

0.1 整除与带余除法

定义 0.1 (整除的定义)

设 $f(x), g(x)$ 是 \mathbb{F} 上的多项式, 若存在 \mathbb{F} 上的多项式 $h(x)$, 使得

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

则称 $g(x)$ 是 $f(x)$ 的因式, 或称 $g(x)$ 可整除 $f(x)$ (也称 $f(x)$ 可被 $g(x)$ 整除), 记为 $g(x) \mid f(x)$.

命题 0.1 (整除的基本性质)

设 $f(x), g(x), h(x) \in \mathbb{K}[x], 0 \neq c \in \mathbb{K}$, 则

- (1) 若 $f(x) \mid g(x)$, 则 $cf(x) \mid g(x)$, 因此非零常数多项式 c 是任一非零多项式的因式;
- (2) $f(x) \mid f(x)$;
- (3) 若 $f(x) \mid g(x), g(x) \mid h(x)$, 则 $f(x) \mid h(x)$;
- (4) 若 $f(x) \mid g(x), f(x) \mid h(x)$, 则对任意的多项式 $u(x), v(x)$, 有

$$f(x) \mid g(x)u(x) + h(x)v(x);$$

- (5) 设 $f(x) \mid g(x), g(x) \mid f(x)$ 且 $f(x), g(x)$ 都是非零多项式, 则存在 \mathbb{K} 中非零元 c , 使

$$f(x) = cg(x).$$

- (6) 若 $g_1(x) \mid f(x), g_2(x) \mid f(x)$, 则 $g_1(x)g_2(x) \mid f^2(x)$.

证明

- (1) 若 $g(x) = f(x)p(x)$, 则

$$g(x) = (cf(x))(c^{-1}p(x)).$$

此即 $cf(x) \mid g(x)$.

特别地, 任取 $a \in \mathbb{K}$, 令 $g(x) = a$, 则 $a \mid a$, 从而 $ca \mid a$, 故 c 是 a 的因式.

- (2) 显然.

- (3) 若 $g(x) = f(x)p(x), h(x) = g(x)q(x)$, 则

$$h(x) = (f(x)p(x))q(x) = f(x)(p(x)q(x)).$$

- (4) 若 $g(x) = f(x)p(x), h(x) = f(x)q(x)$, 则

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

- (5) 设 $g(x) = f(x)p(x), f(x) = g(x)q(x)$, 则

$$f(x) = f(x)(p(x)q(x)).$$

由此即得

$$\deg f(x) = \deg f(x) + \deg(p(x)q(x)),$$

从而

$$\deg(p(x)q(x)) = 0,$$

于是

$$\deg p(x) = \deg q(x) = 0.$$

因此 $p(x)$ 及 $q(x)$ 均为非零常数多项式, 即 $f(x)$ 和 $g(x)$ 相差一个非零常数倍.

- (6) 由 $g_1(x), g_2(x) \mid f(x)$ 可知, 存在多项式 $h_1(x), h_2(x)$, 使得

$$f(x) = g_1(x)h_1(x) = g_2(x)h_2(x).$$


从而 $f^2(x) = g_1(x)g_2(x)h_1(x)h_2(x)$, 故 $g_1(x)g_2(x) \mid f^2(x)$.

□

定义 0.2 (相伴多项式)

若 $f(x) \mid g(x)$, $g(x) \mid f(x)$ 且 $f(x), g(x)$ 都是非零多项式, 则 $f(x), g(x)$ (即可以互相整除的两个多项式) 称为**相伴多项式**, 记为 $f(x) \sim g(x)$.

♣

 **笔记** 由整除的基本性质 (5) 可知, 相伴的多项式只相差一个非零常数倍.

命题 0.2 (相伴多项式的基本性质)

若 $f(x) \sim g(x)$, 则任意的多项式 $u(x)$ 都有 $f(x)u(x) \sim g(x)u(x)$.

♣

证明 由 $f(x) \sim g(x)$ 及整除的基本性质 (4) 可知, 任意的多项式 $u(x)$ 都有 $f(x)u(x) \mid g(x)u(x)$, $g(x)u(x) \mid f(x)u(x)$. 故 $f(x)u(x) \sim g(x)u(x)$. □

定理 0.1 (多项式的带余除法)

设 $f(x), g(x) \in \mathbb{F}[x]$, $g(x) \neq 0$, 则必存在唯一的 $q(x), r(x) \in \mathbb{F}[x]$, 使得

$$f(x) = g(x)q(x) + r(x),$$

且 $\deg r(x) < \deg g(x)$.

♥

证明 若 $\deg f(x) < \deg g(x)$, 只需令 $q(x) = 0, r(x) = f(x)$ 即可. 现设 $\deg f(x) \geq \deg g(x)$, 对 $f(x)$ 的次数用数学归纳法. 若 $\deg f(x) = 0$, 则 $\deg g(x) = 0$. 因此可设 $f(x) = a, g(x) = b (a \neq 0, b \neq 0)$. 这时令 $q(x) = ab^{-1}, r(x) = 0$ 即可. 作为归纳假设, 我们设结论对小于 n 次的多项式均成立. 设

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, a_n \neq 0, \\ g(x) &= b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0, b_m \neq 0, \end{aligned}$$

由于 $n \geq m$, 可令

$$f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x),$$

则 $\deg f_1(x) < n$. 由归纳假设, 有

$$f_1(x) = g(x)q_1(x) + r(x),$$

且 $\deg r(x) < \deg g(x)$, 于是

$$f(x) - a_n b_m^{-1} x^{n-m} g(x) = g(x)q_1(x) + r(x).$$

因此

$$f(x) = g(x)(a_n b_m^{-1} x^{n-m} + q_1(x)) + r(x).$$

令

$$q(x) = a_n b_m^{-1} x^{n-m} + q_1(x),$$

即得 $f(x) = g(x)q(x) + r(x)$.

再证明唯一性. 设另有 $p(x), t(x)$, 使

$$f(x) = g(x)p(x) + t(x),$$

且 $\deg t(x) < \deg g(x)$, 则

$$g(x)(q(x) - p(x)) = t(x) - r(x).$$

注意上式左边若 $q(x) - p(x) \neq 0$, 便有

$$\deg g(x)(q(x) - p(x)) \geq \deg g(x) > \deg (t(x) - r(x)),$$

引出矛盾. 因此只可能 $p(x) = q(x), t(x) = r(x)$. □

推论 0.1

设 $f(x), g(x) \in \mathbb{F}[x], g(x) \neq 0$, 必存在唯一的 $q(x), r(x) \in \mathbb{F}[x]$, 使得 $f(x) = g(x)q(x) + r(x)$. 则 $g(x) \mid f(x)$ 的充要条件是 $r(x) = 0$. ♥

例题 0.1 设 $g(x) = ax + b \in \mathbb{F}[x]$ 且 $a \neq 0$, 又 $f(x) \in \mathbb{F}[x]$, 求证: $g(x) \mid f(x)^2$ 的充要条件是 $g(x) \mid f(x)$.

证明 充分性显然, 只需证明必要性.

证法一: 设 $f(x) = g(x)q(x) + r$, 则

$$f(x)^2 = g(x)^2 q(x)^2 + 2rg(x)q(x) + r^2.$$

由 $g(x) \mid f(x)^2$ 及 **推论 0.1** 可得 $r^2 = 0$, 即 $r = 0$, 从而 $g(x) \mid f(x)$.

证法二: 由余数定理, $f\left(-\frac{b}{a}\right)^2 = 0$, 故 $f\left(-\frac{b}{a}\right) = 0$, 从而 $g(x) \mid f(x)$. □

例题 0.2 设 $g(x) = ax^2 + bx + c (abc \neq 0)$, $f(x) = x^3 + px^2 + qx + r$, 满足 $g(x) \mid f(x)$, 求证:

$$\frac{ap - b}{a} = \frac{aq - c}{b} = \frac{ar}{c}.$$

证明 用待定系数法, 设

$$x^3 + px^2 + qx + r = (ax^2 + bx + c)(mx + n) = amx^3 + (an + bm)x^2 + (bn + cm)x + cn.$$

比较系数得

$$am = 1, an + bm = p, bn + cm = q, cn = r.$$

由此即可得到所需等式. □

0.1.1 凑项法

“凑项法”是指在要证明的等式中添加若干项再减去若干项来证明结论的方法.

命题 0.3

$(x^d - a^d) \mid (x^n - a^n)$ 的充要条件是 $d \mid n$, 其中 $a \neq 0$. ♣

证明 (\Leftarrow): 由 $d \mid n$ 可设 $n = kd, k \in \mathbb{N}_+$. 从而

$$x^n - a^n = (x^d)^k - (a^d)^k = (x^d - a^d)(x^{d(k-1)} + x^{d(k-2)}a^d + \cdots + a^{d(k-1)}).$$

故 $(x^d - a^d) \mid (x^n - a^n)$.

(\Rightarrow): 假设 $d \nmid n$, 则由带余除法可知, 存在 $q, r \in \mathbb{N}_+$ 且 $0 \leq r < d$, 使得 $n = qd + r$. 于是

$$x^n - a^n = x^{dq+r} - a^{dq+r} = (x^{dq} - a^{dq})x^r + x^r a^{dq} - a^{dq+r} = (x^{dq} - a^{dq})x^r + a^{dq}(x^r - a^r).$$

注意到 $(x^{dq} - a^{dq}) \mid (x^d - a^d)$, 但由 $0 \leq r < d$ 可知, $(x^d - a^d) \nmid (x^r - a^r)$. 故 $(x^d - a^d) \nmid (x^n - a^n)$ 矛盾! □

例题 0.3 设 $f(x) = x^{3m} + x^{3n+1} + x^{3p+2}$, 其中 m, n, p 为自然数, 又 $g(x) = x^2 + x + 1$, 求证: $g(x) \mid f(x)$.

证明 由 **命题 0.3** 可知, $(x^3 - 1) \mid (x^{3k} - 1), \forall k \in \mathbb{N}_+$. 又因为 $(x^2 + x + 1) \mid (x^3 - 1)$, 所以 $(x^2 + x + 1) \mid (x^{3k} - 1), \forall k \in \mathbb{N}_+$. 注意到

$$x^{3m} + x^{3n+1} + x^{3p+2} = (x^{3m} - 1) + x(x^{3n} - 1) + x^2(x^{3p} - 1) + (x^2 + x + 1).$$

再结合 $(x^2 + x + 1) \mid (x^{3m} - 1), (x^{3n} - 1), (x^{3p} - 1)$ 可得 $g(x) \mid f(x)$. □