

# 代数自然数论

孙松茂

(江苏省太仓市立新布厂, 太仓, 215400)

**摘要** 证明了  $Q(\theta)$  中任一代数整数可表示为  $S(\theta)$  中两数之差,  $Q(\theta)$  中任一代数数可表示为  $S(\theta)$  中两数之商。

**主题词** 代数数域; 代数整数; 共轭数; 主整数; 代数自然数; 共轭对数向量

**中图分类号** O156.2

## 1 代数数域中的主整数及代数自然数

设  $Q(\theta)$  是  $n$  次代数数域, 记  $\theta = \theta_1$ , 并以  $\theta_2, \theta_3, \dots, \theta_n$  表示  $\theta$  所适合的  $n$  次整系数既约多项式的其它  $n-1$  个根. 已知  $Q(\theta)$  中的任一数  $\alpha$  可表示为  $\alpha = \alpha(\theta) = a_{n-1}\theta^{n-1} + a_{n-2}\theta^{n-2} + \dots + a_0, a_j \in Q(j=0, 1, \dots, n-1)$ . 定义  $\alpha_i = \alpha(\theta_i) (i=2, 3, \dots, n)$  为  $\alpha = \alpha_1$  的共轭数, 乘积  $\alpha_1\alpha_2\cdots\alpha_n = N(\alpha)$  称为  $\alpha$  的范数. 若  $N(\alpha) = \pm 1$ , 则称  $\alpha$  为单位数<sup>[1]</sup>. 因  $\alpha(\theta_i) + \beta(\theta_i)$  及  $\alpha(\theta_i)\beta(\theta_i) (i=2, 3, \dots, n)$  是  $\alpha(\theta) + \beta(\theta)$  及  $\alpha(\theta)\beta(\theta)$  的共轭数, 有  $(\alpha + \beta)_i = \alpha_i + \beta_i$  及  $(\alpha\beta)_i = \alpha_i\beta_i$ .

**定义 1.1** 设  $\alpha$  是  $Q(\theta)$  中的代数数. 如果  $|\alpha| \geq |\alpha_i| (i=2, 3, \dots, n)$ , 则称  $\alpha$  是  $Q(\theta)$  中的主代数数, 特别当  $\alpha$  是代数整数时, 称  $\alpha$  是  $Q(\theta)$  中的主代数整数, 简称主整数, 它们的全体称为  $Q(\theta)$  中的主整数集, 记作  $S(\theta)$ . 若  $Q(\theta)$  是实域,  $Q(\theta)$  中的非负主整数称为代数自然数, 它们的全体称为  $Q(\theta)$  中的代数自然数集, 记作  $M(\theta)$ .

显然, 每个有理整数都是主整数。

**定义 1.2** 设  $\alpha$  是  $Q(\theta)$  中不等于零的代数数, 称  $n-1$  元实数组  $(\ln|\alpha/\alpha_2|, \ln|\alpha/\alpha_3|, \dots, \ln|\alpha/\alpha_n|)$  为  $\alpha$  的共轭对数向量。

由于  $(\alpha\beta)_i = \alpha_i\beta_i$ , 因此  $\alpha\beta$  的共轭对数向量的各分量应是  $\alpha, \beta$  的共轭对数向量相应分量之和。

据定义 1.1, 主代数数的共轭对数向量的每个分量都不小于零, 反过来说, 共轭对数向量的每个分量都不小于零的代数数必是主代数数. 若代数数  $\alpha$  的共轭对数向量的每个分量都等于零, 则称此代数数为平凡代数数. 显然有理整数都是平凡的主整数。

**定理 1.1** 设  $r$  是任一正实数, 则  $n$  次代数数域  $Q(\theta)$  中绝对值不大于  $r$  的主整数的个数是有限的。

证(略)。

由定理 1.1 可知,  $S(\theta)$  在复平面或实数轴上无聚点, 即它是离散集。

收稿日期: 1995-08-28

规定复数间的顺序法则:绝对值不相等的两复数,以绝对值小者在前;绝对值相等的两复数,以实部大者在前;绝对值相等、实部也相等的两复数,以虚部系数大者在前。

按此法则, $S(\theta)$  或  $M(\theta)$  中的全部数都可排成以  $0, 1, \dots$  开始的有序数列,分别称为  $Q(\theta)$  中的主整数列或代数自然数列,仍用  $S(\theta)$  或  $M(\theta)$  来表示。

**定义 1.3** 设  $S(\theta)$  是  $n$  次代数数域  $Q(\theta)$  中的主整数列, $S(\theta)$  中列于最前的  $n$  次的数称为  $Q(\theta)$  的中心数,中心数所适合的  $n$  次整系数既约多项式称为  $Q(\theta)$  的中心定义多项式。

在  $Q(\theta)$  的每个代数数的共轭对数向量中,若有某个分量总等于零,即有数  $j$  ( $j$  为  $2, 3, \dots, n$  中的一个),对于  $Q(\theta)$  中的任一数  $\alpha_i, |\alpha_i| = |\alpha_j|$  总能成立,容易证明,  $\alpha_i$  与  $\alpha_j$  是一对共轭复数,因而  $\theta_i$  与  $\theta_j$  也是一对共轭复数。 $\theta_2, \theta_3, \dots, \theta_n$  中至多只有一个是  $\theta_1$  的共轭复数,因此  $Q(\theta)$  中代数数的共轭对数向量中至多只有一个分量总等于零,若某代数数域  $Q(\theta)$  中的代数数都是平凡代数数,则它们的共轭对数向量只有一个恒等于零的分量,即  $Q(\theta)$  的次数为 2。事实上,所含代数数都是平凡代数数的平凡代数数域,只有有理数域  $Q$  及  $Q(\sqrt{-m}), m = 1, 2, 3, 5, 6, 7, \dots$ 。它们的代数整数集即是主整数集,由此即得:

**定理 1.2** 平凡代数数域  $Q(\theta)$  中的主整数集  $S(\theta)$  是一个环。

## 2 主整数集中的素数

**定理 2.1**  $S(\theta)$  关于乘法封闭。即若  $\alpha, \beta \in S(\theta)$ , 则  $\alpha\beta \in S(\theta)$ 。

证(略)。

$S(\theta)$  既然对于乘法组成一个半群,当然可以考虑  $S(\theta)$  中的整除性问题。但  $S(\theta)$  中往往含有非 1 的单位数,便会有一些特殊的情况。

若  $S(\theta)$  中最前的非  $\pm 1$  单位数为  $\omega_1$ , 且  $S(\theta)$  中的每个单位数都可表示为  $\pm \omega_1^{m_1}$  ( $m_1 = 0, 1, 2, \dots$ ), 则称  $S(\theta)$  中有一个基元单位数  $\omega_1$ 。若除此之外,  $S(\theta)$  中另有不能如此表示的单位数,记其中在  $S(\theta)$  中最前的一个为  $\omega_2$ , 且  $S(\theta)$  中的单位数都可表示为  $\pm \omega_1^{m_1} \omega_2^{m_2}$  ( $m_1, m_2 = 0, \pm 1, \pm 2, \dots$ ), 则称  $S(\theta)$  中有两个基元单位数  $\omega_1, \omega_2$ 。一般若  $S(\theta)$  中的单位数都可表示为  $\pm \omega_1^{m_1} \omega_2^{m_2} \dots \omega_k^{m_k}$  ( $m_i = 0, \pm 1, \pm 2, \dots, i = 1, 2, \dots, k$ ), 则称  $S(\theta)$  中有  $k$  个基元单位数  $\omega_1, \omega_2, \dots, \omega_k$ 。这时整数  $m_1, m_2, \dots, m_k$  应满足这样的条件,即如果  $\omega_i$  ( $i = 1, 2, \dots, k$ ) 的共轭对数向量为  $(\xi_{i2}, \xi_{i3}, \dots, \xi_{in})$ , 则  $\xi_i = \sum_j m_j \xi_{ij} \geq 0$  ( $j = 2, 3, \dots, n$ ) 不等式成立。

除规定  $S(\theta)$  中的基元单位数为素数之外,还有如下定义。

**定义 2.1** 对于  $S(\theta)$  中的非单位数  $\alpha$ , 若  $S(\theta)$  中有不都是单位数的数  $\beta, \gamma$ , 使得  $\alpha = \beta\gamma$ , 或  $S(\theta)$  中有非  $\pm 1$  单位数  $\omega$  及都不是单位数的数  $\beta, \gamma$ , 使得  $\alpha = \beta\gamma\omega^{-1}$ , 则称  $\alpha$  在  $S(\theta)$  中可分解, 否则称  $\alpha$  为  $S(\theta)$  中的素数。

如果  $S(\theta)$  中的数  $\alpha$  除以某个单位数  $\omega$  所得商不是主整数, 但  $\alpha'\omega^{-t}$  ( $s, t = 1, 2, \dots$ ) 却是主整数, 那么当  $S \rightarrow \infty$  时, 使  $\alpha'\omega^{-t}$  成为主整数的  $t/s$  的上限称为  $\alpha$  中单位数  $\omega$  的含量, 这一数值很容易从  $\alpha$  及  $\omega$  的共轭对数向量算出。

## 3 $S(\theta)$ 在 $Q(\theta)$ 中的地位

**定理 3.1**  $Q(\theta)$  中的任一代数整数  $\alpha$  都可表示为  $S(\theta)$  中两数之差。

**证明** 若  $Q(\theta)$  是平凡代数数域, 由定理 1.2, 本定理成立, 否则先约定, 若  $\theta_i$  是  $\theta$  的共轭复数, 因为  $|\alpha| = |\alpha_i|$  总能成立, 因此在证明中可将  $\alpha_i$  暂且不计. 若  $\alpha$  是主整数, 则  $\alpha = \alpha - 0$ , 本定理成立; 若不记  $f = \max_{i=2,3,\dots,n} (|\alpha| + |\alpha_i|)$ ,  $g = \min_{i=2,3,\dots,n} (|\beta| - |\beta_i|)$ , 根据上述约定,  $Q(\theta)$  中总有一个主整数  $\beta$ , 使得  $g > 0$ . 因此总有一个正整数  $m$ , 使得  $mg - f > 0$ , 这时  $\gamma = m\beta + \alpha$  是  $Q(\theta)$  中的代数整数, 且  $|\gamma| - |\gamma_i| = |m\beta + \alpha| - |m\beta_i + \alpha_i| \geq m|\beta| - |\alpha| - m|\beta_i| - |\alpha_i| = m(|\beta| - |\beta_i|) - (|\alpha| + |\alpha_i|) \geq mg - f > 0$ , ( $i = 2, 3, \dots, n$ ). 因此  $\gamma$  是  $Q(\theta)$  中的主整数,  $\alpha$  是  $S(\theta)$  中两数之差, 即  $\alpha = \gamma - m\beta$ .

**定义 3.1** 设  $\alpha$  是  $Q(\theta)$  中的代数整数,  $\alpha = \beta - \gamma$ ,  $\beta, \gamma \in S(\theta)$ , 在  $\alpha$  的所有这样的表达式中, 数列  $S(\theta)$  中位置最前的  $\gamma = \gamma_0$  称为  $\alpha$  的最小减数,  $\alpha = \beta_0 - \gamma_0$  称为  $\alpha$  的最简差式.

**定理 3.2**  $Q(\theta)$  中的任一代数数都可表示为  $S(\theta)$  中两数之商.

**证明** 已知  $Q(\theta)$  中的代数数  $\alpha$  总可表示为  $\alpha = \tau/t$ ,  $\tau$  是  $Q(\theta)$  中的代数整数,  $t$  是一个正有理整数. 若  $Q(\theta)$  是平凡代数数域,  $\tau$  必是主整数, 定理成立. 否则约定当  $\theta_i$  是  $\theta$  的共轭复数时, 证明中将  $\alpha_i$  暂且不计. 若  $\tau$  是主整数, 定理成立. 否则  $f = \min_{i=2,3,\dots,n} \ln |\tau/\tau_i|$  是负数, 记  $g = \min_{i=2,3,\dots,n} \ln |\beta/\beta_i|$ . 根据上述约定,  $S(\theta)$  中总有主整数  $\beta$ , 使得  $g > 0$ . 因此总有正整数  $m$ , 使得  $mg + f > 0$ . 这时  $\gamma = \beta^m \tau$  是  $Q(\theta)$  中的代数整数, 且它的共轭对数向量的每个分量

$$\ln |\gamma/\gamma_i| = m \ln |\beta/\beta_i| + \ln |\tau/\tau_i| \geq mg + f > 0 \quad (i = 2, 3, \dots, n).$$

因此  $\gamma$  是  $S(\theta)$  中的数,  $\tau$  是两主整数之商, 即  $\tau = \gamma/\beta^m$ , 从而  $\alpha = \gamma/(t\beta^m)$ , 即  $\alpha$  是  $S(\theta)$  中两数之商.

**定义 3.2** 设  $\alpha$  是  $Q(\theta)$  中的代数数,  $\alpha = \beta/\gamma$ ,  $\beta, \gamma \in S(\theta)$ , 在  $\alpha$  的所有这样的表达式中, 在数列  $S(\theta)$  中位置最前的  $\gamma = \gamma_0$  称为  $\alpha$  的最小分母,  $\alpha = \beta_0/\gamma_0$  称为  $\alpha$  的既约分式.

## 4 代数自然数集的性质

前已证明, 当  $Q(\theta)$  是平凡代数数域时, 它的主整数集  $S(\theta)$  关于加法封闭, 非平凡的主整数集  $S(\theta)$  中两数相加便有可能得到非主整数. 但当  $Q(\theta)$  是实域时, 代数自然数集  $M(\theta)$  是  $S(\theta)$  的对加法封闭的子集.

**定理 4.1**  $M(\theta)$  关于加法封闭, 即若  $\alpha, \beta \in M(\theta)$ , 则  $\alpha + \beta \in M(\theta)$ .

证(略).

$M(\theta)$  对乘法也封闭, 定理 3.1, 3.2 对  $M(\theta)$  适用, 只是用  $M(\theta)$  中两数之商表示代数数时, 至多差一个正负号.  $M(\theta)$  中的素数可按定义 2.1 来规定. 另外,  $M(\theta)$  中的数对加法也有素数.

**定义 4.1** 对  $M(\theta)$  中的数  $\alpha$ , 若  $M(\theta)$  中有不等于零的数  $\beta, \gamma$ , 使得  $\alpha = \beta + \gamma$ , 则称  $\alpha$  在  $M(\theta)$  中可分裂, 否则称  $\alpha$  为  $M(\theta)$  中的加法素数.

已知自然数列中仅有一个加法素数 1, 二次代数自然数集  $M(\sqrt{m})$  ( $m = 2, 3, \dots$ ) 中, 当  $m \equiv 2, 3 \pmod{4}$  时, 有 2 个加法素数 1,  $\sqrt{m}$ ; 当  $m \equiv 1 \pmod{4}$  时, 有 3 个加法素数 1,  $(\sqrt{m} + 1)/2$ ,  $\sqrt{m}$ . 其他的代数自然数集多数有无数个加法素数.

**定理 4.2** 设  $\theta$  是  $n$  次整系数既约多项式

$$x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0 \quad (1)$$

的根, 记

$$\theta^n = g_{m,n-1}\theta^{n-1} + g_{m,n-2}\theta^{n-2} + \dots + g_{m,1}\theta + g_{m,0}$$

若极限  $\lim_{m \rightarrow \infty} \frac{g_{m,j}}{g_{m,0}} = hj \quad (j = 1, 2, \dots, n-1)$  存在, 则  $hj = -\frac{1}{a_0}(\theta_1^{n-j} + a_{n-1}\theta_1^{n-j-1} + \dots + a_{j+1}\theta)$ .  $\theta_1$  是(1)的实根, 且有  $|\theta_1| > |\theta_i| \quad (i = 2, 3, \dots, n)$ .

**证明** 由式(1)

$$\begin{aligned}\theta^m &= \theta \cdot \theta^{m-1} = \theta(g_{m-1,n-1}\theta^{n-1} + g_{m-1,n-2}\theta^{n-2} + \dots + g_{m-1,0}) \\ &= (g_{m-1,n-2} - a_{n-1}g_{m-1,n-1})\theta^{n-1} + (g_{m-1,n-3} - a_{n-2}g_{m-1,n-1})\theta^{n-2} \\ &\quad + \dots + (g_{m-1,0} - a_1g_{m-1,n-1})\theta + (-a_0g_{m-1,n-1})\end{aligned}$$

可得

$$\begin{aligned}g_{m,n-1} &= g_{m-1,n-2} - a_{n-1}g_{m-1,n-1} \\ g_{m,n-2} &= g_{m-1,n-3} - a_{n-2}g_{m-1,n-1} \\ \dots \quad \dots \quad \dots \quad \dots \quad \dots \\ g_{m,1} &= g_{m-1,0} - a_1g_{m-1,n-1} \\ g_{m,0} &= -a_0g_{m-1,n-1}\end{aligned} \quad (2)$$

将式(2)的  $m$  换成  $m-1$ , 代入  $g_{m,1}$  得

$$g_{m,1} = -a_1g_{m-1,n-1} - a_0g_{m-2,n-1} \quad (3)$$

再将式(3)的  $m$  换成  $m-1$ , 代入  $g_{m,2}$ , 依次类推, 可得

$$\begin{aligned}g_{m,2} &= -a_2g_{m-1,n-1} - a_1g_{m-2,n-1} - a_0g_{m-3,n-1} \\ \dots \quad \dots \quad \dots \quad \dots \quad \dots \\ g_{m,n-1} &= -a_{n-1}g_{m-1,n-1} - a_{n-2}g_{m-2,n-1} - \dots - a_0g_{m-n,n-1}\end{aligned} \quad (5)$$

将式(5)的  $m$  换成  $m+n-2$ , 所得等式右端最后两项与式(3)的右端相同, 将式(5)中的  $m$  换成  $m+n-3$ , 所得等式右端最后三项与式(4)的右端相同  $\dots$  等. 将上述结果一一代入(3), (4),  $\dots$  各等式的右端, 即得

$$\begin{aligned}g_{m,1} &= g_{m+n-2,n-1} + a_{n-1}g_{m+n-3,n-1} + \dots + a_2g_{m,n-1} \\ g_{m,2} &= g_{m+n-3,n-1} + a_{n-1}g_{m+n-4,n-1} + \dots + a_3g_{m,n-1} \\ \dots \quad \dots \quad \dots \quad \dots \quad \dots \\ g_{m,n-2} &= g_{m+1,n-1} + a_{n-1}g_{m,n-1} \\ g_{m,n-1} &= g_{m,n-1}\end{aligned}$$

式(5)实际上是数列  $g_{0,n-1}, g_{1,n-1}, \dots, g_{m,n-1}, \dots$  的递推式, 据[2], 多项式(1)是这一数列的特征方程, 因此  $g_{m,n-1}$  的通项为

$$g_{m,n-1} = C_1\theta_1^{m-1} + C_2\theta_2^{m-1} + \dots + C_n\theta_n^{m-1}$$

$\theta_1, \theta_2, \dots, \theta_n$  是(1)的  $n$  个根,  $C_1, C_2, \dots, C_n$  是待定常数。

由于  $\theta_1, \theta_2, \dots, \theta_n$  也都是常数, 因此该式也可写成

$$g_{m,n-1} = C_1\theta_1^m + C_2\theta_2^m + \dots + C_n\theta_n^m \quad (6)$$

已知  $g_{0,n-1} = g_{1,n-1} = \dots = g_{n-2,n-1} = 0, g_{n-1,n-1} = 1$  代入式(6), 得到线性方程组

$$\begin{aligned}C_1 + C_2 + \dots + C_n &= 0 \\ C_1\theta_1 + C_2\theta_2 + \dots + C_n\theta_n &= 0 \\ C_1\theta_1^2 + C_2\theta_2^2 + \dots + C_n\theta_n^2 &= 0 \\ \dots \quad \dots \quad \dots \quad \dots \quad \dots \\ C_1\theta_1^{n-1} + C_2\theta_2^{n-1} + \dots + C_n\theta_n^{n-1} &= 1\end{aligned}$$

方程组的系数行列式为 Vandermonde 行列式  $V = (\theta_2 - \theta_1)(\theta_3 - \theta_1)\dots(\theta_n - \theta_{n-1})$ . 由于(1)

是既约多项式,  $\theta_1, \theta_2, \dots, \theta_n$  两两不相等, 从而  $V \neq 0$ . 同理, 由该行列式前  $n-1$  行组成的  $n$  个子行列式也都是不等于零的 Vandermonde 行列式. 由此可知, 从线性方程组解出的  $C_1, C_2, \dots, C_n$  都不等于零.

设在  $\theta_1, \theta_2, \dots, \theta_n$  中, 绝对值最大的为  $\theta_1$ . 如为实数, 则有  $|\theta_1| > |\theta_i|, (i = 2, 3, \dots, n)$ , 且  $|\theta_1| > 1$ . 当  $m \rightarrow \infty$  时, 有  $|C_1 \theta_1^m| \gg |\sum C_i \theta_i^m| (i = 2, 3, \dots, n)$ . 因此当  $m$  足够大时, 可认为  $g_{m,n-1} = C_1 \theta_1^m$ . 将此结果用于  $g_{m,1}, g_{m,2}, \dots, g_{m,n-1}$  各表达式及式(2), 可得

$$\begin{aligned} g_{m,n-1} &= C_1 \theta_1^m \\ g_{m,n-2} &= C_1 \theta_1^{m+1} + a_{n-1} C_1 \theta_1^m \\ &\dots \dots \dots \dots \dots \\ g_{m,2} &= C_1 \theta_1^{m+n-3} + a_{n-1} C_1 \theta_1^{m+n-4} + \dots + a_3 C_1 \theta_1^m \\ g_{m,1} &= C_1 \theta_1^{m+n-2} + a_{n-1} C_1 \theta_1^{m+n-3} + \dots + a_2 C_1 \theta_1^m \\ g_{m,0} &= -a_0 C_1 \theta_1^{m-1} \end{aligned}$$

将上列各式的两端都除以最后一式两端, 由于  $C_1 \neq 0$ , 即得

$$hj = \lim_{m \rightarrow \infty} \frac{g_{m,j}}{g_{m,0}} = -\frac{1}{a} (\theta_1^{n-j} + a_{n-1} \theta_1^{n-j-1} + \dots + a_{j+1} \theta_1) \quad (j = 1, 2, \dots, n-1)$$

如果  $\theta_1$  是虚数, 则  $|\theta_1| = |\theta_2| \geq |\theta_i|, (i = 3, 4, \dots, n)$ . 若有  $|\theta_1| = |\theta_2| > |\theta_i|$ , 则当  $m$  足够大时, 可认为  $g_{m,n-1} = C_1 \theta_1^m + C_2 \theta_2^m$ . 易知,  $C_1$  与  $C_2$  是一对共轭复数,  $C_1 \theta_1^m$  与  $C_2 \theta_2^m$  也是一对共轭复数, 它们的和是实部之和, 即  $g_{m,n-1} = 2R(C_1 \theta_1^m)$ . 代入式(2), 得  $g_{m,0} = -2a_0 R(C_1 \theta_1^{m-1})$ . 这时

$$g_{m,n-1}/g_{m,0} = -R(C_1 \theta_1^m)/[a_0 R(C_1 \theta_1^{m-1})]$$

当  $m \rightarrow \infty$  时, 这一比式不可能趋近于某一实数.

从定理 4.2 可知  $M(\theta)$  中的  $n$  次数经多次相乘后, 所得的积中,  $\theta^{n-1}, \theta^{n-2}, \dots, \theta, 1$  的系数之比趋于同一比值, 这称为代数自然数的自然趋同现象.

# 参 考 文 献

- 柯 召, 孙 琦. 数论讲义(下). 高等教育出版社, 1987
- 谢力之等. 数列递推式. 电子工业出版社, 1987

## Algebraic Theory of Natural Numbers

Sun Songmao

(Lixin Cloth Factory, Taicang, Jiangsu, 215400)

**Abstract** In this paper, we prove any algebraic integral number of  $Q(\theta)$  can be expressed as the difference of two numbers of  $S(\theta)$ , and any algebraic number of  $Q(\theta)$  can be expressed as the quotient of two numbers of  $S(\theta)$ .

**Subject-words** Algebraic number field; Algebraic integral number; Conjugate number; Subject integral number; Algebraic natural number; Conjugate logarithmic vector