0.1 不可约多项式与因式分解

定义 0.1 (不可约多项式的定义)

设 $f(x)$ 是数域 $\mathbb{F}$ 上的多项式, 若 $f(x)$ 可以分解为两个次数小于 $f(x)$ 的 $\mathbb{F}$ 上多项式之积, 则称 $f(x)$ 是 $\mathbb{F}$ 上的可约多项式, 否则称 $f(x)$ 为 $\mathbb{F}$ 上的不可约多项式.

命题 0.1 (不可约多项式的基本性质)

(1) 设 $p(x)$ 是数域 $\mathbb{K}$ 上的不可约多项式, 则对 $\mathbb{K}$ 上任一多项式 $f(x)$, 或者 $p(x) \mid f(x)$, 或者 $(p(x), f(x)) = 1$.

(2) 设 $p(x)$ 是数域 $\mathbb{F}$ 上的不可约多项式, $f(x)$ 是 $\mathbb{F}$ 上的多项式. 证明: 若 $p(x)$ 的某个复根 a 也是 $f(x)$ 的根, 则 $p(x) \mid f(x)$. 特别地, $p(x)$ 的任一复根都是 $f(x)$ 的根.

笔记 不可约多项式的基本性质 (2) 表明: 不可约多项式也满足极小多项式的基本性质.

证明

(1) 设 $d(x) = (p(x), f(x))$. 因为 $p(x)$ 不可约, 故 $f(x)$ 的因式只能是非零常数多项式或 $cp(x)(c \neq 0)$, 从而或者 $d(x) = 1$ 或者 $d(x) = cp(x)$ (首一多项式), 故得结论.

(2) 若 $(p(x), f(x)) = 1$, 则存在 $\mathbb{F}$ 上的多项式 $u(x), v(x)$, 使得 $p(x)u(x) + f(x)v(x) = 1$. 令 $x = a$ 可得 $1 = p(a)u(a) + f(a)v(a) = 0$, 矛盾. 因此 $p(x)$ 与 $f(x)$ 不互素, 从而只能是 $p(x) \mid f(x)$, 结论得证.

□

定理 0.1 (不可约多项式的"素性")

设 $p(x)$ 是数域 $\mathbb{F}$ 上的非常数多项式, 则 $p(x)$ 为 $\mathbb{F}$ 上不可约多项式的充要条件是对 $\mathbb{F}$ 上任意适合 $p(x) \mid f(x)g(x)$ 的多项式 $f(x)$ 与 $g(x)$, 或者 $p(x) \mid f(x)$, 或者 $p(x) \mid g(x)$.

证明 必要性: 设 $p(x)$ 是 $\mathbb{F}[x]$ 中的不可约多项式, 且 $p(x) \mid f(x)g(x)$. 若 $p(x) \mid f(x)$, 则结论成立. 若 $p(x) \nmid f(x)$, 则由定理可知 $(p(x), f(x)) = 1$, 从而由互素多项式与最大公因式的基本性质可知 $p(x) \mid g(x)$.

充分性:(反证法) 假设 $p(x)$ 可约, 则必存在次数小于 $\deg(p(x))$ 的多项式 $f(x)$,$g(x)$, 使得 $p(x) = f(x)g(x)$. 从而 $p(x) \mid f(x)g(x)$, 于是由条件可知 $p(x) \mid f(x)$ 或 $p(x) \mid g(x)$. 因此 $\deg(p(x)) \leqslant \deg(f(x))$ 或 $\deg(g(x))$. 这与 $\deg(p(x)) > \deg(f(x))$,$\deg(g(x))$ 矛盾. □

推论 0.1

设 $p(x)$ 为不可约多项式且

$$p(x) \mid f_1(x)f_2(x)\cdots f_m(x),$$

则 $p(x)$ 必可整除其中某个 $f_i(x)$.

证明 由不可约多项式的"素性"归纳可得. □

命题 0.2

设 $f(x)$ 是数域 $\mathbb{F}$ 上的非常数多项式, 求证: $f(x)$ 等于某个不可约多项式的幂的充要条件是对任意的非常数多项式 $g(x)$, 或者 $f(x)$ 和 $g(x)$ 互素, 或者 $f(x)$ 可以整除 $g(x)$ 的某个幂.

证明 设 $f(x) = p(x)^k$, $p(x)$ 在 $\mathbb{F}$ 上不可约, 且 $f(x)$ 和 $g(x)$ 不互素, 则 $p(x)$ 是 $f(x)$ 和 $g(x)$ 的公因式, 故 $f(x)$ 可以整除 $g(x)^k$.

反之, 由因式分解定理, 可设 $f(x) = p(x)^m h(x)$, $p(x)$ 在 $\mathbb{F}$ 上不可约, $\deg h(x) > 0$, 且 $p(x)$ 不能整除 $h(x)$, 则 $h(x) \mid f(x)$, 故 $f(x)$ 不和 $h(x)$ 互素. 由于 $\deg h(x) < \deg f(x)$, 因此 $f(x)$ 也不能整除 $h(x)$. 若存在正整数 $k \geqslant 2$, 使得 $f(x) \mid h^k(x)$, 则存在 $g \in \mathbb{F}[x]$, 使得 $f(x) = g(x)h^k(x) = p^m(x)h(x)$, 于是 $p^m(x) = g(x)h^{k-1}(x)$. 从而 $h^{k-1}(x) \mid p^m(x)$. 但由 $p(x) \nmid h(x)$ 且 $p(x)$ 不可约知 $(p(x), h(x)) = 1$, 因此由互素多项式和最大公因式的基本性质**??**知 $(p^m(x), h^{k-1}(x)) =$

1, 矛盾! □

定义 0.2 (代数数)

设 u 是复数域中某个数, 若 u 适合某个非零有理系数多项式 (或整系数多项式) $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$, 则称 u 是一个**代数数**. ♣

定义 0.3 (极小多项式 (最小多项式))

对任一代数数 u, 存在唯一一个 u 适合的首一有理系数多项式 $g(x)$, 使得 $g(x)$ 是 u 适合的所有非零有理系数多项式中次数最小者. 这样的 $g(x)$ 称为 u 的**极小多项式**或**最小多项式**. ♣

证明 现在证明这个定义是良定义的, 只须证明对任一代数数所对应的极小多项式的存在性和唯一性.

先证存在性. 在 u 适合的所有非零有理系数多项式构成的集合中 (由假设这个集合非空, 否则 u 就不是一个代数数), 由良序公理可知, 存在一个次数最小的多项式, 然后将其首一化, 即可得到 u 的极小多项式 $g(x)$.

再证唯一性. 为了证明极小多项式的唯一性, 我们先证明极小多项式的一个基本性质, 即极小多项式可以整除 u 适合的任一多项式 $f(x)$. 假设

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

则由 $f(u)=g(u)=0$ 可知 $r(u)=0$. 若 $r(x)\neq 0$, 则 u 适合一个比 $g(x)$ 的次数更小的多项式 $r(x)$, 这和 $g(x)$ 是极小多项式矛盾. 因此 $r(x)=0$, 即 $g(x)\mid f(x)$. 设 $h(x)$ 也是 u 的极小多项式, 则由上述性质可得 $g(x)\mid h(x), h(x)\mid g(x)$, 从而 $g(x)$ 和 $h(x)$ 只差一个非零常数, 又它们都是首一的, 故只能相等, 唯一性得证. □

命题 0.3 (极小多项式的基本性质)

(1) 设 $g(x)$ 为 u 的极小多项式, 则 $g(x)$ 一定整除 u 适合的任一多项式 $f(x)$. ♠

证明

(1) 假设

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

则由 $f(u)=g(u)=0$ 可知 $r(u)=0$. 若 $r(x)\neq 0$, 则 u 适合一个比 $g(x)$ 的次数更小的多项式 $r(x)$, 这和 $g(x)$ 是极小多项式矛盾. 因此 $r(x)=0$, 即 $g(x)\mid f(x)$.

□

命题 0.4 (极小多项式式的充要条件)

设 $g(x)$ 是一个 u 适合的首一有理系数多项式, 则 $g(x)$ 是 u 的极小多项式的充要条件是 $g(x)$ 是有理数域上的不可约多项式. ♠

证明 先证必要性. 若极小多项式 $g(x)$ 在有理数域上可约, 则 $g(x)=g_1(x)g_2(x)$ 可分解为两个比 $g(x)$ 的次数更小的多项式的乘积. 由 $0=g(u)=g_1(u)g_2(u)$ 可知 $g_1(u)$ 和 $g_2(u)$ 中至少有一个等于零. 不妨设 $g_1(u)=0$, 则 u 适合一个比 $g(x)$ 的次数更小的多项式 $g_1(x)$, 这和 $g(x)$ 是极小多项式矛盾.

再证充分性. 设 $g(x)$ 是 u 适合的有理数域上的首一不可约多项式, $h(x)$ 是 u 的极小多项式. 由极小多项式的基本性质 (1)可知 $h(x)\mid g(x)$. 因为 $g(u)=h(u)=0$, 所以 $g(x)$ 和 $h(x)$ 有公共根, 从而 $x-u$ 一定是 $g(x), h(x)$ 的公因式, 于是 $g(x)$ 和 $h(x)$ 不互素. 又 $g(x)$ 是不可约多项式, 因此 $g(x)\mid h(x)$. 于是 $g(x)\sim h(x)$, 即 $g(x)$ 和 $h(x)$ 只差一个非零常数, 而它们又都是首一的, 故只能相等. 因此 $g(x)$ 就是 u 的极小多项式. □

0.1.1 多项式的标准分解

多项式的标准分解是证明某些问题的有力工具.

定理 0.2 (因式分解定理)

设 $f(x)$ 是数域 $\mathbb{K}$ 上的多项式且 $\deg f(x) \geqslant 1$, 则

(1) $f(x)$ 可分解为有限个 $\mathbb{K}$ 上的不可约多项式之积;

(2) 若

$$f(x) = p_1(x)p_2(x)\cdots p_s(x) = q_1(x)q_2(x)\cdots q_t(x). \tag{1}$$

是 $f(x)$ 的两个不可约分解, 即 $p_i(x), q_j(x)$ 都是 $\mathbb{K}$ 上的次数大于零的不可约多项式, 则 $s = t$, 且经过适当调换因式的次序以后, 有

$$q_i(x) \sim p_i(x),\ i = 1, 2, \cdots, s.$$

♡

笔记

1. 这个定理表明, 任一多项式可唯一地分解为若干个不可约多项式之积. 这里唯一是在相伴意义下的唯一, 即相应的多项式可以差一个常数因子. 如果把分解式中相同或仅差一个常数的因式合并在一起, 就得到了一个 **标准分解式**:
$$f(x) = cp_1(x)^{e_1}p_2(x)^{e_2}\cdots p_m(x)^{e_m}, \tag{2}$$
其中 $c \neq 0, p_i(x)$ 是互异的首一不可约多项式, $e_i \geqslant 1(i = 1, 2, \cdots, m)$.
若 $e_i > 1$ $(e_i = 1)$, 我们称(2)式中的因式 $p_i(x)$ 为 $f(x)$ 的e_i **重因式 (单因式)**. 显然这时 $p_i(x)^{e_i} \mid f(x)$, 但 $p_i(x)^{e_i+1}$ 不能整除 $f(x)$.
2. 设 $f(x), g(x)$ 是 $\mathbb{K}$ 上的两个多项式, 在它们的标准分解式中适当添加零次项, 就能得到公共的标准分解. 故对 $\mathbb{K}$ 上任意的两个多项式 $f(x), g(X)$, 都可以不妨设它们有如下的**公共的标准分解式**:
$$f(x) = c_1p_1(x)^{e_1}p_2(x)^{e_2}\cdots p_n(x)^{e_n};$$
$$g(x) = c_2p_1(x)^{f_1}p_2(x)^{f_2}\cdots p_n(x)^{f_n},$$
其中 $e_i \geqslant 0, f_i \geqslant 0(i = 1, 2, \cdots, n)$.

证明 (1) 对多项式 $f(x)$ 的次数用数学归纳法. 若 $\deg f(x) = 1$, 结论显然成立. 设次数小于 n 的多项式都可以分解为 $\mathbb{K}$ 上的不可约多项式之积而 $\deg f(x) = n$. 若 $f(x)$ 不可约, 结论自然成立. 若 $f(x)$ 可约, 则

$$f(x) = f_1(x)f_2(x),$$

其中 $f_1(x), f_2(x)$ 的次数小于 n, 由归纳假设它们可以分解为有限个 $\mathbb{K}$ 上的不可约多项式之积. 所有这些多项式之积就是 $f(x)$.

(2) 对(1)式中的 s 用数学归纳法. 若 $s = 1$, 则 $f(x) = p_1(x)$, 因此 $f(x)$ 是不可约多项式, 于是 $t = 1, q_1(x) = p_1(x)$. 现假设对不可约因式个数小于 s 的多项式结论正确. 由(1)式, 有

$$p_1(x) \mid q_1(x)q_2(x)\cdots q_t(x),$$

由推论 0.1可知, 必存在某个 i, 不妨设 $i = 1$, 使

$$p_1(x) \mid q_1(x).$$

但是 $p_1(x), q_1(x)$ 都是不可约多项式, 因此存在 $0 \neq c_1 \in \mathbb{K}$, 使

$$q_1(x) = c_1p_1(x),$$

此即 $p_1(x) \sim q_1(x)$. 将上式代入(1)式并消去 $p_1(x)$, 得到

$$p_2(x)\cdots p_s(x) = c_1q_2(x)\cdots q_t(x).$$

这时左边为 $s - 1$ 个不可约多项式之积, 由归纳假设, $s - 1 = t - 1$, 即 $s = t$. 另一方面, 存在 $0 \neq c_i \in \mathbb{K}$, 使 $q_i(x) = c_ip_i(x)$. □

推论 0.2

设 $f(x), g(x)$ 是 $\mathbb{K}$ 上的两个多项式, 不妨设它们有如下的公共的标准分解式:

$$f(x) = c_1 p_1(x)^{e_1} p_2(x)^{e_2} \cdots p_n(x)^{e_n};$$
$$g(x) = c_2 p_1(x)^{f_1} p_2(x)^{f_2} \cdots p_n(x)^{f_n},$$

其中 $e_i \geqslant 0, f_i \geqslant 0 (i = 1, 2, \cdots, n)$, 则 $f(x), g(x)$ 的最大公因式

$$(f(x), g(x)) = p_1(x)^{k_1} p_2(x)^{k_2} \cdots p_n(x)^{k_n},$$

其中 $k_i = \min\{e_i, f_i\} (i = 1, 2, \cdots, n)$.

类似地, $f(x), g(x)$ 的最小公倍式

$$[f(x), g(x)] = p_1(x)^{h_1} p_2(x)^{h_2} \cdots p_n(x)^{h_n},$$

其中 $h_i = \max\{e_i, f_i\} (i = 1, 2, \cdots, n)$.

♡

证明 利用最大公因式和最小公倍式的定义容易证明. □

命题 0.5 (整除关系在平方下不变)

证明:$g(x)^2 \mid f(x)^2$ 的充要条件是 $g(x) \mid f(x)$.

♠

证明 充分性是显然的, 只需证明必要性. 设 $f(x), g(x)$ 的公共标准分解为

$$f(x) = c p_1(x)^{e_1} p_2(x)^{e_2} \cdots p_k(x)^{e_k}, \quad g(x) = d p_1(x)^{f_1} p_2(x)^{f_2} \cdots p_k(x)^{f_k},$$

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

$$f(x)^2 = c^2 p_1(x)^{2e_1} p_2(x)^{2e_2} \cdots p_k(x)^{2e_k}, \quad g(x)^2 = d^2 p_1(x)^{2f_1} p_2(x)^{2f_2} \cdots p_k(x)^{2f_k}.$$

若 $g(x)^2 \mid f(x)^2$, 则 $2f_i \leqslant 2e_i$, 从而 $f_i \leqslant e_i (1 \leqslant i \leqslant k)$. 因此 $g(x) \mid f(x)$. □