0.1 最大公因式与互素多项式

定义 0.1 (最大公因式和互素)

设 $f(x), g(x)$ 是 $\mathbb{F}$ 上的多项式,$d(x)$ 是 $\mathbb{F}$ 上的首 1 多项式, 若 $d(x)$ 满足
(i) $d(x)$ 是 $f(x), g(x)$ 的公因式,
(ii) 对 $f(x), g(x)$ 的任一公因式 $h(x)$, 都有 $h(x) \mid d(x)$,
则称 $d(x)$ 为 $f(x), g(x)$ 的**最大公因式** (或称 $d(x)$ 为 $f(x), g(x)$ 的 g.c.d.), 记为 $d(x) = (f(x), g(x))$. 特别地, 若 $d(x) = 1$, 则称 $f(x), g(x)$ 互素.

命题 0.1

(1) 若 $\mathbb{F}$ 上的多项式 $d_0(x)$(但不一定是首 1 多项式) 也满足
(i) $d_0(x)$ 是 $f(x), g(x)$ 的公因式,
(ii) 对 $f(x), g(x)$ 的任一公因式 $h(x)$, 都有 $h(x) \mid d_0(x)$,
则 $d_0(x) \sim d(x)$, 即 $d_0(x)$ 与 $d(x)$ 相差一个非零常数倍.
(2) 对 $\forall a, b \in \mathbb{F}, (af(x), bg(x)) = (f(x), g(x)) = d(x)$.

证明

(1) 证明是显然的.
(2) 证明是显然的.

□

定义 0.2 (最小公倍式)

设 $f(x), g(x)$ 是 $\mathbb{F}$ 上的多项式,$m(x)$ 是 $\mathbb{F}$ 上的首 1 多项式, 若 $d(x)$ 满足
(i) $m(x)$ 是 $f(x)$ 与 $g(x)$ 的公倍式,
(ii) 对 $f(x)$ 与 $g(x)$ 的任一公倍式 $l(x)$ 均有 $m(x) \mid l(x)$,
则称 $m(x)$ 为 $f(x)$ 与 $g(x)$ 的**最小公倍式** (或称 $m(x)$ 为 $f(x), g(x)$ 的 l.c.m.), 记为 $m(x) = [f(x), g(x)]$.

命题 0.2

(1) 若 $\mathbb{F}$ 上的多项式 $m_0(x)$(但不一定是首 1 多项式) 也满足
(i) $m(x)$ 是 $f(x)$ 与 $g(x)$ 的公倍式,
(ii) 对 $f(x)$ 与 $g(x)$ 的任一公倍式 $l(x)$ 均有 $m(x) \mid l(x)$,
则 $m_0(x) \sim m(x)$, 即 $m_0(x)$ 与 $m(x)$ 相差一个非零常数倍.
(2) 对 $\forall a, b \in \mathbb{F}, [af(x), bg(x)] = [f(x), g(x)] = m(x)$.

证明

(1) 证明是显然的.
(2) 证明是显然的.

□

定理 0.1 (最大公因式的必要条件)

设 $f(x), g(x)$ 是 $\mathbb{F}$ 上的多项式,$d(x)$ 是它们的最大公因式, 则必存在 $\mathbb{F}$ 上的多项式 $u(x), v(x)$, 使得

$$f(x)u(x) + g(x)v(x) = d(x).$$

注 设 $d(x) = f(x)u(x) + g(x)v(x)$, 则 $d(x)$ 不一定是 $f(x)$ 和 $g(x)$ 的最大公因式.

证明 若 $f(x) = 0$, 则显然 $(f(x), g(x)) = g(x)$; 若 $g(x) = 0$, 则 $(f(x), g(x)) = f(x)$. 故不妨设 $f(x) \neq 0, g(x) \neq 0$. 由带余

除法, 我们有下列等式:

$$
\begin{aligned}
f(x) &= g(x)q_1(x) + r_1(x),\\
g(x) &= r_1(x)q_2(x) + r_2(x),\\
r_1(x) &= r_2(x)q_3(x) + r_3(x),\\
&\cdots\cdots\cdots\\
r_{s-2}(x) &= r_{s-1}(x)q_s(x) + r_s(x),\\
&\cdots\cdots\cdots
\end{aligned}
$$

余式的次数是严格递减的, 因此经过有限步后, 必有一个等式其余式为零. 不妨设 $r_{s+1}(x) = 0$, 于是

$$r_{s-1}(x) = r_s(x)q_{s+1}(x). \tag{1}$$

现在要证明 $r_s(x)$ 即为 $f(x)$ 与 $g(x)$ 的最大公因式. 由上式知 $r_s(x) \mid r_{s-1}(x)$, 但

$$r_{s-2}(x) = r_{s-1}(x)q_s(x) + r_s(x), \tag{2}$$

因此 $r_s(x) \mid r_{s-2}(x)$. 这样可一直推下去, 得到 $r_s(x) \mid g(x), r_s(x) \mid f(x)$. 这表明 $r_s(x)$ 是 $f(x)$ 与 $g(x)$ 的公因式. 又设 $h(x)$ 是 $f(x)$ 与 $g(x)$ 的公因式, 则 $h(x) \mid r_1(x)$, 于是 $h(x) \mid r_2(x)$, 不断往下推, 容易看出有 $h(x) \mid r_s(x)$. 因此 $r_s(x)$ 是最大公因式.

再证明(1)式. 从(2)式得

$$r_s(x) = r_{s-2}(x) - r_{s-1}(x)q_s(x), \tag{3}$$

但我们有

$$r_{s-3}(x) = r_{s-2}(x)q_{s-1}(x) + r_{s-1}(x),) \tag{4}$$

从(4)式中解出 $r_{s-1}(x)$ 代入(3)式, 得

$$r_s(x) = r_{s-2}(x)(1 + q_{s-1}(x)q_s(x)) - r_{s-3}(x)q_s(x).$$

用类似的方法逐步将 $r_i(x)$ 用 $r_{i-1}(x), r_{i-2}(x)$ 代入, 最后得到

$$r_s(x) = f(x)u(x) + g(x)v(x).$$

显然 $u(x), v(x) \in \mathbb{K}[x]$. □

定理 0.2 (最大公因式的充分条件)

设 $f(x), g(x), d(x)$ 是 $\mathbb{F}$ 上的多项式. 若 $d(x) \mid f(x), d(x) \mid g(x)$ 并且存在 $\mathbb{F}$ 上的多项式 $u(x), v(X)$, 使得 $d(x) = f(x)u(x) + g(x)v(x)$, 则 $d(x)$ 必是 $f(x)$ 和 $g(x)$ 的最大公因式.

证明 如果同时 $d(x) \mid f(x), d(x) \mid g(x)$, 则 $d(x)$ 是 $f(x)$ 和 $g(x)$ 的公因式. 若 $h(x)$ 也是 $f(x), g(x)$ 的公因式, 则由 $h(x) \mid f(x),h(x) \mid g(x)$ 可推出 $h(x) \mid (f(x)u(x) + g(x)v(x)) = d(x)$, 因此 $d(x)$ 是最大公因式. □

例题 0.1 设 $(f(x), g(x)) = d(x)$, 求证: 对任意的正整数 n,

$$(f(x)^n, f(x)^{n-1}g(x), \cdots, g(x)^n) = d(x)^n.$$

证明 显然 $d(x)^n$ 是 $f(x)^{n-k}g(x)^k (0 \leqslant k \leqslant n)$ 的公因式. 又假设

$$f(x)u(x) + g(x)v(x) = d(x),$$

两边同时 n 次方得到

$$f^n(x)u^n(x) + f^{n-1}(x)g(x)u^{n-1}(x)v(x) + \cdots + g^n(x)v^n(x) = d^n(x).$$

于是由最大公因式的充分条件可知 $d(x)^n$ 是 $f(x)^{n-k}g(x)^k (0 \leqslant k \leqslant n)$ 的最大公因式. □

推论 0.1 (次数不小于 1 的多项式互素的充要条件)

设 $f(x), g(x)$ 是次数不小于 1 的多项式互素的充要条件是必唯一地存在两个多项式 $u(x), v(x)$, 使得

$$f(x)u(x) + g(x)v(x) = 1,$$

且 $\deg u(x) < \deg g(x), \deg v(x) < \deg f(x)$.

证明 充分性由多项式互素的充要条件可直接得到. 下面证明必要性.

先证存在性. 因为 $(f(x), g(x)) = 1$ 且 $\deg f(x), \deg g(x) > 1$, 所以由多项式互素的充要条件可知, 必存在非零多项式 $h(x), k(x)$, 使得

$$f(x)h(x) + g(x)k(x) = 1. \tag{5}$$

由带余除法可知, 存在 $q(x), u(x)$, 使得

$$h(x) = g(x)q(x) + u(x), \quad \deg u(x) < \deg g(x).$$

代入(5)式可得

$$f(x)[g(x)q(x) + u(x)] + g(x)k(x) = 1.$$

即有

$$f(x)u(x) + g(x)[f(x)q(x) + k(x)] = 1. \tag{6}$$

令 $v(x) = f(x)q(x) + k(x)$, 则 $\deg v(x) < \deg f(x)$. 否则, 若 $\deg v(x) \geqslant \deg f(x)$, 则由(6)式可知

$$f(x)u(x) + g(x)v(x) = 1. \tag{7}$$

从而由 $\deg v(x) \geqslant \deg f(x)$ 及 $\deg u(x) < \deg g(x)$ 可得

$$\deg(f(x)u(x)) = \deg f(x) + \deg u(x) < \deg v(x) + \deg g(x) = \deg(g(x)v(x)).$$

而由(7)式可知 $\deg(f(x)u(x)) = \deg(1 - g(x)v(x)) = \deg(g(x)v(x))$ 矛盾!

再证唯一性, 设另有 $u_1(x), v_1(x)$ 适合条件, 即

$$f(x)u_1(x) + g(x)v_1(x) = f(x)u(x) + g(x)v(x) = 1.$$

从而

$$f(x)(u(x) - u_1(x)) = g(x)(v(x) - v_1(x)).$$

上式表明 $g(x) \mid f(x)(u(x) - u_1(x))$, 又由于 $(f(x), g(x)) = 1$, 因此 $g(x) \mid (u(x) - u_1(x))$. 而 $\deg(u(x) - u_1(x)) < \deg g(x)$, 故 $u(x) - u_1(x) = 0$, 即 $u(x) = u_1(x)$. 同理可得 $v(x) = v_1(x)$. □

定理 0.3 (多项式互素的充要条件)

设 $f(x), g(x)$ 是 $\mathbb{F}$ 上的多项式. 则

(1) $(f(x), g(x)) = 1$ 的充要条件是存在 $\mathbb{F}$ 上的多项式 $u(x), v(x)$, 使得 $f(x)u(x) + g(x)v(x) = 1$.

(2) $(f(x), g(x)) = 1$ 的充要条件是对任意给定的正整数 m, n, $(f(x)^m, g(x)^n) = 1$.

证明

1. 必要性: 由最大公因式的必要条件立得.

   充分性: 设 $(f(x), g(x)) = d(x)$, 则由 $f(x)u(x) + g(x)v(x) = 1$ 可知,$d(x) \mid 1$, 因此 $d(x) = 1$.

2. 必要性由命题 0.4即得. 反过来, 若 $d(x) \neq 1$ 是 $f(x)$ 和 $g(x)$ 的公因式, 则它也是 $f(x)^m$ 和 $g(x)^n$ 的公因式, 因此 $f(x)^m$ 和 $g(x)^n$ 不可能互素.

□

命题 0.3 (互素多项式和最大公因式的基本性质)

设 $f(x), g(x), f_1(x), f_2(x) \in \mathbb{K}[x]$, 则

(1) 若 $f_1(x) \mid g(x), f_2(x) \mid g(x)$, 且 $(f_1(x), f_2(x)) = 1$, 则 $f_1(x)f_2(x) \mid g(x)$.

(2) 若 $(f(x), g(x)) = 1$, 且 $f(x) \mid g(x)h(x)$, 则 $f(x) \mid h(x)$.

(3) 若 $(f(x), g(x)) = d(x), f(x) = f_1(x)d(x), g(x) = g_1(x)d(x)$, 则 $(f_1(x), g_1(x)) = 1$.

(4) 若 $(f(x), g(x)) = d(x)$, 则 $(t(x)f(x), t(x)g(x)) = t(x)d(x)$.

(5) 若 $(f_1(x), g(x)) = 1, (f_2(x), g(x)) = 1$, 则 $(f_1(x)f_2(x), g(x)) = 1$.

(6) 若 $(f(x), g(x)) = 1$, 则 $(f(x^m), g(x^m)) = 1$, 其中 m 为任一正整数.

(7) 若 $(f(x), g(x)) = 1$, 则 $(f(x)g(x), f(x) + g(x)) = 1$.

证明

(1) 由多项式互素的充要条件 (1)可知, 存在 $u(x), v(x) \in \mathbb{K}[x]$, 使

$$f_1(x)u(x) + f_2(x)v(x) = 1.$$

设 $g(x) = f_1(x)s(x) = f_2(x)t(x)$, 则

$$\begin{aligned} g(x) &= g(x)(f_1(x)u(x) + f_2(x)v(x)) \\ &= f_2(x)t(x)f_1(x)u(x) + f_1(x)s(x)f_2(x)v(x) \\ &= f_1(x)f_2(x)(t(x)u(x) + s(x)v(x)), \end{aligned}$$

即 $f_1(x)f_2(x) \mid g(x)$.

(2) 由多项式互素的充要条件可知, 存在 $u(x), v(x) \in \mathbb{K}[x]$, 使

$$f(x)u(x) + g(x)v(x) = 1,$$

则

$$f(x)u(x)h(x) + g(x)v(x)h(x) = h(x).$$

因上式左边可被 $f(x)$ 整除, 故 $f(x) \mid h(x)$.

(3) 由多项式互素的充要条件可知, 存在 $u(x), v(x) \in \mathbb{K}[x]$, 使

$$f(x)u(x) + g(x)v(x) = d(x),$$

即

$$f_1(x)d(x)u(x) + g_1(x)d(x)v(x) = d(x),$$

两边消去 $d(x)$ 即得

$$f_1(x)u(x) + g_1(x)v(x) = 1,$$

因此 $f_1(x), g_1(x)$ 互素.

(4) $u(x), v(x) \in \mathbb{K}[x]$, 使

$$f(x)u(x) + g(x)v(x) = d(x),$$

则

$$t(x)f(x)u(x) + t(x)g(x)v(x) = t(x)d(x).$$

因此, 若 $h(x) \mid t(x)f(x), h(x) \mid t(x)g(x)$, 则必有 $h(x) \mid t(x)d(x)$. 又 $t(x)d(x)$ 是 $t(x)f(x), t(x)g(x)$ 的公因式, 因此 $t(x)d(x)$ 是 $t(x)f(x)$ 与 $t(x)g(x)$ 的最大公因式.

(5) 由多项式互素的充要条件可知, 存在 $u_1(x), v_1(x), u_2(x), v_2(x) \in \mathbb{K}[x]$, 使

$$f_1(x)u_1(x) + g(x)v_1(x) = 1,$$

$$f_2(x)u_2(x) + g(x)v_2(x) = 1,$$

将上两式两边分别相乘得

$$(f_1(x)f_2(x))u_1(x)u_2(x)+g(x)(v_1(x)f_2(x)u_2(x)+g(x)v_1(x)v_2(x)+v_2(x)f_1(x)u_1(x))=1.$$

这就是说 $f_1(x)f_2(x)$ 和 $g(x)$ 互素.

(6) 因为 $f(x)$ 和 $g(x)$ 互素, 故存在多项式 $u(x),v(x)$, 使得

$$f(x)u(x)+g(x)v(x)=1,$$

从而有

$$f(x^m)u(x^m)+g(x^m)v(x^m)=1,$$

于是 $f(x^m)$ 和 $g(x^m)$ 互素.

(7) 由互素多项式的充要条件 (1)可知, 存在 $u(x),v(x)$, 使得

$$f(x)u(x)+g(x)v(x)=1.$$

从而

$$f(x)[u(x)-v(x)]+[f(x)+g(x)]v(x)=1.$$

故由互素多项式的充要条件 (1)可知,$(f(x),f(x)+g(x))=1$. 同理可得,$(f(x),f(x)+g(x))=1$. 再由互素多项式和最大公因式的基本性质 (5)即得 $(f(x)g(x),f(x)+g(x))=1$.

□

定理 0.4 (多个多项式的最大公因式的必要条件)

设 $d(x)$ 是 $f_1(x),f_2(x),\cdots,f_m(x)$ 的最大公因式, 求证: 必存在多项式 $g_1(x),g_2(x),\cdots,g_m(x)$, 使得

$$f_1(x)g_1(x)+f_2(x)g_2(x)+\cdots+f_m(x)g_m(x)=d(x).$$

证明 用数学归纳法. 对 $m=2$, 结论已成立. 设结论对 $m-1$ 成立. 设 $h(x)$ 是 $f_1(x),f_2(x),\cdots,f_{m-1}(x)$ 的最大公因式, 则有 $g_1(x),g_2(x),\cdots,g_{m-1}(x)$, 使得

$$f_1(x)g_1(x)+f_2(x)g_2(x)+\cdots+f_{m-1}(x)g_{m-1}(x)=h(x).$$

结合上式由条件可知 $d(x)$ 是 $h(x)$ 和 $f_m(x)$ 的最大公因式, 故存在 $u(x),v(x)$, 使得

$$h(x)u(x)+f_m(x)v(x)=d(x).$$

将 $h(x)$ 代入可得

$$f_1(x)g_1(x)u(x)+f_2(x)g_2(x)u(x)+\cdots+f_{m-1}(x)g_{m-1}(x)u(x)+f_m(x)v(x)=d(x),$$

即知结论成立. □

推论 0.2 (多个多项式互素的充要条件)

数域 $\mathbb{F}$ 上的多项式 $f_1(x),f_2(x),\cdots,f_m(x)$ 互素的充要条件是存在 $\mathbb{F}$ 上的多项式 $g_1(x),g_2(x),\cdots,g_m(x)$, 使得

$$f_1(x)g_1(x)+f_2(x)g_2(x)+\cdots+f_m(x)g_m(x)=1.$$

证明 必要性: 由多个多项式的最大公因式的必要条件立即得到.

充分性: 设存在 $\mathbb{F}$ 上的多项式 $g_1(x),g_2(x),\cdots,g_m(x)$, 使得

$$f_1(x)g_1(x)+f_2(x)g_2(x)+\cdots+f_m(x)g_m(x)=1.$$

设 $d(x)$ 是 $f_1(x),f_2(x),\cdots,f_m(x)$ 的最大公因式, 则由上式可知,$d(x)\mid 1$, 从而 $d(x)=1$. □

命题 0.4 (两两互素的多项式组的乘积也互素)

设 $f_1(x),\cdots,f_m(x),g_1(x),\cdots,g_n(x)$ 为多项式, 且

$$(f_i(x),g_j(x))=1,1\leqslant i\leqslant m;1\leqslant j\leqslant n,$$

求证:

$$(f_1(x)f_2(x)\cdots f_m(x),g_1(x)g_2(x)\cdots g_n(x))=1.$$

证明 利用互素多项式和最大公因式的基本性质 (5)以及数学归纳法即得结论. □

推论 0.3

设 $f(x),g(x)$ 为多项式, 若 $(f(x),g(x))=1$, 则 $(f(x),g^n(x))=1$.

证明 在命题 0.4(上一个命题)中取 $f_1(x)=f(x),f_i(x)=1(i=2,3\cdots,n),g_j(x)=g(x)(j=1,2,\cdots,n)$ 即可得到结论.
□

命题 0.5

设 $f,f_i\in\mathbb{F}[x],i=1,2,\cdots,n$ 满足 $f=f_1f_2\cdots f_n$, 并有 $f_i,i=1,2,\cdots,n$ 两两互素, 则

$$\gcd\left(\frac{f}{f_1},\frac{f}{f_2},\cdots,\frac{f}{f_n}\right)=1.$$

证明 假设

$$\gcd\left(\frac{f}{f_1},\frac{f}{f_2},\cdots,\frac{f}{f_n}\right)=\gcd\left(\prod_{i\neq1}f_i,\prod_{i\neq2}f_i,\cdots,\prod_{i\neq n}f_i\right)=g(x)\neq1,$$

则由因式分解定理知, 存在数域 $\mathbb{F}$ 上的不可约多项式 $p(x)$, 使得 $p(x)|g(x)$. 从而

$$p|\prod_{i\neq1}f_i,\prod_{i\neq2}f_i,\cdots,\prod_{i\neq n}f_i.$$

由推论**??**可知

$$\begin{aligned}
&p|\prod_{i\neq1}f_i\Longrightarrow p\,(x)\text{必可整除}f_2,f_3\cdots,f_n\text{中的某一个}\Longrightarrow\text{存在}k_1\neq1\cap\{1,2,\cdots,n\},\text{使得}p|f_{k_1}, \qquad (8)\\
&p|\prod_{i\neq2}f_i\Longrightarrow p\,(x)\text{必可整除}f_1,f_3\cdots,f_n\text{中的某一个}\Longrightarrow\text{存在}k_2\neq2\cap\{1,2,\cdots,n\},\text{使得}p|f_{k_2},\\
&\qquad\qquad\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&p|\prod_{i\neq n}f_i\Longrightarrow p\,(x)\text{必可整除}f_1,f_2\cdots,f_{n-1}\text{中的某一个}\Longrightarrow\text{存在}k_n\neq n\cap\{1,2,\cdots,n\},\text{使得}p|f_{k_n},
\end{aligned}$$

因此 $p|f_{k_1},f_{k_2},\cdots,f_{k_n}$. 从而存在 $j,l\in\{1,2,\cdots,n\}$, 使得 $k_j\neq k_l$. 否则, 若 $k_1=k_2=\cdots=k_n$, 则 $k_1\neq1,2,\cdots,n$. 这与(8)式矛盾! 于是 $p|f_{k_j},f_{k_l}$, 即 $\gcd(f_{k_j},f_{k_l})=p(x)\neq1$, 这与 f_{k_j},f_{k_l} 互素矛盾! 故 $\gcd\left(\frac{f}{f_1},\frac{f}{f_2},\cdots,\frac{f}{f_n}\right)=1$. □

定理 0.5 (中国剩余定理)

设 $g_1(x),\cdots,g_n(x)$ 是两两互素的多项式,$r_1(x),\cdots,r_n(x)$ 是 n 个多项式, 则存在多项式 $f(x),q_1(x),\cdots,q_n(x)$, 使

$$f(x)=g_i(x)q_i(x)+r_i(x),i=1,\cdots,n.$$

证明 先证明存在多项式 $f_i(x)$, 使对任意的 i, 有

$$f_i(x)=g_i(x)p_i(x)+1,\ g_j(x)\mid f_i(x)(j\neq i).$$

一旦得证, 只需令 $f(x)=r_1(x)f_1(x)+\cdots+r_n(x)f_n(x)$ 即可. 现构造 $f_1(x)$ 如下. 因为 $g_1(x)$ 和 $g_j(x)(j\neq1)$ 互素, 故存在 $u_j(x),v_j(x)$, 使 $g_1(x)u_j(x)+g_j(x)v_j(x)=1$. 令

$$f_1(x)=g_2(x)v_2(x)\cdots g_n(x)v_n(x)=(1-g_1(x)u_2(x))\cdots(1-g_1(x)u_n(x)),$$

显然 $f_1(x)$ 符合要求. 同理可构造 $f_i(x)$. □

命题 0.6 (两个多项式的乘积与其最大公因式和最小公倍式的乘积相伴)

设 $f(x), g(x)$ 是非零多项式, 则

$$f(x)g(x) \sim (f(x), g(x))[f(x), g(x)].$$

证明 证法一: 设 $d(x) = (f(x), g(x))$ 且 $f(x) = f_0(x)d(x), g(x) = g_0(x)d(x)$, 则由互素多项式和最大公因式的基本性质 (3)可知 $f_0(x), g_0(x)$ 互素. 设 $l(x)$ 是 $f(x), g(x)$ 的公倍式且

$$l(x) = f(x)u(x) = g(x)v(x),$$

则 $f_0(x)d(x)u(x) = g_0(x)d(x)v(x)$, 消去 $d(x)$ 得

$$f_0(x)u(x) = g_0(x)v(x).$$

上式表明 $f_0(x) \mid g_0(x)v(x), g_0(x) \mid f_0(x)u(x)$, 又因为 $f_0(x), g_0(x)$ 互素, 所以由互素多项式和最大公因式的基本性质 (2)可知,$f_0(x) \mid v(x), g_0(x) \mid u(x)$. 设 $u(x) = g_0(x)p(x)$, 则

$$l(x) = f_0(x)d(x)g_0(x)p(x),$$

即 $f_0(x)d(x)g_0(x) \mid l(x)$. 显然 $f_0(x)d(x)g_0(x)$ 是 $f(x), g(x)$ 的公倍式, 因此由命题 0.1(1)可知

$$\frac{f(x)g(x)}{d(x)} = f_0(x)d(x)g_0(x) \sim [f(x), g(x)].$$

故由相伴多项式的基本性质可知

$$f(x)g(x) \sim (f(x), g(x))[f(x), g(x)].$$

证法二: 设 $f(x), g(x)$ 的公共标准分解为

$$f(x) = c_1p_1(x)^{e_1}p_2(x)^{e_2}\cdots p_k(x)^{e_k}, \quad g(x) = c_2p_1(x)^{f_1}p_2(x)^{f_2}\cdots p_k(x)^{f_k},$$

其中 $p_i(x)$ 为互不相同的首一不可约多项式,c, d 是非零常数, 则

$$d(x) = p_1(x)^{r_1}p_2(x)^{r_2}\cdots p_k(x)^{r_k}, \quad h(x) = p_1(x)^{s_1}p_2(x)^{s_2}\cdots p_k(x)^{s_k},$$

其中 $r_i = \min\{e_i, f_i\}, s_i = \max\{e_i, f_i\}$. 注意到

$$f(x)g(x) = c_1c_2p_1(x)^{e_1+f_1}p_2(x)^{e_2+f_2}\cdots p_k(x)^{e_k+f_k},$$

并且

$$(f(x), g(x)) = p_1(x)^{r_1}p_2(x)^{r_2}\cdots p_k(x)^{r_k}, \quad [f(x), g(x)] = p_1(x)^{s_1}p_2(x)^{s_2}\cdots p_k(x)^{s_k},$$

其中 $r_i = \min\{e_i, f_i\}, s_i = \max\{e_i, f_i\}$. 令 $c = c_1c_2$, 则有

$$f(x)g(x) = cd(x)h(x).$$

□

命题 0.7 (最大公因式与最小公倍式在开方下不变)

设 $(f(x), g(x)) = d(x), [f(x), g(x)] = h(x)$, 求证:

$$(f(x)^n, g(x)^n) = d(x)^n, \ [f(x)^n, g(x)^n] = h(x)^n.$$

注 不妨设 $f(x), g(x)$ 都是首一多项式的原因: 若 $f(x), g(x)$ 的首项系数分别为 a, b, 则用 $\frac{f(x)}{a}, \frac{g(x)}{b}$ 代替, 再结合命题 0.1(2)和命题 0.2(2)即可得到结论.

证明 证法一: 不妨设 $f(x), g(x)$ 都是首 1 多项式, $f(x) = f_1(x)d(x), g(x) = g_1(x)d(x)$, 则 $f_1(x), g_1(x), d(x)$ 都是首 1 多项式. 由互素多项式和最大公因式的基本性质 (3)可知 $(f_1(x), g_1(x)) = 1$. 由命题 0.6可知 $h(x) \sim f_1(x)g_1(x)d(x)$, 又因为 $h(x), f_1(x), g_1(x), d(x)$ 均为首 1 多项式, 所以 $h(x) = f_1(x)g_1(x)d(x)$. 由命题 0.4可知,$(f_1(x)^n, g_1(x)^n) = 1$, 从而由互

素多项式和最大公因式的基本性质 (4)可知

$$(f(x)^n, g(x)^n) = (f_1(x)^n d(x)^n, g_1(x)^n d(x)^n) = d(x)^n.$$

由命题 0.6可知 $f(x)^n g(x)^n \sim (f(x)^n, g(x)^n)[f(x)^n, g(x)^n]$, 又因为 $f(x), g(x)$ 都是首 1 多项式, 所以 $f(x)^n g(x)^n = (f(x)^n, g(x)^n)[f(x)^n, g(x)^n] = d(x)^n[f(x)^n, g(x)^n]$. 于是可得

$$[f(x)^n, g(x)^n] = f_1(x)^n g_1(x)^n d(x)^n = h(x)^n.$$

证法二:设 $f(x), g(x)$ 的公共标准分解为

$$f(x) = cp_1(x)^{e_1} p_2(x)^{e_2} \cdots p_k(x)^{e_k}, \quad g(x) = dp_1(x)^{f_1} p_2(x)^{f_2} \cdots p_k(x)^{f_k},$$

其中 $p_i(x)$ 为互不相同的首一不可约多项式,c, d 是非零常数, 则

$$d(x) = p_1(x)^{r_1} p_2(x)^{r_2} \cdots p_k(x)^{r_k}, \quad h(x) = p_1(x)^{s_1} p_2(x)^{s_2} \cdots p_k(x)^{s_k},$$

其中 $r_i = \min\{e_i, f_i\}, s_i = \max\{e_i, f_i\}$. 注意到

$$f(x)^n = c^n p_1(x)^{ne_1} p_2(x)^{ne_2} \cdots p_k(x)^{ne_k}, \quad g(x)^n = d^n p_1(x)^{nf_1} p_2(x)^{nf_2} \cdots p_k(x)^{nf_k},$$

并且 $\min\{ne_i, nf_i\} = nr_i, \max\{ne_i, nf_i\} = ns_i$, 因此

$$(f(x)^n, g(x)^n) = p_1(x)^{nr_1} p_2(x)^{nr_2} \cdots p_k(x)^{nr_k} = d(x)^n,$$
$$[f(x)^n, g(x)^n] = p_1(x)^{ns_1} p_2(x)^{ns_2} \cdots p_k(x)^{ns_k} = h(x)^n.$$

□

命题 0.8

设 $f(x) = x^m - 1, g(x) = x^n - 1$, 求证: $(f(x), g(x)) = x^d - 1$, 其中 d 是 m, n 的最大公因子.

证明 证法一: 不妨设 $m \geqslant n, m = nq + r$, 先证明 $(x^m - 1, x^n - 1) = (x^r - 1, x^n - 1)$. 假设 $d_1(x) = (x^m - 1, x^n - 1), d_2(x) = (x^r - 1, x^n - 1)$. 注意到

$$x^m - 1 = x^{nq+r} - 1 = x^r(x^{nq} - 1) + (x^r - 1),$$

$(x^n - 1) \mid (x^{nq} - 1)$, 故 $d_1(x) \mid (x^r - 1)$, 从而 $d_1(x) \mid d_2(x)$. 从上式也可以看出 $d_2(x) \mid (x^m - 1)$, 从而 $d_2(x) \mid d_1(x)$, 因此 $d_1(x) = d_2(x)$. 又设 $n = q_1 r + r_1$, 则 $(x^m - 1, x^n - 1) = (x^n - 1, x^r - 1) = (x^r - 1, x^{r_1} - 1)$. 再由辗转相除, 有某个 $r_{s-1} = q_{s+1} r_s$, 其中 $r_s = d$ 是 m, n 的最大公因子, 于是 $(x^m - 1, x^n - 1) = (x^{r_{s-1}} - 1, x^{r_s} - 1) = x^d - 1$.

证法二:只需求出 $f(x), g(x)$ 的公根. $f(x)$ 的根为

$$\cos \frac{2k\pi}{m} + \mathrm{i} \sin \frac{2k\pi}{m}, 1 \leqslant k \leqslant m,$$

$g(x)$ 的根为

$$\cos \frac{2k\pi}{n} + \mathrm{i} \sin \frac{2k\pi}{n}, 1 \leqslant k \leqslant n,$$

则公根为

$$\cos \frac{2k\pi}{d} + \mathrm{i} \sin \frac{2k\pi}{d}, 1 \leqslant k \leqslant d.$$

这就是 $x^d - 1$ 的全部根, 于是结论成立. □