唯一分解

2023 年 11 月 12 日

目录

1 唯一分解

对于算术基本定理的推广来说，不可约多项式就像是构成多项式的基本块，类似于定理中的素数一样。并且，当我们说$f(x)$是不可约多项式的乘积时，我们也应当允许$f(x)$自身就是不可约多项式。

1.1 唯一分解定理

若k是域，则每个次数≥ 1的多项式$f(x) \in k[x]$都是一些非零常数和不可约多项式的乘积，即：若

$$f(x) = ap_1(x)\cdots p_m(x) \;\; f(x) = bq_1(x)\cdots q_n(x)$$

是两个$f(x)$的分解，且p, q是不可约多项式，则$a = b$，$m = n$对每个i都有$q_i = p_i$

证明： 分解的存在性我们已经在上一章证明过了，现在我们证明唯一性即可。

等式$f(x) = ap_1(x)\cdots p_m(x)$给出了其首系数是$a$。因此乘积里的多项式都是首一的。因此对于两个系数$a, b$来说，就有$a = b$。现在足够来给我们证明

$$p_1(x)\cdots p_m(x) = q_1(x)\cdots q_n(x)$$

的唯一性了。我们对$M = \max\{m, n\} \geq 1$时进行归纳。当$M = 1$时，等式成立，我们有$p_1(x) = q_1(x)$。对于归纳步骤，我们设$p_m(x) \mid q_1(x)\cdots q_n(x)$，利用欧拉定理可知存在某个$i$使得$p_m \mid q_i(x)$是成立的。但$q_i(x)$是不可约多项式，因子只有自身和1，因此$q_i(x) = p_m(x)$。现在，我们重建索引$i$，我们假设$q_n(x) = p_m(x)$并消去，就得到了$p_1(x)\cdots p_{m-1}(x) = q_1(x)\cdots q_{n-1}(x)$。由归纳假设，因为$m = n$，那么$m - 1 = n - 1$对所有多项式成立，因此对于每个$i$都有$q_i = p_i$

1.1.1 例子

我们来检查一个例子，在$I_4[x]$中，多项式

$$x^2 - 1 = (x - 1)(x + 1) = (x - 3)(x + 3)$$

都是成立且都是不可约的因子。

当$x = 1, -1$时，结果都是[0]，所以是一个根，这个等式是成立的。而对于另外两个，$x = 3, -3$则有$3^2 - 1 = [8] = [0]$也是其中的根，所以这个等式也是成立的。这意味着在$I_4[x]$中，唯一分解定理是不成立的。

设k是域，且假设$f(x) \in k[x]$是可分离的，那么就存在一些元素$a, r_1, \cdots, r_n \in k$使得

$$f(x) = a\prod_{i=1}^{n}(x - r_i)$$

成立若$r_1, \cdots, r_s$其中有$s \geq n$是$f(x)$中不同的根，则我们有

$$f(x) = a(x - r_1)^{e_1} \cdots (x - r_s)^{e_s}$$

其中$e_j \geq 1$对每个j成立。而我们把e_j称为根r_j的重数。由于线性多项式总是不可约的，所以唯一分解也表明了重数是well-defined的。

注意： 一个整环R被我们称为UFD，即唯一分解整环。那么这说明每个非零非单位$r \in R$是不可约元素的乘积。这种分解在本质上是唯一的。

1.2 命题

令k是域且令$g(x) = ap_1^{e_1} \cdots p_n^{e_n} \in k[x]$和设$h(x) = bp_1^{f_1} \cdots p_n^{f_n} \in k[x]$，其中$a, b \in k$。而$p_i$是不同的首一不可约多项式，而$e_i, f_i \geq 0$对所有$i$成立，定义

$$m_i = \min\{e_i, f_i\}, M_i = \max\{e_i, f_i\}$$

则

$$(g, h) = p_1^{m_1} \cdots p_n^{m_n},\ [g, h] = p_1^{M_1} \cdots p_n^{M_n}$$

证明： 比较简单，不想写

1.3 引理

令k是域，且$b(x) \in k[x]$是一个次数$\deg(b) \geq 1$的多项式。每个非零$f(x) \in k[x]$可以表示为：

$$f(x) = d_m(x)b(x)^m + \cdots + d_j(x)b(x)^j + \cdots + d_0(x)$$

其中，对每个j，要么$d_j(x) = 0$要么$\deg(d_j) < \deg(b)$

证明： 利用除法，则有$g(x), d_0(x) \in k[x]$使得

$$f(x) = g(x)b(x) + d_0(x)$$

其中$d_0(x) = 0$或者$\deg(d_0) < \deg(b)$。现在$\deg(f) = \deg(gb)$。而$\deg(b) \geq 1$有$\deg(g) < \deg(f)$。由归纳假设则这里有一些$d_j(x) \in k[x]$使得每个$d_j(x) = 0$或者$\deg(d_j) < \deg(b)$，即

$$g(x) = d_m b^{m-1} + \cdots + d_2 b + d_1$$

因此

$$\begin{aligned} f = gb + d_0 &= (d_m b^{m-1} + \cdots + d_2 b + d_1)b + d_0 \\ &= d_m b^m + \cdots + d_2 b^2 + d_1 b + d_0 \end{aligned}$$

1.4 定义：互素

多项式$q_1(x), \cdots, q_n(x) \in k[x]$，其中$k$是域，它们是互素的是在说对$i \neq j$都有$(q_i, q_j) = 1$

1.5 引理

令k是域，且令$f(x)/g(x) \in k(x)$，假设$g(x) = q_1(x) \cdots q_m(x) \in k[x]$且其中$q_i, q_j$互素。则这里存在一些$a_i(x) \in k[x]$使得

$$\frac{f(x)}{g(x)} = \sum_{i=1}^{m} \frac{a_i(x)}{q_i(x)}$$

证明： 我们对$m \geq 1$进行归纳，当$m = 1$时是成立的。现在我们设$q_1, q_2 \cdots q_m$是互素的，则这里有一些多项式s, t使得$1 = sq_1 + tq_2 \cdots q_m$，因此

$$\begin{aligned} \frac{f}{g} =& (sq_1 + tq_2 \cdots q_m)\frac{f}{g} \\ =& \frac{sq_1 f}{g} + \frac{tq_2 \cdots q_m f}{g} \\ =& \frac{sq_1 f}{q_1 \cdots q_m} + \frac{tq_2 \cdots q_m f}{q_1 \cdots q_m} \\ =& \frac{sf}{q_2 \cdots q_m} + \frac{tf}{q_1} \end{aligned}$$

其中$q_2, \cdots, q_m$是互素的，由归纳假设可知定理成立。

1.6 定理：部分分式

令k是域，且令其一个首一多项式$g(x)\in k[x]$的不可约分解为

$$g(x)=p_1(x)^{e_1}\cdots p_m(x)^{e_m}$$

若$f(x)/g(x)\in k(x)$，则

$$\frac{f(x)}{g(x)}=h(x)+\sum_{i=1}^{m}\left(\frac{d_{i_1}(x)}{p_i(x)}+\frac{d_{i_2}(x)}{p_i(x)^2}+\cdots+\frac{d_{i_{e_i}}(x)}{p_i(x)^{e_i}}\right)$$

其中$h(x)\in k[x]$且$d_{ij}(x)=0$或则$\deg(d_{ij})<\deg(p_i)$对所有j成立。

证明 多项式$p_1(x)^{e_1},p_2(x)^{e_2},\cdots,p_m(x)^{e_m}$是俩俩互素的，利用引理1.5可知，存在一些$a_i(x)\in k[x]$使得

$$f(x)=\sum_{i=1}^{m}\frac{a_i(x)}{p_i(x)^{e_i}}$$

对于每个i，除法给出多项式$Q_i(x)$和$R_i(x)$使得$a_i(x)=Q_i(x)p_i(x)^{e_i}+R_i(x)$，其中要么$R_i(x)=0$，要么$\deg(R_i)<\deg(p_i(x)^{e_i})$。现在我们有

$$\frac{a_i(x)}{p_i(x)^{e_i}}=Q_i(x)+\frac{R_i(x)}{p_i(x)^{e_i}}$$

利用引理1.3，$R_i(x)$可以被写为一些多项式之和。

$$R_i(x)=d_{im}p_i(x)^m+d_{i,m-1}(x)p_i(x)^{m-1}+\cdots+d_{i0}(x)$$

其中，对所有j要么$d_{ij}=0$要么$\deg(d_{ij})<\deg(p_i)$，更一般的我们有$\deg(R_i)<\deg(p_i^{e_i})$，得到$m\le e_i$，因此

$$\begin{aligned}\frac{a_i}{p_i(x)^{e_i}}=&\frac{d_{im}p_i(x)^m+d_{i,m-1}(x)p_i(x)^{m-1}+\cdots+d_{i0}(x)}{p_i(x)^{e_i}}\\=&Q_i(x)+\frac{d_{im}(x)p_i(x)^m}{p_i(x)^{e_i}}+\frac{d_{i,m-1}(x)p_i(x)^{m-1}}{p_i(x)^{e_i}}+\cdots+\frac{d_{i0}(x)}{p_i(x)^{e_i}}\end{aligned}$$

因此，只要消掉分子上的多项式变成定理的形状就是我们要的了，注意$1\le s\le e_i$然后我们只需要把所有的不少有理多项式的和加起来记为$h(x)$，则定理得证。

2 习题

> 若$f(x) \in R[x]$，证明$f(x)$在C中无重根当且仅当$(f, f') = 1$

证明： 设$f(x)$是无重根的多项式，那么$f(x)$可以被分解为一些一次不可约多项式的乘积，即

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_n)$$

而

$$\begin{aligned} f'(x) \quad &= (x - a_2)(x - a_3) \cdots (x - a_n) \\ &+ (x - a_1)(x - a_3) \cdots (x - a_n) \\ &+ \cdots \\ &+ (x - a_1)(x - a_2) \cdots + (x - a_{n-1}) \end{aligned}$$

是$n-1$次的。而$f'(x)$中无法提出公因子，因此$(f, f') = 1$。反过来，若$(f, f') = 1$，我们假设是存在重根，即

$$f(x) = (x - a_1)^{e_1}(x - a_2)^{e_2} \cdots$$

其中$e_i \geq 1$对于其导数来说，若刚刚好$e_i = 1$对某项成立。但对$e_i > 1$的来说还会保留一个因子，那么对于这个非零的多项式来说$f'(x)$至少存在一个公因子$(x - a_j)^{e_j}$对某个j成立，其中$e_j > 0$，使得$(x - a_j)^{e_j} \mid f(x)$。因此$(f, f') \neq 1$矛盾。