in R$.

**定义 0.2 (本原多项式)**

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

注 设 $R[x]$ 的单位群也就是 $R$ 的单位群 $U$, 于是若 $f(x)\in U$, 则 $c(f)\sim 1$.

**定理 0.1**

设 $R[x]$ 是唯一析因环 $R$ 上的一元多项式环, 则有下列结论:

(1) $R[x]$ 中任一非零多项式 $f(x)$ 是 $c(f)$ 与一本原多项式 $f_1(x)$ 的积, 即

$$f(x)=c(f)f_1(x) \tag{1}$$

且这种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) 本原多项式的积为本原多项式.

**证明**

(1) 设 $c(f)=d,f(x)=\sum_{k=0}^{n} a_k x^k$, 于是 $a_k=da'_k$, 因而由引理????知 $d(a'_0,a'_1,\cdots,a'_n)\sim(a_0,a_1,\cdots,a_n)=d$, 从而再由定理????知 $(a'_0,a'_1,\cdots,a'_n)\sim 1$, 故 $f_1(x)=\sum_{k=0}^{n} a'_k x^k$ 为本原多项式且式(1)成立.

若另有 $f(x)=d_1f_2(x),d_1\in R,c(f_2)\sim 1$, 则 $d_1c(f_2)\sim c(d_1f_2(x))\sim c(f)=d$, 故由定理????知 $d_1\sim d$, 再由定理????知 $d_1=du(u\in U)$, 因而 $f(x)=df_1(x)=duf_2(x)$, 从而由命题????得 $f_1(x)=uf_2(x)$, 由定理????知 $f_1(x)\sim f_2(x)$, 亦即 $f(x)$ 的上述分解在相伴意义下唯一.

(2) 设 $f(x)$ 不可约且 $\deg f(x)>0,d=c(f)$. 由结论 (1) 知 $f(x)=df_1(x)$. 由 $\deg f(x)>0$ 知 $\deg f_1(x)>0$, 从而 $f_1(x)\notin U$. 若 $d\notin U$, 则 $f(x)$ 有非平凡的真因子 $d$, 与 $f(x)$ 不可约矛盾. 故必有 $d\in U$, 即 $c(f)=d\sim 1$, 即 $f(x)$ 是本原的.

(3) 设 $f(x)=\sum_{k=0}^{n} a_k x^k,a_n\neq 0;g(x)=\sum_{k=0}^{m} b_k x^k,b_m\neq 0$ 都是本原多项式. 又

$$h(x)=f(x)g(x)=\sum_{k=0}^{m+n} c_k x^k,$$

其中,

$$c_k=\sum_{i+j=k} a_i b_j,\quad k=0,1,\cdots,m+n.$$

假设 $c(h)\notin U$, 则由有限析因条件和定理??知有 $R$ 中素元素 $p|c(h)$, 即有 $p|c_k(k=0,1,\cdots,m+n)$.

由 $c(f)\sim c(g)\sim 1$ 及引理????知 $(p,c(f))\sim(p,c(g))\sim(p,1)\sim 1$. 因此 $p$ 于是由引理????知存在 $r,s$, 使得

$$p|a_i,0\leqslant i\leqslant r-1,\quad p\nmid a_r;\quad p|b_j,0\leqslant i\leqslant s-1,\quad p\nmid b_s,$$

再由

$$c_{r+s}=\sum_{i+j=r+s}a_ib_j=a_rb_s+\sum_{\substack{i<r,\\ i+j=r+s}}a_ib_j+\sum_{\substack{j<s,\\ i+j=r+s}}a_ib_j$$

及 $p\mid c_{r+s}$ 可知

$$p\left|\sum_{\substack{i<r,\\ i+j=r+s}}a_ib_j,\quad p\right|\sum_{\substack{j<s,\\ i+j=r+s}}a_ib_j,\quad p|a_rb_s,$$

这与 $p\nmid a_r,b_s$ 矛盾! 故 $c(h)\sim 1$, 即 $f(x)g(x)$ 是本原多项式.

□

**定理 0.2**

设 $F$ 是唯一析因环 $R$ 的分式域. 于是 $F[x]\supseteq R[x]$. 又设 $S$ 为 $R[x]$ 中本原多项式的集合,$R[x]$ 中相伴关系记为 $\overset{R}{\sim}$,$F[x]$ 中相伴关系记为 $\overset{F}{\sim}$, 则有下列结论:

(1) $\forall f(x)\in F[x],f(x)\neq 0,\exists g(x)\in S$, 使 $f(x)\overset{F}{\sim}g(x)$ 且 $g(x)$ 在 $\overset{R}{\sim}$ 意义下是唯一的;

(2) 设 $f_1(x),f_2(x)\in F[x]$,$g(x),g_1(x),g_2(x)\in S$ 且

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

则有

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

(3) 设 $f(x)\in R[x]$,$\deg f(x)\geqslant 1$, 则 $f(x)$ 在 $R[x]$ 中不可约的充要条件是 $f(x)$ 在 $F[x]$ 中也不可约.

**证明**

(1) 设 $f(x)=\sum_{k=0}^{n}d_kx^k\in F[x]$, 即 $d_k\in F$. 于是由 $F$ 是 $R$ 的分式域知 $d_k=\dfrac{a_k}{b_k}$,$a_k,b_k\in R$,$b_k\neq 0$,$0\leqslant k\leqslant n$. 令 $b=b_0b_1\cdots b_n$, 则有

$$d_kb=a_k\prod_{i\neq k}b_i\in R,\quad 0\leqslant k\leqslant n.$$

再令 $d=(d_0b,d_1b,\cdots,d_nb)\in R\setminus\{0\}$, 则由 $d\mid d_kb$ 知存在 $c_k\in R\setminus\{0\}$, 使 $dc_k=d_kb$. 于是由引理**????**知

$$d\,(c_0,c_1,\cdots,c_n)\overset{R}{\sim}(dc_0,dc_1,\cdots,dc_n)=(d_0b,d_1b,\cdots,d_nb)=d.$$

于是再由定理**????**得

$$(c_0,c_1,\cdots,c_n)\overset{R}{\sim}1.$$

而

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

其中 $\dfrac{d}{b}\in F$,$g(x)=\sum_{k=0}^{n}c_kx^k\in R[x]$,$(c_0,c_1,\cdots,c_n)\overset{R}{\sim}1$, 故 $g(x)\in S$ 且 $g(x)=\dfrac{b}{d}f(x)$. 这样得到 $f(x)\overset{F}{\sim}g(x)$.

现设 $f(x)\overset{F}{\sim}g_1(x)$,$g_1(x)\in S$. 又 $f(x)\overset{F}{\sim}g(x)$, 所以 $g_1(x)\overset{F}{\sim}g(x)$, 即 $\exists u\in F^*$, 使 $g_1(x)=ug(x)$. 又 $u=\dfrac{d'}{d}$,$d',d\in R$, 故有 $dg_1(x)=d'g(x)\in R[x]$. 由定理 0.1(1)知 $d'g(x)$ 是其自身的一个分解, 从而 $g_1(x)\overset{R}{\sim}g(x)$. 唯一性得证.

(2) 由于 $f_1(x)\overset{F}{\sim}g_1(x)$,$f_2(x)\overset{F}{\sim}g_2(x)$, 故由相伴关系对乘法构成同余关系知

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

由定理 0.1(3)知 $g_1(x)g_2(x)\in S$. 再由本定理的结论 (1)知 $g_1(x)g_2(x)\overset{R}{\sim}g(x)$.

(3) **必要性**: 用反证法证明. 假设 $f(x)$ 作为 $F[x]$ 中的多项式是可约的, 由 $F[x]$ 的单位群为 $F^*$, 故有 $f_1(x),f_2(x)\in$

$F[x]$ 且 $\deg f_i(x) \geqslant 1$, 使得 $f(x) = f_1(x)f_2(x)$. 由本定理的结论 (1)知 $\exists g_1(x), g_2(x) \in S$, 使

$$g_i(x) \overset{F}{\sim} f_i(x), \quad i = 1, 2.$$

于是相伴关系对乘法构成同余关系知

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

因为 $f(x)$ 在 $R[x]$ 中不可约, 所以由定理 0.1(2)有 $f(x) \in S$. 又 $f(x) \overset{F}{\sim} f(x)$, 故再由本定理的结论 (2)知 $f(x) \overset{R}{\sim} g_1(x)g_2(x)$. 这与已知的 $f(x)$ 在 $R[x]$ 中不可约矛盾, 故 $f(x)$ 在 $F[x]$ 中也不可约.

**充分性**: 若 $f(x)$ 在 $R[x]$ 中可约, 则存在 $f_1(x), f_2(x) \in R[x] \subseteq F[x]$, 使 $f(x) = f_1(x)f_2(x)$. 从而 $f(x)$ 在 $F[x]$ 中也可约, 矛盾!

□

**定理 0.3**

唯一析因环 $R$ 上的一元多项式环 $R[x]$ 也是唯一析因环.

**证明** 设 $U$ 为 $R^*$ 中可逆元素的集合,$f(x) \in R[x], f(x) \neq 0$. 于是由定理 0.1(1)知 $\exists d \in R, g(x) \in S$, 使得

$$f(x) = dg(x).$$

因 $d \in R$, 则有 $d = p_1p_2\cdots p_t, p_i(1 \leqslant i \leqslant t)$ 为 $R$ 中不可约元素, 在 $R[x]$ 中也不可约. 若 $\deg f(x) = 0$, 则 $\deg g(x) = 0, g(x) \sim 1$, 故 $g(x) \in U$, 即 $f(x)$ 可分解为有限个不可约元素之积. 再设 $\deg g(x) > 0$, 于是 $\deg g(x) = \deg f(x)$. 设 $F$ 为 $R$ 的分式域, 则由定理**????**知 $F[x]$ 是 Euclid 环, 进而也是唯一析因环. 于是 $g(x) \in F[x]$ 可分解为不可约多项式的积

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

根据定理 0.2(1)有 $p_i(x) \in S$(其中 $S$ 为 $R[x]$ 中本原多项式的集合) 且满足 $p_i(x) \overset{F}{\sim} g_i(x)$, 由命题**??**知 $p_i(x)$ 是 $F[x]$ 中不可约多项式. 并且由相伴关系对乘法构成同余关系知

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

由定理 0.1(3)知 $p_1(x)p_2(x)\cdots p_r(x)$ 为本原多项式, 又 $g(x)$ 也是本原多项式, 故由定理 0.2(2)得

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

因此可不妨设 $g(x) = p_1(x)p_2(x)\cdots p_r(x), p_i(x)$ 是 $F[x]$ 中的不可约多项式, 由定理 0.2(3)知 $p_i(x)$ 在 $R[x]$ 中也不可约, 故 $f(x)$ 可分解为 $R[x]$ 中有限个不可约元素之积

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

下面证因式分解的唯一性. 设 $f(x)$ 还有分解式

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

其中,$q_i$ 为 $R$ 中不可约元素,$q_j(x)$ 为 $R[x]$ 中不可约多项式且 $\deg q_j(x) > 0$. 由定理 0.1(2)知 $q_j(x) \in S$, 故由定理 0.1(3)知 $q_1(x)q_2(x)\cdots q_s(x) \in S$. 再由定理 0.1(1)知有

$$p_1p_2\cdots p_t \sim q_1q_2\cdots q_{t'},$$
$$p_1(x)p_2(x)\cdots p_r(x) \overset{R}{\sim} q_1(x)q_2(x)\cdots q_s(x).$$

由 $R$ 为唯一析因环知 $t = t'$ 且 $\exists \pi_1 \in S_t$, 使得 $p_i \sim q_{\pi_1(i)}$. 又由定理 0.2(3)知 $p_i(x), q_j(x)$ 均为 $F[x]$ 中不可约多项式, 而 $F[x]$ 为 Euclid 环, 由定理**??**知 $F[x]$ 也是唯一析因环, 故 $r = s$ 且 $\exists \pi_2 \in S_r$, 使得 $p_i(x) \overset{F}{\sim} q_{\pi_2(i)}(x)$. 又由定理 0.1(2)知 $p_i(x), q_{\pi_2(i)}(x)$ 都是 $R[x]$ 中的本原多项式且 $p_i(x) \overset{F}{\sim} p_i(x)$, 故再由定理 0.2(1)知 $p_i(x) \overset{R}{\sim} q_{\pi_2(i)}(x)$. 因此, 在 $R[x]$ 中因式分解唯一性定理成立, 即 $R[x]$ 也是唯一析因环.

□

**推论 0.1**

唯一析因环 $R$ 上的 $n$ 元多项式环 $R[x_1,x_2,\cdots,x_n]$ 也是唯一析因环.

**证明** 对 $n$ 用数学归纳法, 再根据定理 0.3同理可证.

□

**定理 0.4**

设 $F$ 是唯一析因环 $R$ 的分式域, 又 $f(x)=\sum_{k=0}^{n}a_kx^k\in R[x],a_n\neq 0(n>1)$. 若有 $R$ 中素元素 $p$ 满足

(1) $p\nmid a_n$;

(2) $p|a_k,0\leqslant k\leqslant n-1$;

(3) $p^2\nmid a_0$,

则 $f(x)$ 是 $F[x]$ 中不可约元素.

**证明** 由定理 0.2(3), 只需证明 $f(x)$ 在 $R[x]$ 中不能分解为两个次数大于零的多项式的乘积即可. 若不然, 则有 $f(x)=g(x)h(x)$, 其中

$$g(x)=\sum_{k=0}^{r}b_kx^k,\quad b_k\in R,\ b_r\neq 0,\ r\geqslant 1,$$

$$h(x)=\sum_{k=0}^{s}c_kx^k,\quad c_k\in R,\ c_s\neq 0,\ s\geqslant 1$$

且有

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

从而 $p\mid b_0c_0$. 由素元素定义知 $p\mid b_0$ 或 $p\mid c_0$, 不妨设 $p|c_0,p\nmid b_0$. 又 $p\nmid a_n$, 故 $p\nmid c_s,p\nmid b_r$, 因而存在 $t\in\{1,2,\cdots,s\}$, 使得 $p|c_i(0\leqslant i\leqslant t-1),p\nmid c_t$. 而

$$a_t=\sum_{i+j=t}c_ib_j=\sum_{\substack{i<t,\\ i+j=t}}c_ib_j+c_tb_0.$$

由 $p$ 能整除上式右端第一项, 而 $p\nmid c_tb_0$, 故 $p\nmid a_t$. 这与定理中条件 (2) 矛盾, 故 $f(x)$ 在 $F[x]$ 中不可约.

□

**例题 0.1** 设 $p$ 为素数,$f(x)=x^{p-1}+x^{p-2}+\cdots+1\in\mathbb{Q}[x]$ 是不可约多项式.

**证明** 令 $g(x)=f(x+1)$,

$$g(x)=\frac{(x+1)^p-1}{x}=\sum_{k=1}^{p}\mathrm{C}_p^kx^{k-1}.$$

由 $\mathrm{C}_p^p=1,p|\mathrm{C}_p^k(1\leqslant k\leqslant p-1),p^2\nmid\mathrm{C}_p^1=p$ 知 $g(x)$ 为 $\mathbb{Q}[x]$ 中不可约多项式, 从而 $f(x)$ 为不可约多项式.

□

**例题 0.2** $f(x,y)=x^2y+x^2+y^2+2y+2\in\mathbb{Q}[x,y]$ 是不可约多项式.

**证明** 由定理**??**知 $\mathbb{Q}[x,y]=(\mathbb{Q}[x])[y]$, 而 $x^2y+x^2+y^2+2y+2=y^2+y(x^2+2)+(x^2+2)$. 又 $x^2+2$ 是 $\mathbb{Q}[x]$ 中不可约多项式, 由定理 0.1(3)知 $x^2+2$ 也是 $\mathbb{Q}[x]$ 中的素元素, 故由 Eisenstein 判别法知 $f(x,y)$ 为不可约多项式.

□