

高等代数加：多项式（讲稿）

1 数域、多项式环

最小的数域是 \mathbb{Q} , 最大的数域是 \mathbb{C} . 多项式集合 $\mathbb{F}[x]$ 关于通常的加法和乘法构成一个环.

2 带余除法与整除

定理 2.1. 设 $g(x) \in \mathbb{F}[x] \setminus \{0\}$, 对于任意 $f(x) \in \mathbb{F}[x]$, 存在唯一的 $q(x), r(x) \in \mathbb{F}[x]$ 使得

$$f(x) = q(x)g(x) + r(x), \deg r(x) < \deg g(x).$$

特别地, 若 $r(x) = 0$, 则称 $g(x)$ 整除 $f(x)$, 记为 $g(x)|f(x)$.

注 2.1. 考虑映射

$$\begin{aligned} \varphi: \mathbb{F}[x] &\longrightarrow \mathbb{F}_{n-1}[x] \\ f(x) &\longmapsto r(x) \end{aligned}$$

其中 $n = \deg g(x)$, $r(x)$ 为 $f(x)$ 除 $g(x)$ 所得的余式. 可以验证 φ 是一个线性映射, 并且是满射, 以及

$$\ker \varphi = \{f(x) \in \mathbb{F}[x] : \exists q(x) \in \mathbb{F}[x], f(x) = q(x)g(x)\} = g(x) \cdot \mathbb{F}[x] =: g\mathbb{F}[x].$$

那么按照同态基本定理就有

$$\mathbb{F}[x]/g\mathbb{F}[x] \simeq \mathbb{F}_{n-1}[x] \simeq \mathbb{F}^n,$$

进而 $\dim_{\mathbb{F}} \mathbb{F}[x]/g\mathbb{F}[x] = n = \deg g(x)$.

注 2.2. 带余除法的结果不随数域的扩大而改变. 即设 $\mathbb{F}_1 \subset \mathbb{F}_2$ 是两个数域, 而 $f(x), g(x) \in \mathbb{F}_1[x]$, 并且在 $\mathbb{F}_1[x]$ 中成立

$$f(x) = q(x)g(x) + r(x), \deg r(x) < \deg g(x),$$

那么上式也是在 $\mathbb{F}_2[x]$ 中 $f(x)$ 对 $g(x)$ 作带余除法的结果.

推论 2.2. $g(x)|f(x) \text{ (in } \mathbb{F}_1[x]) \iff g(x)|f(x) \text{ (in } \mathbb{F}_2[x])$.

例 2.1. 在 \mathbb{Q} 上成立 $x^2 + 1 | x^n + 1$ 的充要条件是 $n \equiv 2 \pmod{4}$.

推论 2.3. $(f(x), g(x)) = d(x) \text{ (in } \mathbb{F}_1[x]) \iff (f(x), g(x)) = d(x) \text{ (in } \mathbb{F}_2[x])$.

3 最大公因式与互素

定理 3.1. 设 $f(x), g(x) \in \mathbb{F}[x]$, 且 $(f(x), g(x)) = d(x)$, 那么存在 $u(x), v(x) \in \mathbb{F}[x]$ 使得

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

注 3.1. 若还有首一多项式 $d(x)$ 是 $f(x), g(x)$ 的公因式, 那么 Bezout 等式是 $(f(x), g(x)) = d(x)$ 的充分条件. 特别地, $(f(x), g(x)) = 1$ 的充要条件是存在 u, v 使得 $uf + vg = 1$.

注 3.2. 辗转相除法求出 $u(x), v(x), d(x)$, 并且这样求出的 u, v 次数就是最低的.

4 多项式的根与重因式

引理 4.1 (余式定理). $x - c | f(x)$ 的充要条件是 c 是 $f(x)$ 的根.

定义 4.1. 称 $p(x)$ 是 $f(x)$ 的 k 重因式, 若

$$p^i(x) | f(x), i = 1, 2, \dots, k, p^{k+1}(x) \nmid f(x).$$

命题 4.2. 若 $p(x)$ 不可约, 且 $p(x)$ 是 $f(x)$ 的 k 重因式, 那么 $p(x)$ 是 $f'(x)$ 的 $k-1$ 重因式.

推论 4.3. $f(x)$ 没有重因式的充要条件是 $(f(x), f'(x)) = 1$.

推论 4.4. 多项式 $g(x) = \frac{f(x)}{(f(x), f'(x))}$ 与 $f(x)$ 有相同的不可约因式, 且无重因式.

推论 4.5. 不可约多项式 $p(x)$ 是 $f(x)$ 的 k 重因式的充要条件是

$$p(x) | f^{(i)}(x), i = 0, 1, \dots, k-1, p(x) \nmid f^{(k)}(x).$$

5 唯一分解定理

命题 5.1. $f(x) \in \mathbb{F}[x]$ 不可约的充要条件是对任意 $a \in \mathbb{F}$ 有 $f(x+a)$ 不可约.

定理 5.2. 设首一多项式 $f(x) \in \mathbb{F}[x]$, 则存在 \mathbb{F} 上的首一不可约多项式 $p_i(x)$ 使得

$$f(x) = p_1^{n_1}(x) \cdots p_s^{n_s}(x).$$

定理 5.3. 设首一多项式 $f(x) \in \mathbb{C}[x]$, 那么存在相异复数 c_i 使得

$$f(x) = (x - c_1)^{n_1} \cdots (x - c_s)^{n_s},$$

其中 $\deg f(x) = n_1 + \cdots + n_s$.

推论 5.4 (Vieta 公式). 设数域 \mathbb{F} 上的多项式 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ 的 n 个复根为 x_1, \dots, x_n , 则有

$$\sigma_k = \sum_{1 \leq i_1 < \cdots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k} = (-1)^k \frac{a_{n-k}}{a_n}.$$

定理 5.5. 设首一多项式 $f(x) \in \mathbb{R}[x]$, 那么

$$f(x) = (x - c_1)^{n_1} \cdots (x - c_s)^{n_s} (x^2 + p_1 x + q_1)^{m_1} \cdots (x^2 + p_l x + q_l)^{m_l},$$

其中 $c_i, p_j, q_j \in \mathbb{R}$, 且 $p_j^2 - 4q_j < 0$, 以及 $\deg f(x) = n_1 + \cdots + n_s + 2m_1 + \cdots + 2m_l$.

定理 5.6. 设 $f(x) \in \mathbb{Z}[x]$, 那么 $f(x)$ 在 \mathbb{Q} 上不可约的充要条件是 $f(x)$ 在 $\mathbb{Z}[x]$ 上不可约.

命题 5.7. 设 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, 那么 $\frac{p}{q}$ 是 $f(x)$ 的有理根的必要条件是 $p \mid a_0, q \mid a_n$.

定理 5.8 (爱森斯坦判别法). 设 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, 若存在素数 p 使得 $p \mid a_i, i = 1, 2, \cdots, n-1$, 且 $p \nmid a_n, p^2 \nmid a_0$, 那么 $f(x)$ 在 \mathbb{Z} 上不可约.

例 5.1. 设 p 是素数, 那么 $\Phi_p(x) = 1 + x + \frac{x}{2!} + \cdots + \frac{x^p}{p!}$ 在 \mathbb{Q} 上不可约.

例 5.2. 设 $p > 2$ 是素数, 那么 $x^p + px + 1$ 在 \mathbb{Q} 上不可约.

6 习题解答

题 1. 设有理系数多项式 $f(x)$ 在 \mathbb{Q} 上不可约, 而非零复数 α 是 $f(x)$ 的根.

(1) 定义

$$M = \{g(x) \in \mathbb{Q}[x] : g(\alpha) = 0\} \subset \mathbb{Q}[x],$$

证明: $g(x) \in M$ 的充分必要条件是 $f(x) | g(x)$;

证明. 充分性是显然的, 下面证明必要性.

断言 $f(x)$ 是 M 中次数最低的非 0 多项式. 若不然, 存在 $r(x) \in \mathbb{Q}[x]$ 使得 $r(\alpha) = 0$, 且 $0 < \deg r(x) < \deg f(x)$. 那么在 \mathbb{C} 上 $f(x)$ 与 $r(x)$ 有公因式 $x - \alpha$, 而最大公因式不随数域扩大而改变, 这就得到在 \mathbb{Q} 上 $(f(x), r(x)) \neq 1$, 与 $f(x)$ 的不可约性矛盾.

设 $g(x) \in M$, 作带余除法有 $g(x) = q(x)f(x) + r(x)$, 其中 $\deg r(x) < \deg f(x)$. 由 $f(\alpha) = g(\alpha) = 0$ 有 $r(\alpha) = 0$, 结合断言可知 $r(x) = 0$, 于是有 $f(x) | g(x)$. \square

(2) 定义

$$\mathbb{Q}[\alpha] = \{h(\alpha) : h(x) \in \mathbb{Q}[x]\},$$

计算 $\dim_{\mathbb{Q}} \mathbb{Q}[\alpha]$;

解. 设 $\deg f(x) = n$, 来证 $1, \alpha, \dots, \alpha^{n-1}$ 是 $\mathbb{Q}[\alpha]$ 的一组基.

设 $a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} = 0$, 则 α 是多项式 $g(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$ 的根, 即 $g(x) \in M$, 由上题可知 $g(x)$ 是零多项式, 即 $a_0 = a_1 = \dots = a_{n-1} = 0$, 从而 $1, \alpha, \dots, \alpha^{n-1}$ 是线性无关的.

设 $h(\alpha) \in \mathbb{Q}[\alpha]$, 作带余除法 $h(x) = u(x)f(x) + v(x)$, 其中 $\deg v(x) < \deg f(x) = n$. 则有 $h(\alpha) = v(\alpha)$ 可由 $1, \alpha, \dots, \alpha^{n-1}$ 线性表示.

综上所述可知 $1, \alpha, \dots, \alpha^{n-1}$ 是 $\mathbb{Q}[\alpha]$ 的一组基, 那么 $\dim_{\mathbb{Q}} \mathbb{Q}[\alpha] = n = \deg f(x)$. \square

注 6.1. $\mathbb{Q}[\alpha] \simeq \mathbb{Q}[x]/M = \mathbb{Q}[x]/f \cdot \mathbb{Q}[x] \simeq \mathbb{Q}^n$.

(3) 证明: $\mathbb{Q}[\alpha]$ 是一个数域.

证明. 容易看出 $0, 1 \in \mathbb{Q}[\alpha]$ 且 $\mathbb{Q}[\alpha]$ 关于加减乘法封闭, 只需证明除法封闭.

由上题可知 $\mathbb{Q}[\alpha] = \{h(\alpha) : h(x) \in \mathbb{Q}_{n-1}[x]\}$, 只需证明对任意 $h(x) \in \mathbb{Q}_{n-1}[x] \setminus \{0\}$, 存在 $\lambda(x) \in \mathbb{Q}_{n-1}[x]$ 使得 $\lambda(\alpha) = \frac{1}{h(\alpha)}$.

由于 $\deg h(x) < \deg f(x)$, 由 $f(x)$ 的不可约性得到 $(h(x), f(x)) = 1$, 那么存在 $\lambda(x), \mu(x) \in \mathbb{Q}_{n-1}[x]$ 使得

$$\lambda(x)h(x) + \mu(x)f(x) = 1,$$

于是有 $\lambda(\alpha)h(\alpha) = 1$. \square

题 2. 记 $\mathbb{C}_{n-1}[x]$ 为全体次数不超过 $n-1$ 的复系数多项式构成的复线性空间.

(1) 证明: $\dim_{\mathbb{C}} \mathbb{C}_{n-1}[x] = n$;

证明. 验证 $1, x, \dots, x^{n-1}$ 是 $\mathbb{C}_{n-1}[x]$ 的一组基即可. \square

(2) 设 a_1, \dots, a_n 为互不相同的复数. 给出多项式 $\delta_1, \dots, \delta_n \in \mathbb{C}_{n-1}[x]$ 使得 $\delta_i(a_i) = 1$, 且 $i \neq j$ 时有 $\delta_i(a_j) = 0$, 并证明 $\delta_1, \dots, \delta_n$ 构成 $\mathbb{C}_{n-1}[x]$ 的一组基;

证明. 定义 $\delta_i(x) = \frac{\prod_{j \neq i} (x - a_j)}{\prod_{j \neq i} (a_i - a_j)}$, 则其符合题意.

设有 $k_1 \delta_1 + \dots + k_n \delta_n = 0$, 带入 a_i 可得 $k_i = 0$, 于是知 $\delta_1, \dots, \delta_n$ 线性无关, 又 $\mathbb{C}_{n-1}[x]$ 维数为 n , 这就证明了 $\delta_1, \dots, \delta_n$ 是 $\mathbb{C}_{n-1}[x]$ 的一组基. \square

(3) 证明: 对于任意复数 b_1, \dots, b_n , 存在多项式 $f(x) \in \mathbb{C}_{n-1}[x]$ 使得 $f(a_i) = b_i$.

证明. 取 $f(x) = \sum_{i=1}^n b_i \delta_i(x)$ 即可. \square

(4) 证明中国剩余定理: 设 $g_1(x), \dots, g_s(x) \in \mathbb{F}[x]$ 两两互素, $f_1(x), \dots, f_s(x) \in \mathbb{F}[x]$, 且 $\deg f_i(x) < \deg g_i(x)$. 那么存在唯一的 $f(x) \in \mathbb{F}[x]$, 使得 $f(x)$ 除以 $g_i(x)$ 的余式为 $f_i(x) (i = 1, \dots, s)$, 并且 $\deg f(x) < \sum_{i=1}^s \deg g_i(x)$.

证明. 定义 $G_i(x) = \prod_{j \neq i} g_j(x)$, 则 $g_i(x)$ 与 $G_i(x)$ 互素, 那么存在 $u_i(x), v_i(x)$ 使得 $u_i(x) g_i(x) + v_i(x) G_i(x) = 1$. 取 $F_i(x) = v_i(x) G_i(x)$, 则 $F_i(x)$ 除以 $g_i(x)$ 的余式恰为 1, 并且被 $g_j(x)$ 整除. 于是取 $f_0(x) = \sum_{i=1}^s f_i(x) F_i(x)$ 可满足余式要求. 最后做带余除法 $f_0(x) = q_0(x) \prod_{i=1}^s g_i(x) + f(x)$, 取 $f(x)$ 即可满足次数要求. \square

题 3. 设 a_1, a_2, \dots, a_n 是 n 个不同的整数, 证明: 方程组

$$\begin{cases} a_1^{n-1} x_1 + a_1^{n-2} x_2 + \dots + a_1 x_{n-1} + x_n = -a_1^n \\ a_2^{n-1} x_1 + a_2^{n-2} x_2 + \dots + a_2 x_{n-1} + x_n = -a_2^n \\ \vdots \\ a_n^{n-1} x_1 + a_n^{n-2} x_2 + \dots + a_n x_{n-1} + x_n = -a_n^n \end{cases}$$

有唯一解, 并求出它的解.

证明. 由系数矩阵行列式非零知有唯一解, 且 a_1, a_2, \dots, a_n 是多项式 $f(x) = x^n + x_1 x^{n-1} + \dots + x_{n-1} x + x_n$ 的根, 于是由韦达公式就有 $x_i = (-1)^i \sigma_i$. \square

题 4. 设 $A \in \mathbb{R}^{n \times n}$ 是 n 阶实方阵, 已知 A 的特征值均为实数, 且 A 的一阶主子式之和与二阶主子式之和均为 0, 证明: A 是幂零阵.

证明. 设 A 的特征值为 $\lambda_1, \dots, \lambda_n$, 则 $\lambda_1^2 + \dots + \lambda_n^2 = \sigma_1^2 - 2\sigma_2 = 0$, 又 λ_i 都是实数, 这就有 $\lambda_1 = \dots = \lambda_n = 0$, 因此 A 是幂零阵. \square