§5.3 最大公因式

教学目的和要求 熟练掌握最大公因式的概念，性质与结论；熟练掌握互素的概念和充要条件；了解中国剩余定理的内容和思想方法.

一. 最大公因式

定义 设 $f(x), g(x), d(x) \in K[x]$, 称 $d(x)$ 是 $f(x), g(x)$ 的最大公因式，如果

(1) $d(x)|f(x), d(x)|g(x)$;

(2) 若 $h(x)|f(x), h(x)|g(x)$, 则 $h(x)|d(x)$.

注 设 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的最大公因式，$0 \neq c \in K$, 则 $cd(x)$ 也是 $f(x)$ 和 $g(x)$ 的最大公因式. 设 $d(x), d_1(x)$ 是 $f(x)$ 与 $g(x)$ 的最大公因式，则存在 $c \in K$, 使得 $d(x) = cd_1(x)$. 首项系数为 1 的最大公因式唯一，记为 $(f(x), g(x))$.

注 $f(x)$ 是 $f(x)$ 与 0 的最大公因式；8 是 6 和 7 的最大公因式. $(0, 2x^2) = x^2$; $(0, 0) = 0$.

引理 设 $f(x), g(x) \in K[x]$, 则 $(f(x), g(x)) = (f(x) - l(x)g(x), g(x))$.

证法 1 设 $(f(x), g(x)) = d(x)$, 要证 $(f(x) - l(x)g(x), g(x)) = d(x)$.

(1) 如果 $d(x)|f(x)$ 且 $d(x)|g(x)$, 则 $d(x)|g(x)$ 且 $d(x)|(f(x) - l(x)g(x))$;

(2) 若 $h(x)|g(x)$ 且 $h(x)|(f(x) - l(x)g(x))$, 则 $h(x)|f(x)$ 且 $h(x)|g(x)$,

所以 $h(x)|d(x)$.

证法 2 设 $d(x) = (f(x), g(x)), d_1(x) = (f(x) - l(x)g(x), g(x))$. 则 $d(x)|f(x)$ 且 $d(x)|g(x)$, 故 $d(x)|(f(x) - l(x)g(x))$ 且 $d(x)|g(x)$, 所以 $d(x)|d_1(x)$. 另一方面，若 $d_1(x)|(f(x) - l(x)g(x))$ 且 $d_1(x)|g(x)$, 则 $d_1(x)|f(x)$ 且 $d_1(x)|g(x)$, 故 $d_1(x)|d(x)$. 又因为 $d(x), d_1(x)$ 首项系数为 1, 所以 $d(x) = d_1(x)$. □

定理 设 $f(x), g(x) \in K[x]$, 则存在 $f(x)$ 与 $g(x)$ 的最大公因式 $d(x)$, 且存在 $u(x), v(x) \in K[x]$, 使得 $d(x) = u(x)f(x) + v(x)g(x)$.

证明 若 $f(x) = g(x) = 0$, 取 $d(x) = u(x) = v(x) = 0$ 即可. 若 $f(x) = 0$, $g(x) \neq 0$, 则 $(f(x), g(x)) = cg(x)$, 其中 c 是 $g(x)$ 的首项系数的倒数；同理，若 $g(x) = 0$,$f(x) \neq 0$ 时，结论成立.

设 $f(x)\neq 0\neq g(x)$, 由带余除法有

$$f(x)=g(x)q_1(x)+r_1(x),\quad \text{其中}\deg r_1(x)<\deg g(x);$$

$$g(x)=r_1(x)q_2(x)+r_2(x),\quad \text{其中}\deg r_2(x)<\deg r_1(x);$$

$$r_1(x)=r_2(x)q_3(x)+r_3(x),\quad \text{其中}\deg r_3(x)<\deg r_2(x);$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$r_{s-2}=r_{s-1}q_s(x)+r_s(x),\quad \text{其中}\deg r_s(x)<\deg r_{s-1}(x);$$

$$r_{s-1}(x)=r_s(x)q_{s+1}(x)+0.$$

由引理知 $(f(x),g(x))=(f(x)-g(x)q_1(x),g(x))=(r_1(x),g(x))=(r_1(x),r_2(x))$ $=\cdots=(r_{s-1}(x),r_s(x)=cr_s(x))$, 其中 c 为 $r_s(x)$ 的首项系数的倒数. 另一方面,

$$r_s(x)=r_{s-2}(x)-r_{s-1}(x)q_s(x);$$

$$r_{s-1}(x)=r_{s-3}(x)-r_{s-2}(x)q_{s-1}(x),$$

所以 $r_s(x)=(1-q_{s-1}(x))r_{s-2}(x)-q_s(x)r_{s-3}(x)$, 逐步代入，得

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

下面介绍计算最大公因式的辗转相除法.

例 1 $f(x)=x^4-x^3-x^2+2x-1, g(x)=x^3-2x+1$ 求 $(f(x),g(x))$ 和 $u(x),v(x)$, 使 $u(x)f(x)+v(x)g(x)=(f(x),g(x))$.

	x^4	$-x^3$	$-x^2$	$+2x$	-1	x^3		$-2x$	$+1$	
$q_1(x)=x-1$	x^4		$-2x^2$	$+x$		x^3	$-x^2$			$q(x)=x+1$
		$-x^3$	$+x^2$	$+x$	-1		x^2	$-2x$	$+1$	
		$-x^3$		$+2x$	-1		x^2	$-x$		
$q_3(x)=-x$	$r_1(x)$	$=$	x^2	$-x$		r_2	$=$	$-x$	$+1$	
			x^2	$-x$						
					0					

因为 $(f(x),g(x))=x-1=-r_2(x)$, 所以 $r_2(x)=g(x)-r_1(x)q_2(x)$= $g(x)-(f(x)-g(x)q_1(x))q_2(x)=f(x)(-q_2(x))+g(x)[1+q_1(x)q_2(x)]$, 故 $u(x)=q_2(x)=x+1$, $v(x)=-1-q_1(x)q_2(x)=-x^2$. □

下面介绍多个多项式的最大公因式.

定义 设 $f_i(x)\in K[x],1\le i\le m$, $d(x)$ 称为 $f_i(x),1\le i\le m$ 的最大公因式, 如果

(1) $d(x)|f_i(x),1\le i\le m$;

(2) 设 $h(x)|f_i(x),1\le i\le m$, 则 $h(x)|d(x)$.

记 $f_i(x),1\le i\le m$ 的首项系数为 1 的最大公因式为 $(f_1(x),f_2(x),\cdots,f_m(x))$.

引理 $((f(x),g(x)),h(x))=(f(x),g(x),h(x))=(f(x),(g(x),h(x))$.

证明 设 $d_1(x)=(f(x),g(x)),d(x)=(f(x),g(x),h(x))$, 要证 $(d_1(x),h(x))=d(x)$.

(1) 若 $d(x)|h(x),d(x)|g(x),d(x)|f(x)$, 所以 $d(x)|h(x),d(x)|d_1(x)$;

(2) 若 $l(x)|d_1(x),l(x)|h(x)$, 则 $l(x)|f(x),l(x)|g(x),l(x)|h(x)$, 所以 $l(x)|d(x)$.

同理可得另一等式. □

注 设 $f_i(x)\in K[x],1\le i\le m$, $c(x)$ 称为 $f_i(x),1\le i\le m$ 的最小公倍式, 如果

(1) $f_i(x)|c(x),1\le i\le m$;

(2) 设 $f_i(x)|h(x),1\le i\le m$, 则 $c(x)|h(x)$.

记 $f_i(x),1\le i\le m$ 的首项系数为 1 的最小公倍式为 $[f_1(x),f_2(x),\cdots,f_m(x)]$.

二. 互素

定义 设 $f(x),g(x)\in K[x]$, 若 $(f(x),g(x))=1$, 则称 $f(x)$ 与 $g(x)$ 互素, 或称互质.

定理 设 $f(x),g(x)\in K[x]$, 则 $f(x)$ 与 $g(x)$ 互素的充分必要条件是存在 $u(x),v(x)\in K[x]$, 使得 $f(x)u(x)+g(x)v(x)=1$.

证明 必要性已证. 现证充分性. 设 $d(x)=(f(x),g(x))$, 则 $d(x)|f(x),d(x)|g(x)$, 所以 $d(x)|f(x)u(x)+g(x)v(x)$, 即 $d(x)|1$. 又 $d(x)$ 首项系数为 1, 所以 $d(x)=1$. □

推论 1 设 $f_1(x)|g(x), f_2(x)|g(x)$, 且 $(f_1(x), f_2(x)) = 1$, 则 $f_1(x)f_2(x)|g(x)$.

证明 因为 $(f_1(x), f_2(x)) = 1$, 所以存在 $u(x), v(x) \in K[x]$, 使得 $f_1(x)u(x) + f_2(x)v(x) = 1$. 由 $f_1(x)|g(x), f_2(x)|g(x)$, 知道存在 $s(x), t(x) \in K[x]$, 使得 $g(x) = f_1(x)s(x) = f_2(x)t(x)$. 所以 $g(x) = g(x)(f_1(x)u(x)+f_2(x)v(x)) = (f_2(x)t(x))f_1(x)u_x + f_1(x)s(x)f_2(x)v(x) = f_1(x)f_2(x)(t(x)u(x) + s(x)v(x))$. 因此 $f_1(x)f_2(x)|g(x)$. □

推论 2 设 $f(x)|g(x)h(x), (f(x), g(x)) = 1$, 则 $f(x)|h(x)$.

证明 因为 $(f(x), g(x)) = 1$, 所以存在 $u(x), v(x) \in K[x]$, 使得 $f(x)u(x) + g(x)v(x) = 1$. 因而 $f(x)u(x)h(x) + g(x)v(x)h(x) = h(x)$. 又因为 $f(x)|g(x)h(x)$, 故 $f(x)|h(x)$. □

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

证明 因为 $(f(x), g(x)) = d(x)$, 所以存在 $u(x), v(x) \in K[x]$, 使得 $f(x)u(x) + g(x)v(x) = d(x)$. 进一步有 $f_1(x)u(x) + g_1(x)v(x) = 1$. 因而 $(f_1(x), g_1(x)) = 1$. □

推论 4 设 $(f(x), g(x)) = d(x)$, $t(x)$ 为首项系数为 1 的多项式, 则 $(f(x)t(x), g(x)t(x)) = d(x)t(x)$.

证明 因为 $(f(x), g(x)) = d(x)$, 显然有 $d(x)t(x)|f(x)t(x), d(x)t(x)|g(x)t(x)$. 同时存在 $u(x), v(x) \in K[x]$, 使得 $f(x)u(x) + g(x)v(x) = d(x)$. 所以 $f(x)t(x)u(x) + g(x)t(x)v(x) = d(x)t(x)$. 若 $h(x)|f(x)t(x)$, $h(x)|g(x)t(x)$, 则 $h(x)|d(x)t(x)$. 这样 $(f(x)t(x), g(x)t(x))= d(x)t(x)$. □

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

证明 存在 $u(x), v(x), u_1(x), v_1(x)$, 使得 $f_1(x)u(x)+g(x)v(x) = 1$, $f_2(x)u_1(x)+g(x)v_1(x) = 1$. 所以 $f_1(x)f_2(x)(u(x)u_1(x)+g(x)(f_1(x)u(x)v_1(x)+f_2(x)u_1(x)v(x)+g(x)v(x)v_1(x)) = 1$. 故有 $(f_1(x)f_2(x), g(x)) = 1$. □

推论 6 设 $f(x)g(x) \neq 0$, 则 $f(x)g(x) \sim (f(x), g(x))[f(x), g(x)]$.

证明 设 $(f(x), g(x)) = d(x)$, 则 $f(x) = d(x)f_1(x), g(x) = d(x)g_1(x), f(x)g(x) = d(x)(d(x)f_1(x)g_1(x))$. 记 $m(x) = d(x)f_1(x)g_1(x)$, 可证 $m(x)$ 是 $f(x), g(x)$ 的最小公倍式, 即与 $[f(x), g(x)]$ 相伴. 一方面由定义, 显然 $m(x)$ 是 $f(x), g(x)$ 的公倍

式；另一方面若 $h(x)$ 是 $f(x), g(x)$ 的公倍式， $h(x) = f(x)f_2(x) = g(x)g_2(x)$, 即 $h(x) = d(x)f_1(x)f_2(x) = d(x)g_1(x)g_2(x)$. 因 $f(x)g(x) \neq 0$, 因此 $d(x) \neq 0$, 故 $f_1(x)f_2(x) = g_1(x)g_2(x)$, 进而 $f_1(x)|g_1(x)g_2(x)$. 注意到 $(f_1(x), g_1(x)) = 1$, 所以 $f_1(x)|g_2(x)$, $g_2(x) = f_1(x)t(x)$, 从而 $h(x) = d(x)g_1(x)f_1(x)t(x) = m(x)t(x)$, 即 $m(x)|h(x)$. 命题得证. □

例 2 $(f(x), g(x)) = 1$, 则 $(f(x^m), g(x^m)) = 1$.

证明 因为 $(f(x), g(x)) = 1$, 所以存在 $u(x), v(x) \in K[x]$, 使得 $f(x)u(x) + g(x)v(x) = 1$. 所以 $f(x^m)u(x^m) + g(x^m)v(x^m) = 1$. 故 $(f(x^m), g(x^m)) = 1$.

三. 中国剩余定理

引理 设 $p_1(x), p_2(x), ...p_m(x) \in K[X]$ 两两互素, 则存在 $f_i(x) \in K[X], 1 \leq i \leq m$, 使得 $f_i(x) = l_i(x)p_i(x) + 1$, $f_i(x) = h_{ij}(x)p_j(x), 1 \leq i \neq j \leq m$.

证明：当 $i \neq j$ 时， $(p_i(x), p_j(x)) = 1$. 所以 $(p_i(x), \prod_{j\neq i, j=1}^{m} p_j(x)) = 1$. 因此存在 $u_i(x), v_i(x) \in K[x]$, 使得

$$p_i(x)v_i(x) + (\prod_{j\neq i} p_j(x))u_i(x) = 1$$

令 $f_i(x) = u_i(x)(\prod_{j\neq i} p_j(x))$, $l(x) = -v(x)$, $h_{ij}(x) = (\prod_{r\neq i,j} p_r(x))u_i(x)$ 即得证. □

注 引理中 f_i 等同于满足如下条件： f_i 被 $p_i(x)$ 除后余 1, 同时可被所有 $p_j(x)$, $j \neq i$, $1 \leq j \leq m$ 整除.

中国剩余定理 设 $p_1(x), p_2(x), ..., p_m(x) \in K[x]$ 是两两互素的多项式， a_1, a_2, $\cdots$, $a_m \in K$, 则存在唯一 $g(x), q_i(x) \in K[x], 1 \leq i \leq m$, 使得

$$\deg g(x) < \sum_{i=1}^{m} \deg p_i(x),$$

且

$$g(x) = p_i(x)q_i(x) + a_i, 1 \leq i \leq m.$$

注 定理意义在于存在 $g(x)$, 它被 $p_i(x)$ 除后余 $a_i, 1 \leq i \leq m$.

证明 由引理，存在 $f_i(x), 1 \leq i \leq m$, 使 $f_i(x) = l_i(x)p_i(x) + 1$, $f_i(x) = h_{ij}(x)p_j(x), i \neq j$. 令 $f(x) = \sum_{i=1}^{m} f_i(x)a_i$. 根据带余除法,有 $f(x) = t(x)\prod_{i=1}^{m} p_i(x) + g(x)$, 这里 $\deg g(x) < \deg \prod_{i=1}^{m} p_i(x) = \sum_{i=1}^{m} \deg p_i(x)$. 我们指出这里 $g(x) \neq 0$. 否则，对于固定的 j, 因为 $p_j(x) | \sum_{i=1}^{m} f_i(x)a_i$ 和 $p_j | f_r(x)$, $r \neq j$, 所以 $p_j | f_j(x)a_j$, 与 $f_i(x) = l_i(x)p_i(x) + 1$ 矛盾.

$$\begin{aligned} g(x) &= f(x) - t(x)\prod_{i=1}^{m} p_i(x) \\ &= (\sum_{j\neq i, j=1}^{m} f_j(x)a_j(x) + f_i(x)a_i) - t(x)\prod_{i=1}^{m} p_i(x) \\ &= \sum_{j\neq i} h_j(x)p_i(x)a_j + (l_i(x)p_i(x) + 1)a_i - t(x)\prod_{i=1}^{m} p_i(x) \\ &= p_i(x)(\sum_{j\neq i} h_j(x)a_j + l_i(x) - t(x)\prod_{j\neq i} p_j(x)) + a_i. \end{aligned}$$

再证明唯一性：若 $g(x) \neq g_1(x)$, $g(x) = p_i(x)q_i(x) + a_i, 1 \leq i \leq m$, $g_1(x) = p_i(x)t_i(x) + a_i$, $1 \leq i \leq m$, $q_i(x) \neq t_i(x)$, $1 \leq i \leq m$. 则 $0 \neq g(x) - g_1(x) = p_i(x)(q_i(x) - t_i(x))$. 故 $p_i(x) | g(x) - g_1(x), 1 \leq i \leq m$, 而 $p_i(x), i \neq j$ 两两互素，所以 $p_1(x)p_2(x)...p_m(x) | g(x) - g_1(x)$, $\sum_{i=1}^{m} \deg p_i(x) \leq \max\{\deg g(x), \deg g_1(x)\} < \sum_{i=1}^{m} \deg p_i(x)$, 此为矛盾. 所以 $g(x) = g_1(x)$, 即 $g(x)$ 是唯一的. 进一步，根据带余除法的商的唯一性，知 $q_i(x)$ 是唯一的. □

例 3 (Lagrange **插值公式**) 设 $a_1, a_2, ..., a_m \in K$ 为 m 个不同数，则对任意 $b_1, b_2, ..., b_m \in K$, 存在唯一次数小于 m 的多项式

$$L(x) = \sum_{i=1}^{m} b_i (\prod_{j\neq i} \frac{(x - a_j)}{(a_i - a_j)})$$

满足 $L(a_i) = b_i, 1 \leq i \leq m$.

证明 设 $p_i(x) = x - a_i$, $1 \leq i \leq m$, 则 $p_i(x)$ 两两互素， $\deg p_i(x) = 1$, 显然 $L(a_i) = b_i$, $\deg L(x) = m - 1 < \sum_{i=1}^{m} \deg f_i(x)$, $L(x) = (x - a_i)q_i(x) + b_i$. 根据中国剩余定理，满足条件的 $L(x)$ 唯一确定的. □

作业： P_{194} 2(1), 3, 4; P_{227} 1, 2.

补充作业 1: 设 $p_1(x), p_2(x), ...p_m(x) \in K[x]$ 是两两互素的多项式, $s_1(x), s_2(x), \cdots, s_m(x) \in K[x]$ 则存在唯一 $g(x), q_i(x), 1 \leq i \leq m$, 使得 $\deg g(x) < \sum \deg p_i(x)$ 且 $g(x) = q_i(x)p_i(x) + s_i(x)$, $1 \leq i \leq m$.

补充作业 2: 设 $f(x), g(x) \in K[x]$, 令

$$\Omega = \{u(x)f(x) + v(x)g(x) | u(x), v(x) \in K[x]\}.$$

求证: (1) 若 $a(x), b(x) \in \Omega$, 则 $a(x) \pm b(x) \in \Omega$;

(2) 若 $a(x) \in \Omega$, 则对任意 $h(x) \in K[X]$, 有 $a(x)h(x) \in \Omega$;

(3) 存在首项系数为 1 的 $d(x) \in \Omega$, 使得对 $\forall a(x) \in \Omega$, 有 $d(x)|a(x)$;

(4) $d(x) = (f(x), g(x))$.

思考题: P_{194} 5, 6, 7.

选做: 设 a, b, c 两两互异, 用 $x-a$, $x-b$, $x-c$ 除 $f(x)$ 的余式分别为 r, s, t. 试求用 $(x-a)(x-b)(x-c)$ 除 $f(x)$ 的余式.