第 9 章　唯一分解整环

在初等数论中，我们已经知道整数的唯一素分解的特性．实际上整数的唯一素分解实际上是整数环的一个特性．现在我们考虑的问题是，是否存在比整数环更抽象的一类环，也存在类似于整数环的素分解的特性？回答是肯定的，这类环也是一类整环，我们称之为单一分解整环．本章的主要目的就是要讨论整环中与分解有关的一些基本概念及一个整环为单一分解整环的充要条件．另外，我们还将介绍几种具体唯一分解整环的实例：主理想整环、欧氏环及唯一分解整环上的多项式环．

§1 分解的基本概念

我们知道在整数环中，与唯一分解密切相关的本概念如整除、素数（素元或既约元）唯一分解的概念等．我们将这些概念可以推广到一般的整环中．

首先给出整除的概念．

定义 1　给定整环 R，$a,b\in R$，如果存在 $c\in R$，满足

$$a=bc$$

则称 a 被 b 整除，或 b 整除 a，记为 $b\mid a$．这时称 b 是 a 的因子，a 为 b 的倍元．否则，b 不能整除 a，记为 $b\nmid a$．

下面我们将讨论两个元素互相整除的充要条件．

定理 1　给定整环 R，$a,b\in R$，则 $b\mid a$ 且 $a\mid b$ 的充要条件是 a 与 b 仅相差一个可逆元，即存在一个可逆元 $c\in R$，使

$$a=bc.$$

证明　必要性：若 a,b 相互整除，由 $b\mid a$ 知存在 $c\in R$ 使

$$a=bc;$$

由 $a\mid b$ 知存在 $c'\in R$ 使

$$b=ac'.$$

所以

$$a=bc=acc'.$$

由整环的消去律得 $cc'=1$．得证．

充分性：若存在可逆元 c 使

$$a = bc,$$

则

$$b = ac^{-1}.$$

从而a，b相互整除．得证．

在整数环中，我们知道如果两个整数相互整除，则这两个数仅相差± 1．± 1恰为整数环的所有逆元．这就提示我们，对于整环的整除而言，如果两个因子仅相差一个逆元，我们认为这两个因子是相同的．在这种意义下，整环的素分解才可能具有唯一性．为了进一步定义素元、既约元的概念，首先定义与逆元有关的几个概念．

定义 2 如果ε是整环R的一个可逆元，则称ε是整环R的一个单位．

R中所有单位组成R的子集U构成一个R的乘法子群．

定义 3 给定整环R，对$a,b \in R$，如果存在一个单位ε使$b = a\varepsilon$．则称a与b相伴，b为a的相伴元，记为$a \sim b$．

例 1 在高斯整数环中，即一切形如$a + bi$（a,b是任意整数)的复数（叫做高斯整数）作成的整环中，有逆元的元的模等于 1，故高斯整数环的单位为$1 = (1, 0)$，$-1 = (-1, 0)$，$i = (0, 1)$和$-i = (0, -1)$．

显然，整环中两个元素相伴即意味着相互整除，并且两个元素互为相伴元．在整数环中，a的所有相伴元既为$\pm a$．

定义 4 给定整环R，对$a,b \in R$，若$b \mid a$，且b不为R的单位或者a的相伴元，则称b为a的真因子．否则，b为a的平凡因子．

显然，对任意的$a \in R$，a的所有的平凡因子即为R的单位与a的相伴元．

定理 2 整环中一个不等于零的元a有真因子的充分而且必要条件是存在b和c都不是单位满足

$$a = bc.$$

证明 若a有真因子b，那么

$$a = bc,$$

由真因子的定义这里的b不是单位，c也不是单位．不然的话

$$b = ac^{-1},$$

b是a的相伴元，与b是a的真因子矛盾．充分性显然．得证．

推论 假定$a \neq 0$，并且a有真因子b, 如果

$$a = bc.$$

那么c也是a的真因子．

如同整数环一样，有了真因子与平凡因子的概念，就可以给出既约元与素元的概念．

定义 5　给定整环 R，$p \in R$，且 $p \mid ab$，必有 $p \mid a$ 或 $p \mid b$，则 p 为 R 的一个素元.

易证，若 p 为素元，$\varepsilon \cdot p$ 也是一个素元，其中 ε 为单位.

定义 6 给定整环 R，$p \in R$，如果

$$p = ab,$$

那么 a 或 b 至少有一个为单位，则 p 为 R 的一个既约元.

显然，在整数环中，既约元即为素元，所以我们在数论中并未区分两个概念的区别. 在一般整环中，既约元与素元未必是两个等价的概念. 二者的关系通过以下定理与例子便可知晓.

定理 3　在整环 R 中，每个素元都是既约元.

证明　设 p 是 R 的素元，且

$$p = ab,$$

则 $p \mid ab$，由素元的定义知，$p \mid a$ 或 $p \mid b$. 不妨设 $p \mid a$，但

$$p = ab \Rightarrow a \mid p,$$

即 a 与 p 相伴，从而 b 是单位. 同样可知 a 是单位，即由 $p = ab$ 可知 $a \in U$ 或 $b \in U$，依定义，p 是既约元.

反过来，既约元不一定是素元. 我们看下列例子：

例 2　设 $R = Z\left[\sqrt{-5}\right]$ 即一切形如 $a + b\sqrt{-5}$ 的所有复数关于数的 $+,\times$ 作成的环，这是一个有单位元1的整环. R 的一切单位满足以下性质.

取 $r \neq 0, r \in U$，设

$$r = a + b\sqrt{-5},$$

于是存在 $s \in U,$

$$s = x + y\sqrt{-5}, \quad rs = 1,$$

即

$$rs = (a + b\sqrt{-5})(x + y\sqrt{-5})$$

$$= (ax - 5by) + (bx + ay)\sqrt{-5} = 1,$$

$$\begin{cases} ax-5by=1, \\ bx+ay=0. \end{cases}$$

因 $r\neq 0$ ，故

$$a^2+5b^2\neq 0,$$

x,y 满足下面等式

$$x=\frac{\begin{vmatrix}1 & -5b\\ 0 & a\end{vmatrix}}{\begin{vmatrix}a & -5b\\ b & a\end{vmatrix}}=\frac{a}{a^2+5b^2},\qquad y=\frac{\begin{vmatrix}a & 1\\ b & 0\end{vmatrix}}{\begin{vmatrix}a & -5b\\ b & a\end{vmatrix}}=\frac{-b}{a^2+5b^2}.$$

但 x,y 是整数，故有 $b=0$，从而 $a=\pm 1$，即 R 中的单位只有 ± 1，$U=\{1,-1\}$.

下面我们证明 3 是 R 的一个既约元，但不是 R 的素元.

设

$$3=(a+b\sqrt{-5})(c+d\sqrt{-5}),$$

希望证明，$a+b\sqrt{-5}=\pm 1,$ 或 $c+d\sqrt{-5}=\pm 1$. 用上面同样方法，有

$$c=\frac{3a}{a^2+5b^2},\quad d=\frac{-3b}{a^2+5b^2}.$$

c,d 是整数 $\Rightarrow b=0,\ a=\pm 3,$ 或 $a=\pm 1,$ 但由 3 的分解式可知若 $a\neq\pm 1$，则 $a+b\sqrt{-5}$ 与 3 相伴，$c+d\sqrt{-5}$ 是单位. 从而 3 是既约元.

3 不是素元，因

$$3\mid(2+\sqrt{-5})(2-\sqrt{-5}),$$

下证

$$3\nmid 2+\sqrt{-5},\ \ 3\nmid 2-\sqrt{-5}.$$

若

$$2+\sqrt{-5}=3(x+y\sqrt{-5}),$$

则 $3x=2,\ 3y=1$ 应有整数解 $x,y,$ 这是不可能的. 同样可得 $3\nmid 2-\sqrt{-5}$.

有了因子的概念，我们可以定义公因子、最大公因子的概念.

定义 8　设 R 为整环，对 $a,b\in R$，存在 $d\in R$ 满足

（1）$d \mid a, d \mid b$；

（2）对任意$c \in S$，若$c \mid a, c \mid b$则，$c \mid d$．

则d是a,b的一个最大公约元，记为$d=(a,b)$．

由定义可知若d是a,b的一个最大公约元，对任意$\varepsilon \in U$,则$d\varepsilon$也是a,b的最大公约元．

d'是a,b的一个最大公约元，则存在$\varepsilon \in U$，使得$d'=d\varepsilon, \varepsilon \in U$．

整环中的两个元不一定有最大公约元．如果有也一般不唯一，容易证明任两个最大公因子互为相伴元．由于a,b的最大公约元一般不是唯一确定的，(a,b)表示a,b的任意一个最大公约元．跟整数的最大公因子表示有所区别，在整数环中，我们约定用符号(a,b)表示正的最大公约元，这是唯一确定的．

例 3 设Q是有理数域，求$Q[x]$上的两个多项式

$$4x^4 - x^3 + x^2 - x - 3$$

和

$$8x^4 + 10x^3 + 11x^2 + 10x + 3$$

的最大公因子．

解 易知题设中的两个多项式公共的整系数因子是

$$(4x+3)(x^2+1)\text{，}$$

对任意的常数$a \in Q$，a是Q中的单位，则这两个多项式的最大公因子是

$$a(4x+3)(x^2+1)\text{．}$$

例 4 举例说明整环$R=Z\left[\sqrt{-5}\right]$中，任给两个元$a,b$，未必存在最大公约元．

解 令

$$a=3\left(2+\sqrt{-5}\right),\quad b=\left(2+\sqrt{-5}\right)\left(2-\sqrt{-5}\right)=9\text{；}$$

则a,b的最大公约元不能是单位，因

$$2+\sqrt{-5} \mid a,\ 2+\sqrt{-5} \mid b.$$

又 a 不是 b 的因子，故 a,b 的最大公约元不能是 a．另一方面，

$$a=3\left(2+\sqrt{-5}\right),$$

而 3 和 $2+\sqrt{-5}$ 都是既约元，从而 a,b 的最大公约元如果存在的话，只能是 3 或 $2+\sqrt{-5}$．亦见 3 或 $2+\sqrt{-5}$ 都不是 a,b 的最大公约元，即对于 R 中这两个元 a,b 来说，(a,b) 不存在．

整环中的最大公因子具有以下特性：

性质 1 $(a,(b,c))\sim((a,b),c)$；$(a,(b,c))\sim((a,b),c)$．

性质 2 $c(a,b)\sim(ca,cb)$．

性质 3 若 $(a,b)\sim 1$，$(a,c)\sim 1$，则 $(a,bc)\sim 1$．

上述三个性质与整数的最大公因子的性质证明类似．所不同的是，等号“=”变成“～”．此处仅给出性质 2 的证明．

性质 2 的证明 命

$$d=(a,b),\ c=(ca,cb),$$

则

$$cd\mid ca,\ cd\mid cb\Rightarrow cd\mid e\ .$$

另一方面，

$$ca=ex,\ cb=ey,$$

命 $e=cdu,$ 则

$$ca=cdux,\quad cb=cduy.$$

由消去律知

$$a=dux,\ b=duy\Rightarrow du\mid a,\ du\mid b\Rightarrow du\mid d,$$

即 u 是单位．所以 $c(a,b)\sim(ca,cb)$．

§2 唯一分解整环

这一节的主要目的是讨论几个关于整环的唯一分解的概念以及整环为唯一分解环的充要条件.

首先我们给出唯一分解整环的概念.

定义 1 给定整环 R， $\forall a \in R, a \neq 0$， a 不是单位，若任何两个 a 的既约元的分解满足 $a = p_1 p_2 \cdots p_s$（p_i 是素数 ）和 $a = q_1 q_2 \cdots q_t$（q_i 是素数），则 $r = s$，并且通过调整 q_i 的次序，使得 $q_i = \varepsilon_i p_i$（ε_i 是 R 的单位），则称环 R 为唯一分解环.

根据定义 1，一个整环的零元和单位一定不能唯一的分解. 因为既约元的乘积不可能是 0，所以 0 不能分解. 而 1 的任何因子只能是单位，而既约元不可能为单位，所以 1 也不能进行既约分解.

整环为唯一分解整环需要满足一定的条件. 这个条件跟素元与既约元密切相关. 首先我们考察以下既约元为素元的一个前提条件.

定理 1 如果对于任意 $a, b \in R$， (a, b)存在，那么 R 中任意既约元皆为素元.

证明 设 p 是 R 的既约元，并设 $p \mid ab$. 若 a, b 都不能被 p 整除，则由 p 的既约性，可知 a 与 p 的公约元只有单位，即 $(p, a) \sim 1$. 同样，由 $p \nmid b$，知 $(p, b) \sim 1$. 由上一节的性质 3 知，$(p, ab) \sim 1$.

另一方面，

$$p \mid ab \Rightarrow (p, ab) \sim p \Rightarrow p \sim 1,$$

与 p 不是单位矛盾，此矛盾表明 $p \mid a$ 或 $p \mid b$.

现在我们就问，一个整环的不等于零也不是单位的元是不是都有唯一分解呢. 下例告诉我们不是的.

例 1 令 $R = \{ a + b\sqrt{-3}$， $a, b \in Z \}$.

R 关于数的加、乘显然是一个整环. 容易证明下列结论：

（1） R 只有两个单位，就是 ± 1.（留作习题）

（2）适合条件 $|\alpha|^2 = 4$ 的 R 的元 α 一定是既约元.

首先，既然 $|\alpha|^2 = 4, \alpha \neq 0$；并且由（1），$\alpha$ 也不是单位，假设 β 是 α 的因子

$$\beta = a + b\sqrt{-3}, \quad \alpha = \beta\gamma .$$

那么

$$4 = |\beta|^2 |\gamma|^2$$

但不管 a, b 是什么整数，

$$|\beta|^2 = a^2 + 3b^2 \neq 2,$$

因此 $|\beta|^2 = 1$ 或 4．若是 $|\beta|^2 = 1,$ 容易证明 β 是单位．若 $|\beta|^2 = 4,$ 那么 $|\gamma|^2 = 1$，γ 是单位，所以 α 为既约元． 4 有以下两种分解

$$4 = 2 \bullet 2 = (1+\sqrt{-3})(1-\sqrt{-3}),$$

因为

$$|2|^2 = 4, \quad |1+\sqrt{-3}|^2 = 4, \quad |1-\sqrt{-3}|^2 = 4.$$

由（2）知以上两种分解均为既约分解，由 $(1), 1+\sqrt{-3}, 1-\sqrt{-3}$ 都不是 2 的相伴元．因而，按照定义，以上是两种不同的既约分解．

定理 2 一个整环 R 为唯一分解整环的充要条件是

（i） R 的每一个既不是零又不是单位的元 a 的真因子序列 $a_1, a_2, \cdots a_n, \cdots$ 只有有限项．

（ii） R 的每个既约元 p 为素元．

证明 必要性：若整环 R 为唯一分解整环．对于任意的 $a \in R, a \neq 0, a \neq 1$，$a$ 有既约分解

$$a = p_1 p_2 \cdots p_n,$$

显然 a 的任意真因子序列最多有 n 项．

设 $a, b \in R$， a, b 均非单位， $p_1, p_2, \cdots p_t$ 是出现在 a, b 的某个既约因子分解中所有互不相伴的既约元，则 a, b 有如下形式的分解

$$a = \varepsilon p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}, \quad b = \varepsilon' p_1^{l_1} p_2^{l_2} \cdots p_t^{l_t},$$

这里 $\varepsilon, \varepsilon'$ 是 R 的单位， k_i, l_j 是非负整数．令

$$d = p_1^{s_1} \cdots p_t^{s_t}, \quad s_i = \min\{k_i, l_i\},$$

则 $d \mid a$， $d \mid b$．并且若有 $c \mid a$， $c \mid b$，则 $c = \varepsilon'' p_1^{m_1} \cdots p_t^{m_t}$，其中 ε'' 也是 R 的单位，且由

$m_i \le k_i$， $m_i \le l_i$ 得 $m_i \le \min\{k_i, l_i\}$．于是 $c \mid d$，即 $d = (a,b)$，由定理 1 知，R 中每一既约元均为素元，即（ii）成立．

充分性： 任给 $a \in R, a \ne 0, a \ne 1$．

1 若 a 为既约元，则 $a = a$ 为一个既约分解．

2 若 a 不为既约元，则 a 有真因子 a_1．

（1）若 a_1 为既约元，令 $a_1 = p_1$，则 $a = p_1 b_1$．

（2）若 a_1 不为既约元，则对 a_1 进行真因子分解，依次类推，得到 a 的一个真因子序列：

$$a_1, a_2, \cdots a_n, \cdots \qquad a_{i+1} \mid a_i$$

由（i）知，该真因子序列只包含有限项，则最后一项为既约元．将该既约元记为 p_1，则 $a = p_1 b_1$．

3 若 b_1 为既约元，记 b_1 为 p_2，得到 a 的素分解．若 b_1 不为既约元，进行（2）（3）的分解，得到 $b_2 = p_2 b_3$，依次类推得到 a 的一个下列形势的真因子序列

$$b_0 = a, b_1, ..., b_n, \quad b_i = p_{i+1} b_{i=1} \quad （p_{i+1} 是既约元）$$

最后一项一定为既约元．所以 a 有既约分解 $a = p_1 p_2 \cdots p_s$．

现在证明唯一性：假定 a 有另一既约分解 $a = q_1 q_2 \cdots q_t$．

下证 $r = s$，并且我们可以把这些 q 的次序调换一下，使得 q_i 是 p_i 的相伴元．

我们用归纳法．先证当 $r = 1$ 的时候， a 有唯一分解．这时

$$a = p_1 = q_1 q_2 \cdots q_s$$

若是 $s \ne 1$，那么 $p_1 = q_1 (q_2 \cdots q_s)$，其中 q_1 不是单位，而 $q_2 \cdots q_s$ 作为素元的乘积也不是单位．这就是说，素元 p 可以写成两个非单位的乘积，这不可能．所以 $s = 1 = r, p_1 = q_1$．

现在假定，能写成 $\le r - 1$ 个素元的乘积的元都有唯一分解．在这个假定之下，我们看一个像上面的两种分解的元 a：

$$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

由性质（iii），p_1 能够整除某一个 q_i；把 q_i 的次序换一换，我们可以假定 $p_1 \mid q_1$．但 q_1 是素元，p_1 不是单位，所以

$$p_1 = \varepsilon q_1, q_1 = \varepsilon^{-1} p_1 \text{（}\varepsilon \text{是单位）.}$$

这样

$$\varepsilon q_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s ,$$

$$b = (\varepsilon p_2) \cdots p_r = q_2 q_3 \cdots q_s ,$$

这里 b 是 $r-1$ 个素元的乘积，所以依照归纳法的假定 $r-1 = s-1$．而且，我们可以把 q_i 的次序交换一下，使得

$$q_2 = \varepsilon'_2 (\varepsilon p_2), \quad q_3 = \varepsilon'_3 p_3, \cdots, \quad q_r = \varepsilon'_r p_r \text{（}\varepsilon'_i \text{是单位）}$$

这样我们得到 $s = r$

$$q_1 = \varepsilon^{-1} p_1, \quad q_2 = (\varepsilon \varepsilon'_2) p_2, \quad q_3 = \varepsilon'_3 p_3, \cdots. \quad q_r = \varepsilon'_r p_r .$$

由定理 2 的证明，我们得到下列一个等价的定理.

定理 3 设 S 是有单位元1且满足消去律的可换整环，S 是唯一分解整环的充要条件是

I) S 中任意真因子序列 $a_1, a_2, \cdots a_n, \cdots$ 只能含有有限项；

II）S 中任意二元的最大公约元均存在.

定理 4 在唯一分解整环 R 中，任意的元素 a 可以写成下列标准形式的既约分解

$$a = p_0^{\alpha_0} p_1^{\alpha_1} \cdots p_{n-1}^{\alpha_{n-1}}, \; p_0, \ldots p_{n-1}$$

为互不相伴的既约元.

由于在唯一分解整环中，既约元与素元等价，所以上述分解通常也称为素分解.

在唯一分解整环中，通常可以通过两个元素的标准分解式得到两个元素的最大公因子.

定理 5 在唯一分解整环 R 中，对于 $a, b \in R$，若

$$a = \varepsilon_a p_1^{h_1} p_2^{h_2} \cdots p_n^{h_n}, \quad \text{（}\varepsilon_a \text{是单位，} h_i \geq 0 \text{）}$$

$$b = \varepsilon_b p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}, \quad \text{（}\varepsilon_b \text{是单位，} k_i \geq 0 \text{）}$$

用 l_i 来表示 h_i 与 k_i 中较小的一个，

$$d = p_1^{l_1} p_2^{l_2} \cdots p_n^{l_n},$$

那么 d 为 a,b 的一个最大公因子． a,b 的其他最大公因子 d' 写作 $d' = \varepsilon d$ 的形式．

§3　主理想整环

前面已经介绍了一个整环为唯一分解整环的充要条件．这一节的主要目的是讨论一些具体的唯一分解整环．我们已经知道整数环是唯一分解整环．关于整数环的唯一分解及其它一些特性我们已经在初等数论的第 1 章给除了较详细的讨论，在这里我们不再重复描述．我们感兴趣的是其它的一些具有代表性的唯一分解整环．本节将给出三类唯一分解整环，它们分别是：主理想整环、多项式环、欧氏环，其中欧氏环为一种特殊的主理想整环．

首先我们介绍主理想环。

定义 1　一个整环 R 叫做一个主理想环，假如 R 的每一个理想都是一个主理想．

下面定理说明了主理想环是唯一分解整环．

定理 1 每一个主理想整环 R 为唯一分解整环．

证明 只要证明 R 满足第 2 节定理 3 中的两个条件即可．

首先证明 R 中任意真因子序列仅含有限项．

假设 $a_1, a_2, a_3, \cdots \ (a_i \in R)$ 为 R 的一个真因子序列，其中 a_{i+1} 是 a_i 的因子．根据该序列，我们可以得到一个主理想序列 $(a_1), (a_2), (a_3), \cdots$ ．显然 $(a_1) \subset (a_2) \subset (a_3) \cdots$ ．

$$A = \bigcup_{i=1}^{\infty} (a_i)$$

是一个主理想，记为 $A = (d)$．由 $d \in A$ 知，存在 n，$d \in (a_n)$．下证 a_n 一定是真因子序列的最后一个元素．

反证法：由于 $d \in (a_n), a_{n+1} \in (d)$，可以得到 $a_n \mid d, d \mid a_{n+1}$．从而 $a_{n+1} = ca_n$．由真因子序列知 $a_n = c'a_{n+1}$，因而 $a_{n+1} = cc'a_n$．由整数环的消去律知 $cc' = 1$．从而知 a_{n+1} 是 a_n 的相伴元，与 a_{n+1} 是 a_n 的真因子的假定矛盾．所以主理想整环的任意真因子序列仅含有限项．

下证任两个元素的最大公因子存在．

设 $a, b \in R$，命

$$B = \{ar + bs \mid r, s \in R\},$$

则 B 是 R 的一个理想，但 R 是主理想整环，故存在 $d \in R, B = (d)$．由于

$$a = a \cdot 1 + b \cdot 0, \quad b = a \cdot 0 + b \cdot 1,$$

故 $(d) \supseteq (a), (d) \supseteq (b)$．即 $d \mid a, d \mid b$．假定 $c \mid a, c \mid b$，则 $(c) \supseteq (a), (c) \supseteq (b) \Rightarrow (c)$ 含有所有形如 $ar + bs$ 的元素 $\Rightarrow (c) \supseteq (d)$，从而 $c \mid d$，即 $d = (a, b)$．得证．

例 1 整数环是一个主理想环，因而是一个唯一分解环．

证明 设 A 是整数环 Z 中任一理想，若 A 中所有元素的最大公因子为 1，1 可以表示成有 A 中一些元素的线性组合，则由理想的定义，$1 \in A$，从而 $A = Z = (1)$．

若 A 中所有元有最大公因子 $d > 1$，于是 A 中所有元都可写成 rd $(r \in Z)$ 的形式，于是 $A = (d)$．所以 Z 是主理想环．进而由定理 1 知，Z 是唯一分解环．

例 1 的讨论很容易扩展到一元多项式环 $F[x]$ 上．设 A 是 $F[x]$ 的任一理想，$f(x)$，$g(x)$ 是 A 中任两个多项式，它们互素则有

$$a(x) f(x) + b(x) g(x) = 1,$$

从而 $A = (1)$，否则 $A = (r(x))$，$r(x)$ 是 A 中所有元的最大公因式．从而 $F[x]$ 也是主理想环．当然也是唯一分解环．

下面我们要介绍第二种唯一分解环--欧氏环．

定义 2 给定一个整环 R，如果

(1) 存在一个映射

$$\phi: \ R^* \to N,$$

N 为所有的非负整数集合；

(2) 任意 $a \in R^*$，对任何的 $b \in R$，存在 $q, r \in R$ 满足：

$$b = qa + r,$$

其中 $r = 0$ 或是 $\phi(r) < \phi(a)$．

关于欧氏环，由以下结论：

定理 2 如果整环 R 为欧氏环，则 R 一定是一个主理想整环，从而是一个唯一分解整环.

证明 设 A 是 R 的一个理想，现在证明 A 为主理想.

若是 A 只包含零元，那么 A 是一个主理想. 假定 A 包含不等干零的元. 由欧氏环的定义，存在一个映射 ϕ，在这个映射之下 A 的每一个不等于零的元 x 有一个象 $\phi(x)$. 则集合

$$\{\phi(x) \mid \phi(x) > 0, x \in A\}$$

存在最小元，记为 $\phi(x_0)$， $x_0 \in A$. 下证 $A = (x_0)$. 显然 $(x_0) \subseteq A$，只要证明 $A \subseteq (x_0)$ 即可. 由于 R 为欧氏环，任给 $a \in A$，存在 $q, r \in R$ 满足

$$a = qx_0 + r,$$

其中 $r = 0$ 或是 $\phi(r) < \phi(x_0)$. 由于 $r \in A$ 及 $\phi(x_0)$ 的最小性知 $r = 0$，所以 $a \in (x_0)$，从而 $A \subseteq (x_0)$. 得证.

例 2 域 F 上的一元多项式环 $F[x]$ 是一个欧氏环.

证明 利用多项式的次数我们显然可以规定一个合于条件(1)的映射，就是

$$\phi: \quad f(x) \to f(x) \text{的次数}$$

假定 $g(x) \in F[x]$， $g(x) \neq 0$，那么 $g(x)$ 的最高系数 $a_n \neq 0$. 但 a_n 属于域 F，域的每一个不等于零的元都是一个单位，容易证明：任意的 $f(x) \in F[x]$，存在 $r(x) \in F[x]$ 使得

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

其中 $r(x) = 0$ 或是 $r(x)$ 的次数 $< g(x)$ 的次数. 所以 $F[x]$ 是一个欧氏环是一个欧氏环.

例 3 高斯整数环 R 是欧氏环.

证明 任取 $\alpha \in R^*$， $\alpha = a + bi$. 令

$$\phi: \quad \alpha \mapsto a^2 + b^2,$$

则 v 是 R^* 到非负整数集 N 的映射，下面证明 ϕ 适合条件（2).

对任意的 $\alpha = a + bi$， $\beta = c + di$， $\alpha \in R^*$， $\beta \in R$；由于

$$\phi(\alpha)=a^2+b^2.$$

实际上就是α的模，所以对任意$\alpha\neq 0$，$\phi(\alpha)$恒为正实数，并且满足

$$\phi(\alpha\beta)=\phi(\alpha)\phi(\beta).$$

其次，令$\alpha^{-1}\beta=k+li$，k,l是有理数，取k',l'分别为与k,l最接近的整数，于是有

$$|k-k'|\leq\frac{1}{2},\quad |l-l'|\leq\frac{1}{2}.$$

令$\gamma=k'+l'i$，则

$$\phi(\alpha^{-1}\beta-\gamma)=(k-k')^2+(l-l')^2\leq\frac{1}{4}+\frac{1}{4}=\frac{1}{2}.$$

再令$\delta=\beta-\alpha\gamma$，则$\gamma,\delta\in R$，且$\beta=\alpha\gamma+\delta$，这里若有$\delta\neq 0$，则

$$\phi(\delta)=\phi(\beta-\alpha\gamma)=\phi(\alpha(\alpha^{-1}\beta-\gamma))=\phi(\alpha)\phi(\alpha^{-1}\beta-\gamma)\leq\frac{1}{2}\phi(\alpha)<\phi(\alpha).$$

满足欧氏环定义的第2个条件．得证．

§4　唯一分解整环上的多项式环

从上一节的内容，我们已经知道域上的一元多项式环为唯一分解整环．下面我们考虑更一般形势的多项式环：唯一分解整环R上的多项式环$R[x_1,x_2,....x_n]$．本节的主要目的是要证明多项式环$R[x_1,x_2,....x_n]$是唯一分解整环．我们只要证明主理想环R上的一元多项式环$R[x]$为唯一分解整环．那么可以很容易地推广到多元多项式环．

按多项式因子分解中的习惯称呼，我们将素元称为素多项式，既约元称为不可约多项式或既约多项式，有真因子的多项式叫做可约多项式．

现在我们讨论唯一分解整环R上的一元多项式环$R[x]$的唯一分解性．

首先给出一个相关的定义：

定义1　$R[x]$的一个元$f(x)$叫做一个本原多项式，假如$f(x)$的系数的最大公因子是单位．

首先我们有以下简单结论：

性质 1　任给$f(x)\in R[x]$，R的单位是$R[x]$的仅有的单位．

性质 2　与本原多项式相伴的多项式为本原多项式．

性质 3 一个本原多项式不会等于零.

性质 4 任给 $f(x)\in R[x]$，$f(x)=df_1(x)$，其中 $d\in R$，$f_1(x)$ 为本原多项式. 在相伴的意义下，表示唯一.

性质 1–4 的证明留作习题.

引理 1 假定 $f(x)=g(x)h(x)$，那么 $f(x)$ 是本原多项式，当而且只当 $g(x)$ 和 $h(x)$ 都是本原多项式.

证明 若 $f(x)$ 是本原多项式，显然 $g(x)$ 和 $h(x)$ 也都是本原多项式

现在假定

$$g(x)=a_0+a_1x+\cdots,\qquad h(x)=b_0+b_1x+\cdots$$

是两个本原多项式. 如果

$$f(x)=g(x)h(x)=c_0+c_1x+\cdots$$

不是本原多项式，那么 $c_0,c_1,\cdots$ 有一个最大公因子 d，d 不是 R 的单位. 由于 $g(x)\neq 0$，$h(x)\neq 0$，因而 $f(x)\neq 0$，$d\neq 0$. 这样由于 R 是唯一分解环，有一个 R 的素元 p 可以整除 d，因而可以整除每一个 c_k. 由 $g(x)$ 和 $h(x)$ 是本原多项式知 p 不能整除所有的 a_i，也不能整除所有的 b_j. 假定 a_r 和 b_s 分别是 $g(x)$ 和 $h(x)$ 的第一个不能被 p 整除的系数. $f(x)$ 的系数 c_{r+s} 可以写成以下形式

$$c_{r+s}=a_rb_s+a_{r+1}b_{s-1}+a_{r+2}b_{s-2}+\cdots$$

显然 $p\mid a_rb_s$，从而有 $p\mid a_r$ 或 $p\mid b_s$，与这两个元的取法矛盾. 得证.

令 $Q[x]$ 表示 R 的商域 Q 上的一元多项式环，$Q[x]$ 是唯一分解整环. $R[x]$ 为 $Q[x]$ 的一个子环.

引理 2 $Q[x]$ 的每一个不等于零的多项式 $f(x)$ 都可以写成

$$f(x)=\frac{a}{b}f_0(x),$$

其中 $a,b\in R$，$f_0(x)$ 是 $R[x]$ 的本原多项式. 若 $g_0(x)$ 也有 $f_0(x)$ 的性质，那么 $g_0(x)=\varepsilon f_0(x)$（$\varepsilon$ 是 R 的单位）.

证明 Q 的元都可以写成 $\frac{b}{a}(a,b\in R,a\neq 0)$ 的样子， 因此

$$f(x)=\frac{b_0}{a_0}+\frac{b_1}{a_1}x+\cdots+\frac{b_n}{a_n}x^n,\quad (a_i,b_i\in R).$$

令 $a=a_0a_1\cdots a_n$， 那么

$$f(x)=\frac{1}{a}(c_0+c_1+\cdots+c_nx^n),\quad (c_i\in R).$$

令 b 是 $c_0,c_1,\cdots,c_n$ 的一个最大公因子，那么

$$f(x)=\frac{b}{a}f_0(x),$$

$f_0(x)$ 是本原多项式.

另一方面，若

$$f(x)=\frac{d}{c}g_0(x),$$

$c,d\in I$, $g_0(x)$ 是 $R(x)$ 的本原多项式．那么

$$h(x)=bcf_0(x)=adg_0(x)$$

是 $R(x)$ 的一个多项式．由于 $f_0(x)$ 和 $g_0(x)$ 都是本原多项式， bc 和 ad 都是 $h(x)$ 的系数的最大公因子，因而 $bc=\varepsilon ad$（ε 是 R 的单位）．所以 $\varepsilon f_0(x)=g_0(x)$.

引理 3 $R(x)$ 的一个本原多项式 $f_0(x)$ 在 $R(x)$ 里可约的充分而且必要条件是 $f_0(x)$ 在 $Q[x]$ 里可约.

证明 必要性显然成立.

充分性：假定 $f_0(x)$ 在 $Q[x]$ 里可约．所以存在次数 ≥ 1 的多项式 $g(x),h(x)\in Q[x]$

$$f_0(x)=g(x)h(x)$$

$$f_0(x)=\frac{b}{a}g_0(x)\frac{b'}{a'}h_0(x)=\frac{b}{a}\frac{b'}{a'}g_0(x)h_0(x)$$

$a,b,a',b'\in R$， $g_0(x)$ 和 $h_0(x)$ 都是 $R(x)$ 的本原多项式．由引理 1 $g_0(x)h_0(x)$ 还是本原多项式．由引理

$$2\,f_0(x)=\varepsilon g_0(x)h_0(x)\text{（}\varepsilon\text{是}I\text{的单位）.}$$

因此 $\varepsilon g_0(x),h_0(x)\in R[x]$．所以 $f_0(x)$ 在 $R[x]$ 里可约．证完．

引理4 $R(x)$ 的一个次数大于零的本原多项式 $f_0(x)$ 在 $R(x)$ 里有唯一分解．

证明 首先证明既约分解存在．

若是 $f_0(x)$ 本身不可约，显然成立．假定 $f_0(x)$ 可约，且 $f_0(x)$ 的次数为 n，下用归纳法证明．

$n=1$时，结论显然成立；

假设 $n\le m$，结论也成立；

当 $n=m+1$ 时，由 $f_0(x)$ 可约及引理 1 知，存在次数 $\le m$ 的本原多项式 $g_0(x),h_0(x)\in R[x]$，满足

$$f_0(x)=g_0(x)h_0(x)\,.$$

由归纳假设知 $g_0(x)$、$h_0(x)$ 可以分解成既约多项式的乘积．所以 $f_0(x)$ 的既约分解存在．

唯一性：假定 $f_0(x)$ 有两种既约分解

$$f_0(x)=q_1(x)q_2(x)\cdots q_s(x)=p_1(x)p_2(x)\cdots p_t(x)\qquad(1)$$

其中 $q_i(x),p_j(x)\in R[x],1\le i\le s,1\le j\le t$．由引理 1 及引理3知，$q_i(x),\ p_j(x)$ 在 $Q[x]$ 里既约．由 $Q[x]$ 唯一分解性知，$s=t$ 且通过调整顺序，

$$q_0^{(i)}(x)=\frac{b_i}{a_i}p_0^{(i)}(x)\text{，（}a_i,b_i\in R\text{）.}$$

由引理 2 知

$$q_0^{(i)}(x)=\varepsilon_i p_0^{(i)}(x)\text{（}\varepsilon\text{是}R\text{的单位）.}$$

得证．

现在我们可以证明

定理1 若 R 是唯一分解环，那么 $R(x)$ 也是唯一分解整环．

证明（1） $f(x)$ 为次数为 0，则 $f(x)\in R$，由 R 是唯一分解环知 $f(x)$ 有唯一分解．

（2）若 $f(x)$ 为次数为 ≥ 1，则

$$f(x)=df_0(x)，\ d\in R，$$

$f_0(x)$ 是本原多项式．由 R 的唯一分解性，知 d 有唯一分解

$$d=p_0p_2\cdots p_{m-1}\quad（\ p_i\ 是\ R\ 的素元）.$$

由引理 4 知 $f_0(x)$ 有唯一分解

$$f_0(x)=p_0(x)p_1(x)\cdots p_{r-1}(x).$$

所以 $f(x)$ 在 $R(x)$ 里有既约分解

$$f(x)=p_0p_1\cdots p_{m-1}p_0(x)p_1(x)\cdots p_{r-1}(x).$$

假定 $f(x)$ 在 $R(x)$ 里有另一种既约分解

$$f(x)=q_0q_1\cdots q_{n-1}q_0(x)q_1(x)\cdots q_{t-1}(x).$$

则由引理 1 知，

$$q_0(x)q_1(x)\cdots q_{t-1}(x)、\ p_0(x)p_1(x)\cdots p_{r-1}(x)$$

为在 $R(x)$ 相伴的本原多项式，且由引理 3 知 $q_i(x)$、$p_i(x)$ 在 $Q(x)$ 中既约，由 $Q(x)$ 的单一分解性，通过调整顺序，$t=r$，$q_i(x),\ p_i(x)$ 在 $Q(x)$ 中相伴，从而在 $R(x)$ 中相伴。同样

$$p_0p_1\cdots p_{m-1}、\ q_0q_1\cdots q_{n-1}$$

相伴，由 R 的唯一分解性，通过调整顺序 $n=m$，且 q_i,p_i 相伴．所以 $f(x)$ 在 $R(x)$ 里的既约分解在相伴的意义下是唯一的.

由定理 1，应用归纳法立刻可以得到

定理 2 若 R 是唯一分解整环，那么 $R[x_1,x_2,\cdots,x_n]$ 也是唯一分解整环，$x_1,x_2,\cdots,x_n$ 是 R 上的无关未定元.

应注意的是， 由第 4 节的内容知一个欧氏环一定是一个主理想环，一个主理想环一定是一个唯一分解环．但是反过来一个唯一分解环未必是一个主理想环，一个主理想环也未必是一个欧氏环．下面我们就给出一个唯一分解环不是一个主理想环的例子．

例 域 F 上不定元 x, y 的多项式环 $F[x, y]$ 是唯一分解环，但却不是主理想环.

证明 由定理 2 知， $F[x, y]$ 是唯一分解环.

考虑 $F[x, y]$ 中一切常数项为零的所有多项式作成的集合 A，易证， A 是 $F[x, y]$ 的一个理想. 假定 A 是主理想，则必存在 $f \in F[x, y]$， $A = (f)$. 但 $A \supseteq (x)$， $A \supseteq (y)$，故 $f \mid x$， $f \mid y$，而 x, y 的公因子只有 $F[x, y]$ 中的单位，所以有 f 是 $F[x, y]$ 的单位. 由此推出 $A = F[x, y]$，矛盾. 这表明 A 不是主理想.

习题

1．我们看以下的整环 R， R 刚好包含所有可以写成

$$\frac{m}{2^n}$$（m 是任意整数， $n \geq 0$ 的整数）

形式的有理数. R 的哪些个元是单位，哪些个元是素元？

2. R 是刚好包含所有复数

$$a + bi$$（a, b 是整数）

的整环. 证明：5 不是 R 的素元. 5 有没有唯一分解？

3．设 z 是高斯整数环的既约元，证明： z 能且仅能除尽一个素（自然）数 p.

4．找出高斯整数环的所有既约元.

5．假定在一个唯一分解环里

$$a_1 = db_1, a_2 = db_2, \cdots, a_n = db_n$$

证明：当而且只当 d 是 $a_1, a_2, \cdots, a_n$ 的最大公因子的时候 $b_1, b_2, \cdots, b_n$ 互素.

6．假定 R 是一个整环， (a) 和 (b) 是 R 的两个主理想. 证明： $(a) = (b)$ 当而且只当 b 是 a 的相伴元的时候.

7．证明：主理想的定义中， R 有单位元的条件是多余的. 即整环 R 的每一理想都是主理想，则 R 有单位元.

（考虑 R 本身，也是一个主理想，设 $R = (a)$ 则 $a = ae$. 由此证明， ε 是 R 的单位元）.

8．证明：一个域一定是一个欧氏环.

9．我们看有理数域 F 上的一元多项式环 $F[x]$．理想

$$(x^2+1,\ x^5+x^3+1)$$

等于怎样的一个主理想？

10．证明：由所有复数 $a+bi$（a,b 是整数）所作成的环是一个欧氏环（取 $\phi(a)=|a|^2$）．

11．设 R 是一切形如

$$\alpha=\sum_{i=1}^{n}a_i 2^{2^{\frac{l_i}{k_i}}}$$

的实数所成集合，此处 a_i 是任意整数，k_i,l_i 是非负整数，$i=1,2,\cdots,n$．证明：$(R,+,\cdot)$ 是一个有单位元1的整域．

12．证明：(1) R 的单位是 $R[x]$ 的仅有的单位；

(2)与本原多项式相伴的多项式为本原多项式；

(3)一个本原多项式不会等于零；

(4)任给 $f(x)\in R[x]$，$f(x)=df_1(x)$，其中 $d\in R$，$f_1(x)$ 为本原多项式．在相伴的意义下，表示唯一．

13．设 R 是单一分解整环，若 $f_1(x),f_2(x)\in R[x]$，$f_1(x)f_2(x)$ 是本原多项式，则 $f_1(x),f_2(x)$ 都是本原多项式．

14．设 $f(x)$ 是 $Z[x]$ 中首项系数为1的多项式，若 $f(x)$ 有有理根 α，则 α 是整数．

15．设 R 是一个有单位元1的整环，证明：$R[x]$ 中首项系数为1的多项式能分解成 $R[x]$ 中既约多项式的乘积．