交换环2

2024 年 5 月 21 日

目录

1 唯一分解

我们已经证明了在$\mathbb{Z}$和域$k[x]$上的唯一分解定理，实际上我们进一步的也证明了它们的共同推广，每个欧拉环有唯一分解。我们现在的目标是再推广这个结果，首先将其推广到主理想整环上(PID)，然后推广到$R[x]$上，其中R是具有唯一分解的环。然后得出一个域k上的多变量多项式$k[x_1, \cdots, x_n]$中有唯一分解。且藉此得出两个多变量的多项式有最大公因式。

我们首先回顾一些定义。我们说a是b的相伴元，若存在单位$u \in R$使得$b = ua$。例如，在$\mathbb{Z}$中，单位是± 1，所以整数m的相伴元就只有$\pm m$，在$k[x]$中，k是域，则它的单位是非零常数。那么其中对多项式$f(x) \in k[x]$的相伴元就是$uf(x)$，其中$u \in k, u \neq 0$，结合上述两者，那么$\mathbb{Z}[x]$的相伴元就是$\pm f(x) \in \mathbb{Z}$

考虑两个主理想(a)和(b)，在上次的证明中我们知道，它俩等价当且仅当$a = rb$对某个$r \in R$成立。其中R是交换环。当R是整环的时候我们可以得到更多的信息

1.1 命题

令R是整环，在设$a, b \in R$

1. $a \mid b$和$b \mid a$当且仅当a和b是相伴元。

2. 主理想(a)和(b)是等价的当且仅当a, b是相伴元。

证明： 第一个定理的证明实际上是之前证明过的：

设R是整环，若$a, b \in R$非零，则$a \mid b$且$b \mid a$当且仅当存在某个单位$u \in R$使得$b = ua$

证明2： 若$(a) = (b)$，则$(a) \subseteq (b)$和$(b) \subseteq (a)$成立。因此，$a \in (b)$和$b \in (a)$成立，就有$a \mid b$和$b \mid a$，利用定理1，a, b是相伴元

反之，我们设a, b是相伴元，由于R是整环，那么就有$b = ua$使得$(a) \subseteq (b)$和$b = va \in (a) \subseteq (b)$。因此$(a) = (b)$

1.2 定义：不可约

元素p在交换环中不可约，若其既不是0也不是单位且，并且它的唯一因子是单位或者是p的相伴元。

1.3 定义：不可约元的乘积

若R是交换环，则元$r \in R$是不可约元乘积，若r既不是0也不是单位，且存在不可约元$p_1, \cdots, p_n$，其中$n \geq 1$使得$r = p_1, \cdots, p_n$

1.4 定义：唯一分解整环UFD

整环R称为$\mathbb{UFD}$

1. 每个$r \in R$，既不是0也不是单位，且是一些不可约元的乘积。
2. 若$p_1 \cdots p_m = q_1 \cdots q_n$，其中有$p_i$和$q_j$是不可约的，则$m = n$和存在置换$\sigma \in S_n$对全部$i$使得$p_i$和$q_{\sigma(i)}$是相伴元。

1.5 引理

令R是PID

1. 则这里不存在无限严格上升的理想链

$$I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n \subsetneq I_{n+1} \subsetneq \cdots.$$

2. 若$r \in R$既不为零也不是单位，则r是不可约元素的乘积

证明： 若存在无限严格上升链，则定义$J = \bigcup_{n=1}^{\infty} I_n$，我们说$J$是理想，则$a \in I_n$对某个$n$成立。若$r \in R$，那么$ra \in I_n$。由于$I_n$是理想，因此，$ra \in J$，若$a, b \in J$，则存在理想$I_n, I_m$使得$a \in I_n$和$b \in I_m$，因此，不妨假设$I_n \subseteq I_m$，那么$a, b \in I_m$。由于$I_m$是理想，那么$a - b \in I_m$是理想，$a + b \in I_m$也是理想。因此$a - b \in J$。因此$J$是理想。

由于R是PID，我们有$J = (d)$对某个$d \in J$成立，现在d肯定落在某个I_n中，因此。

$$J = (d) \subseteq I_n \subsetneq I_{n+1} \subseteq J$$

这是一个矛盾

证明2： 设r是元$a \in R$的因子，若r, s非单位，有$a = rs$，r称为a的真因子。我们首先证明r是a的真因子，则$(a) \subsetneq (r)$。利用命题1.1，$(a) \subseteq (r)$。若不等式不是严格的，在后一种情况中，那么a和r是相伴元。则这里存在单位,$u \in R$使的$a = ur$，这与a是r的真因子矛盾。

在这里，我们说非零非单位的元$a \in R$是好的，若其是不可约元的乘积.反之说是坏的，我们来证明的是它非一个坏的元素。若a是坏的，则它非不可约。就有$a = rs$，其中r, s是真因子。但好的元素的乘积一样是好的。所以我们假设至少存在一个因子是坏的，设为r，利用我们刚才证明的第一个命题，那么$(a) \subsetneq (r)$。利用归纳，那么就存在序列，其中$a = a_1$,$r = a_2 \cdots a_n \cdots$是坏元的乘积，使得每个$a_{n+1}$是$a_n$的真因子。那么这里就存在严格上升链

$$(a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq (a_n) \subsetneq (a_{n+1}) \subsetneq \cdots$$

和第一部分矛盾。

1.6 命题

令R是整环，其中每个$r \in R$既不是0也不是单位，而是一些不可约元的乘积。则R是UFD当且仅当对每个不可约元$p \in R$，主理想(p)是R中的素理想。

证明： 设R是UFD。若$a, b \in R$且$ab \in (p)$，则这里有$r \in R$使得

$$ab = rp$$

现在，将a, b, r分解为不可约元的乘积。由唯一分解定理，等式左边有一个p的相伴元。这个相伴元是a或者b的因子，因此就有$a \in (p)$或者$b \in (p)$。

反之，我们修改一下算术基本定理的证明，设

$$p_1 \cdots p_m = q_1 \cdots q_n$$

其中p_i, q_j均为不可约元。我们对$\max\{m, n\} \geq 1$用归纳证明$n = m$且重新编号后，对所有q_i和p_i都是相伴元。基础步骤是$m = n = 1$，此时$q_1 = p_1$，他们互为相伴元，成立。现在，由归纳步骤，就有$p_1 \mid q_1 \cdots q_n$。由假设，(p_1)是素理想。那么就有某个q_j使得$p_1 \mid q_j$。但作为不可约元，q_j除单位和相伴元之外没有其他因子，因此q_j和p_i是相伴元。$q_j = up_1$，其中u是单位。然后我们再两边消去p_1，剩下$p_2 \cdots p_m = uq_1 \cdots q_j \cdots q_n$。由归纳假设$m - 1 = n - 1$。所以适当的编号后对所有$i$使得$q_i$和$p_i$是相伴元。

1.7 定理：

若R是PID，则R是UFD。特别的，每个欧拉环都是UFD

证明： 前两个命题的结果，只需要证明p是不可约元的时候，(p)是素理想。设存在一个理想I使得$(p) \subsetneq I$。由于R是PID，那么$I = (b)$对某个b成立。且b非单位。因此，利用引理1.5，b是p的某个真因子。这与p不可约矛盾，那么(p)是一个极大理想。从而是一个素理想。

1.8 定义：最大公因子

令R是交换环和$a_1, \cdots, a_n \in R$。$a_1 \cdots, a_n$的公因子是元$c \in R$使得$c \mid a_i$对所有i成立。而$a_1, \cdots, a_n$的gcd我们定义为公因子d使得$c \mid d$对所有公因子c成立。

注记： 即使在我们熟悉的$\mathbb{Z}$和$k[x]$中，如果不附加其他条件，那么gcd是不唯一的。例如：若d是一对$\mathbb{Z}$中的整数的gcd那么$-d$实际上也是一个gcd，为了使其只剩一个，我们可以加上限定非负整数。

若R是整环，则这里可以看出若d, d'是元$a_1, \cdots, a_n$的gcd.那么$d \mid d'$和$d' \mid d$成立。因此它俩是相伴元，因此$(d) = (d')$，虽然gcd不唯一，但产生了相同的主理想。

1.9 命题：

若R是UFD，则R中任意一组$a_1, \cdots, a_n$的gcd存在。

证明： 我们只需要两个元素a, b的gcd存在，就能进一步的通过归纳证明。

设这里有单位u和v和一些不可约元使得

$$a = up_1^{e_1}p_2^{e_2} \cdots p_t^{e_t}$$

和

$$b = vp_1^{f_1}p_2^{f_2} \cdots p_t^{f_t}$$

其中$e_i \geq 0$和$f_i \geq 0$对所有i成立。若$c \mid a$，则c有分解式$c = \omega p_1^{g_1} \cdots p_t^{g_t}$，其中$\omega$是单位单位且$g_i \leq e_i$。因此，由该分解式$c$是$a, b$的gcd当且仅当$g_i \leq m_i$对每个$i$成立，其中

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

那么我们就找到了gcd是$p_1^{m_1}\cdots p_t^{m_t}$。

1.10 定义：互素

UFDR中的元素$a_1,\cdots,a_n$称为互素的，若对它们所有的gcd都是单位。因此，对每个$a_1,\cdots,a_n$的公因子都是单位。

接下来我们将证明若R是PID，则$R[x]$也是UFD

1.11 定义：本原

多项式$f(x)=a_nx^n+\cdots+a_1x+a_0\in R[x]$，其中$R$是UFD。我们称该多项式是本原的，若其系数都是互素的，因此。$a_0,a_1,\cdots,a_n$的公因子是单位。

1.12 引理

若R是UFD且$f(x),g(x)\in R[x]$是本原的，则他们的乘积$f(x)g(x)$也是本原的。

证明： 若$\pi: R\to R/(p)$是自然映射$\pi: a\to a+(p)$，那么就存在一个唯一的同态$\bar{\pi}: R[x]\to (R/(p))[x]$。他将每个系数变成$\pi(c)$。因为自然映射是环同态，为此同态的映射依然是一个同态。现在，假设多项式$h(x)\in R[x]$是非本原的，那么就存在一些不可约元p使得$\bar{\pi}(h)=0\in R/(p)$[1]。因此$\bar{\pi}(h)=0$。因此，若f,g的乘积非本原，那么就有不可约元p使得$\bar{\pi}(fg)=\bar{\pi}(f)\bar{\pi}(g)=0\in (R/(p))[x]$。利用命题1.6。由于$(p)$是素理想那么$R/(p)$是整环。那么$(R/[p])[x]$也依然是整环。但，由于$fg$非本原，又因为$R/(p)[x]$是整环，要么$\bar{\pi}(f)$是0，要么$\bar{\pi}(g)$是0。但由题设，$f,g\neq 0$。为此和$R/(p)[x]$是整环矛盾。

1.13 定义：容度

若R是UFD且$f(x)=a_nx^n+\cdots+a_1x+a_0\in R[x]$，定义$c(f)\in R$是$a_n,\cdots,a_1,a_0$的gcd，称$c(f)$是$f(x)$的容度。

[1]令系数都是p的次数就行

注记： 一个多项式的容度并不是唯一的，但任意两个容度是相伴元，当UFD上一个多项式被给定，则$c(f)$表示任意一个容度。

1.14 引理：

令R是UFD

1. 每个非零$f(x) \in R[x]$都有分解：

$$f(x) = c(f)f^*(x)$$

其中$c(f) \in R$，$f^*(x)$是本原的。

2. 在下列条件给定的意义上，分解是唯一的：$f(x) = dg^*(x)$，其中$d \in R$且$g^*(x) \in R[x]$是本原的，则d和$c(f)$是相伴元且$f^*(x)$和$g^*(x)$是相伴元。

3. 令$g^*(x), f(x) \in R[x]$，若g^*是本原的且$g^*(x) \mid bf(x)$，其中$b \in R$，则$g^*(x) \mid f(x)$

证明： 若$a_nx^n + \cdots + a_1x + a_0$和$c(f)$是$f(x)$的容度，则这里存在在$R$对$i = 0, \cdots, n$的分解$a_i = c(f)b_i$，其中$c(f)$是$b_i$的最大公因子，那么我们就有$f(x) = c(f)f^*(x)$成立。因此$f^*(x)$是本原的。

证明2： 为了证明唯一，我们要证明的是$c(f)$和d是唯一的，其中d是$f(x) = dg^*(x)$得到的另一种分解的系数，那么$f(x) = c(f)f^*(x) = dg^*(x)$。其中$c(f) \mid d$，若$c(f)$是真因子，就有$d = rc(f)$，其中$r \in R$非单位，从而$g^*(x) = rf^*(x)$。若$d, c(f)$是相伴的，那么$d = uc(f)$，其中$u$是单位由题设，$g^*(x)$是本原的，那么我们的$g^*(x) = rf^*(x)$不是本原的。是一个矛盾，意味着$d$不是gcd。因此$c(f)$和$d$是相伴的

证明3： 由于$g^*(x) \mid bf(x)$，那么存在$h(x) \in R[x]$使得

$$bf(x) = g^*(x)h(x)$$

利用证明1，我们可以有$h(x) = c(h)h^*(x)$，其中$h^*(x)$是本原的，带入有

$$bf(x) = c(h)g^*(x)h^*(x)$$

那么b整除$c(h)g^*h^*$中的每个系数，即b是这些系数的一个公因子。由于g^*, h^*是本原的，那么它们的乘积也是本原的。所以$c(h)$就是等号右边的一个容度。则$b \mid c(h)$。有$c(h) = ba$对某个$a \in R$成立。那么$bf(x) = c(h)g^*(x)h^*(x) = bag^*(x)h(x)$，消去后得到$f(x) = ag^*(x)h^*(x)$，因此$g^*(x) \mid f(x)$

1.15 定理：高斯

若R是UFD，则$R[x]$也是UFD

证明： 首先，我们对$\deg(f)$进行归纳来证明，那么每个$f(x) \in R[x]$既不是0也不是单位，可以分解为一些不可约多项式的乘积。若$\deg(f) = 0$，则$f(x)$是位于R中的常量。由于R是UFD，那么f是不可约元的乘积。

若$\deg(f) > 0$，则$f(x) = c(f)f^*(x)$，其中$c(f) \in R$并且$f^*(x)$是本原的。现在，$c(f)$要么是单位，要么是不可约元的乘积。由归纳步骤，若$f^*(x)$是不可约的，则我们直接就证明完毕。但若$f^*(x) = g(x)h(x)$，其中g, h是单位，由于$f^*(x)$是本原的，那么g, h都不是常数。且$\deg(g), \deg(h) < \deg(f^*) = \deg(f)$，由归纳假设，$g, h$是不可约的。因此每个多项式都可以分解为一些不可约多项式的乘积。

利用命题1.6，整环$R[x]$是UFD当且仅当对每个不可约元$p[x]$，主理想$(p[x])$是一个素理想。因此，若$p(x) \mid f(x)g(x)$，则$p(x) \mid f(x)$或者$p(x) \mid g(x)$。不妨假设$p(x) \nmid f(x)$。我们来推导几种情况，在下列推导中我们把$f(x)$简写为f。

1. 假设$\deg(p) = 0$，记

$$f(x) = c(f)f^*(x) \text{和} g(x) = c(g)g^*(x)$$

其中$c(f), c(g) \in R$且$f^*(x), g^*(x)$是本原的。现在$p \mid fg$，那么 $p \mid c(f)c(g)f^*g^*$ 由于f^*, g^*本原，利用引理1.14，那么$c(fg)$是$c(f)c(g)$的相伴元。若$p \in R \mid fg$，则p整除fg的每个系数。因此p就是fg系数的公因字，因此$p \mid c(fg) = c(f)c(g) \in R$，因此$p \mid c(f)$要么$p \mid c(g)$若$p \mid c(f)$，则$p \mid f(x)$与假设矛盾。因此$p \mid c(g)$，有$p \mid g(x)$

2. 设$\deg(p) > 0$。令

$$(p, f) = \{sp + tf : s, t \in R[x]\}$$

那么(p,f)是一个包含了$p(x)$和$f(x)$的理想。选择最小次数的$m(x) \in (p,f)$。若$\mathbf{Q} = \mathbf{Frac}(R)$，那么由$Q[x]$中的除法算是，存在多项式$q'(x), r'(x) \in Q[x]$使得$f(x) = m(x)q'(x)+r'(x)$。其中$r'(x) = 0$或者$\deg(r') < \deg(m)$。去掉分母，则有多项式$q(x), r(x) \in R[x]$和常量$b \in R$使得

$$bf(x) = q(x)m(x) + r(x)$$

其中$r(x) = 0$或者$\deg(r) < \deg(m)$。由于$m \in (p,f)$是理想，那么$r = bf - qm \in (p,f)$。因为m是次数最小的项，则$r = 0$。因此$bf(x) = m(x)q(x)$。那么$bf(x) = c(m)m^*(x)q(x)$，那么$m^*(x) \mid bf(x)$。利用引理1.14，那么$m^*(x) \mid f(x)$。

类似的，我们做替换$f(x)$为$p(x)$。有$m^*(x) \mid p(x)$。由于$p(x)$是不可约的，那么因子就只有单位和相伴元。若$m^*(x)$是$p(x)$的相伴元，利用$m^*(x) \mid m(x)$马上就有$p(x) \mid f(x)$。与我们的假设矛盾。因此$m^*(x)$是单位。那么$m(x) = c(m) \in R$，故(p,f)包含非零的常量$c(m)$。由$c(m) = sp + tf$，那么

$$c(m)g = spg + tfg$$

由于$p(x) \mid f(x)g(x)$，我们有$p \mid c(m)g$，但$p(x)$是本原多项式，那么利用引理1.14[3]，$p(x) \mid c(m)gg(x)$，因此$p(x) \mid g(x)$

1.16 推论：

若k是域，则$k[x_1, \cdots, x_n]$是UFD

证明： 我们对$n \geq 1$归纳。当$n = 1$的时候，那正是欧拉定理。[2] 那么$k[x]$是UFD。对归纳步骤，我们记$k[x_1, \cdots, x_{n+1}] = R[x_{n+1}]$，其中$R = k[x_1, \cdots, x_n]$。由归纳定理，$R$是UFD，利用定理1.15，那么就证明完毕了

[2]欧拉：令k是域且$f(x), g(x) \in k[x]$，若$p(x)$是$k[x]$中的不可约多项式，并且$p(x) \mid f(x)g(x)$，则$p(x) \mid f(x)$或者$p(x) \mid g(x)$。更一般的可以拓展到$p(x) \mid f_1(x) \cdots f_n(x)$，则$p(x) \mid f_i(x)$对某个$i$成立。

1.17 推论：

令R是UFD，再令$Q=\mathrm{Frac}(R)$。令$f(x)\in R[x]$，若

$$f(x)=G(x)H(x)\in Q[x]$$

则这里存在因式分解

$$f(x)=g(x)h(x)\in R[x]$$

其中$\deg(g)=\deg(G)$且$\deg(h)=\deg(H)$。实际上g,G是$Q[x]$中相伴多项式，h,H也如上。

因此，若$f(x)\in R[x]$是次数最小的不可约多项式，那么$f(x)\in Q[x]$也是不可约的。

证明： 由定理1.14，那么我们有如下的因式分解：

$$f(x)=c(G)c(G)G^*(x)H^*(x)\in Q[x]$$

其中$G^*,H^*\in R[x]$是去掉分母后的本原多项式。那么由引理1.14 $c(G)c(H)=c(f)$，由于$c(f)\in R$，那么有分解$f(x)h(x)\in R[x]$，其中$g(x)=c(f)G^*(x)$是消去分母后的多项式。$h(x)$同上。

我们还差最后一个定理。

1.18 推论

令k是域且$f(x_1,\cdots,x_n)\in R[x_n]$是本原多项式，其中$R=[x_1,\cdots,x_{n-1}]$。若$f\in R[x_n]$不能分解为两个次数更小的多项式，那么$f\in k[x_1,\cdots,x_n]$是不可约的。

证明： 我们记$f(x_1,\cdots,x_n)=F(x_n)$,设$F(x_n)=G(x_n)H(x_n)$，由于不能再继续分解，故有一次数应为0，我们设为$G(x_n)$。由于F本原，那么G是$k[x_1,\cdots,x_{n-1}]$中的单位，从而$F(x_n)$是$k[x_1,\cdots,x_n]$中的不可约多项式

1.18.1 例子

我们断言$f(x,y)=x^2+y^2-1\in k[x,y]$是不可约的，其中$k$是特征非2的域。记$Q=k(y)=\mathrm{Frac}(k[y])$，视$f(x,y)\in Q[x]$。我们引入下述习题：

设k是一个域且$1+1\neq 0$，证明$\sqrt{1-x^2}\notin k(x)$，其中$k(x)$是有理函数构成的域。

证明： 我们设$f(x)=\sqrt{1-x^2}$在$k(x)$中，那么存在分解$\sqrt{1-x^2}=\dfrac{h(x)}{g(x)}$，即$1-x^2=\dfrac{h(x)^2}{g(x)^2}$，由于$1-x^2$是有理函数，那么有理函数的平方也是有理函数，因此不妨假设$(g,h)=1$是互素的。那么$(1-x^2)g(x)^2=h(x)^2$，那么$(1-x^2)\mid h(x)^2$，不妨设$h^2(x)=s(x)f(x)^2$，再令$g^2(x)=t(x)f(x)^2$

$$f(x)^2t(x)f(x)^2\mid s(x)f(x)^2\to f(x)^2t(x)\mid s(x)$$

那么$(s,t)=1$且$(s,f^2)=(t,f^2)=1$这与$(g,h)=1$矛盾，因此$\sqrt{1-x^2}\notin k(x)$。

当$char=2$，也就是$1+1=0$时，$f(x)=h(x)/g(x)$是成立的。

所以$g(x)=x^2+(y^2-1)$在$Q[x]$中不可约当且仅当$Q=k(y)$中无根。利用上面的习题就可以写出来了。那么$k[x,y]$是一个UFD，它的理想是一个素理想。因为是可以由一个不可约多项式x^2+y^2-1生成的。