决定二类代数整数环 $Z[\sqrt{d}]$ 与 $Z[\sqrt[3]{d}]$ 的所有素元

赵嗣元

一、概　　述

"决定一个非零(交换)整环的 I 的所有素元"是《近世代数》中因子分解理论的中心课题之一(若再能决定 I 的所有不可约元，通过比较就可判定 I 是不是唯一分解环[1])，也是《代数数论》里研究代数整数环的课题之一[2]．我们想对二项扩张的代数整数环 $I=\boldsymbol{Z}[\sqrt[n]{d}]$ 解决这个问题，其中 $\boldsymbol{Z}$ 是有理整数环，n 是大于 1 的自然数，$\boldsymbol{Z}\ni d\neq 0, 1$ 且无 n 次真因子，当 n 为奇数时，还要求 $d\neq -1$．

素元的定义是：非零整环 I 里一个不是单位的非零元 α 之使"$\alpha|\beta\gamma\Longrightarrow\alpha|\beta$ 或 $\alpha|\gamma$"者叫作 I 的一个素元．

判别素元的准则[3]有：$I\ni\alpha$ 是素元 $\Longleftrightarrow I$ 的主理想 (α) 是真的素理想 $\Longleftrightarrow$ 剩余类环 $I/(\alpha)$ 是与 I 不同构的非零整环．

这些准则用起来并不方便，对具体的整环 $I=\boldsymbol{Z}[\sqrt[n]{d}]$ 应可依据其具体特征来给出较为简便(或许是大为简便)的准则，它的具体特征是在其中可引入乘性的范数函数 $N(\alpha)$，以及坐标的 $g.c.d.$ 函数 d_α．

一般在《代数数论》中已经证明在有理数域 $\boldsymbol{Q}$ 上有一个有限代数扩张里全体代数整数组成的环 I 对非零主理想 (α) 的剩余类恰有 $N(\alpha)$ 个[2]．于是 $I/(\alpha)$ 是与 I 不同构的非零整环 $\Longleftrightarrow$ $I/(\alpha)$ 是有 $N(\alpha)$ 个元的有限域 $\Longrightarrow N(\alpha)$ 是一个素数的幂．

但 $N(\alpha)$ 是一个素数的幂不足以保证 $I/(\alpha)$ 是域，从而不足以保证 α 是 I 的素元，这是因为素数幂阶的有限环可能含有零因子．因此还得有办法弄清 $I/(\alpha)$ 的结构．

笔者在教学工作中对 $n=2$ 的情形摸索到一个确定 $\boldsymbol{Z}[\sqrt{d}]/(\alpha)$ 的结构之一初等方法[4]．从而能用 $N(\alpha)$ 与 d_α 来判定 α 是不是素元，所得的结果是简洁的．

定理 1　$\boldsymbol{Z}[\sqrt{d}]$ 的元 $\alpha=a_0+a_1\sqrt{d}$ 是一个素元的充要条件

或者(1)　$N(\alpha)>1=d_\alpha$　是一个素数

或者(2)　$d_\alpha>1=N\left(\dfrac{\alpha}{d_\alpha}\right)$ 是一个奇素数，它使得

$(d_\alpha, d)=1$ 且 d 是模 d_α 之一平方非剩余．

(即 $d^{\frac{p-1}{2}}\equiv -1 \pmod{d_\alpha}$ 此时 $N(\alpha)=d_\alpha^2$ 是素数平方)．

证明中关键性的一步是确定 (α) 内元素形式时从方程组过渡到等价的同余组这一步[4,5]．向 $n>2$ 的推广并不顺利，把同余组化为等价的主对角线上是 1 的高三角形同余组的整

本文于 1984 年 10 月 4 日收到．

数可逆矩阵C的作法又成了一大难关，引进了整化因子与拟本原化等概念之后，仅在$n=3$的情形巧妙地（也可以说是巧合地）构造出了C。这才获得了

定理 2　$\boldsymbol{Z}[\sqrt[3]{d}]$的元$\alpha=a_0+a_1\sqrt[3]{d}+a_2\sqrt[3]{d^2}$是一个素元当且仅当下列互斥的四个条件有且只有一个成立：

(i) $N(\alpha)=d_\alpha^3$，d_α是与d互素的奇素数且d是 mod d_α的一个立方非剩余。

(ii) 素数 $N(\alpha)=d_{\tilde{\tilde{\alpha}}}>d_\alpha=d_{\tilde{\alpha}}=1$。(其中$\bar{\alpha}$为使$\alpha=\bar{\alpha}d_\alpha$者叫作$\alpha$的拟本原化，而$\tilde{\alpha}$为使$|\alpha\tilde{\alpha}|=N(\alpha)$者叫作$\alpha$的标准整化因子)。

(iii)　$N(\alpha)=d_{\tilde{\alpha}}^2$，$d_{\tilde{\alpha}}>d_\alpha=d_{\tilde{\alpha}}=1$为一奇素数，且使由$\alpha$确定的整数$4(b_1b_3+b_2)+b_3^2$*是模$d_{\bar{\alpha}}$之一平方非剩余。

(iv)　$N(\alpha)=d_{\tilde{\alpha}}^2=4$，$d_\alpha=d_{\tilde{\alpha}}=1$，且$2\nmid b_3$而$b_1\not\equiv b_2 \pmod 2$。

近日与袁波同学共同研究时，发现此法有局限性，在向$n>3$的一般情形推广时尚有难以攻克的难关，有待于新的突破，所以说上述C之作出，实为巧合，似乎有些侥倖。

二、关于 $Z[\sqrt[n]{d}]$ 的基本事实和符号

1. 正则表示的矩阵

$I=\boldsymbol{Z}[\sqrt[n]{d}]$是$\boldsymbol{Z}$上交换(结合)代数，其承载$\boldsymbol{Z}$-模是具有基$\{1,\theta=\sqrt[n]{d},\theta^2,\cdots,\theta^{n-1}\}$的$n$-秩自由$\boldsymbol{Z}$-模。它是环$I$的正则表示[6] $\rho:\alpha\longrightarrow\alpha_l=\alpha_r$的表示模$\alpha_l$表$\boldsymbol{Z}$模$I$上用$\alpha$左乘的$\boldsymbol{Z}$-同态：$x\longrightarrow\alpha x\quad(x\in I)$

因I有单位元 1，故正则表示ρ是切实的，即$ker\,\rho=0$，亦即$I\ni\alpha=0\Longleftrightarrow\rho(\alpha)=0$

在取定基$\{1,\theta,\theta^2,\cdots,\theta^{n-1}\}$时，$\rho$等价于矩阵表示$M$：$\alpha\longrightarrow M(\alpha)\in Mn(\boldsymbol{Z})$之使

$$(\rho(\alpha)\cdot 1,\ \rho(\alpha)\theta,\ \cdots,\ \rho(\alpha)\theta^{n-1})=(1,\ \theta,\ \cdots,\ \theta^{n-1})M(\alpha)$$

者。上式即

$$\alpha(1,\ \theta,\ \cdots,\ \theta^{n-1})=(\alpha\cdot 1,\ \alpha\cdot\theta,\ \cdots,\ \alpha\theta^{n-1})=(1,\ \theta,\ \cdots,\theta^{n-1})M(\alpha) \tag{1}$$

由此易见：若$\alpha=a_0+a_1\theta+\cdots+a_{n-1}\theta^{n-1}$则

$$M(\alpha)=\begin{pmatrix} a_0 & da_{n-1} & da_{n-2}\cdots da_2 & da_1 \\ a_1 & a_0 & da_{n-1}\cdots da_3 & da_2 \\ a_2 & a_1 & a_0\ \vdots\ \cdots da_4 & da_3 \\ \vdots & \vdots & \vdots\quad\cdots & \vdots \\ a_{n-2} & a_{n-3} & a_{n-4}\ \cdots a_0 & da_{n-1} \\ a_{n-1} & a_{n-2} & a_{n-3}\ \cdots a_1 & a_0 \end{pmatrix} \tag{2}$$

特别对$m\in\boldsymbol{Z}$ 有 $M(m)=dieg\{m,\ m\cdots,\ m\}=mE_n$，$E_n$，表$n$阶单位矩阵。

矩阵表示M也是切实的，这是因为它与ρ等价故有 $I\ni\alpha=0\Longleftrightarrow M(\alpha)=0$

由于ρ与M都是$\boldsymbol{Z}$-代数的单一同态，所以都保持乘法，从而对$\forall\alpha,\beta\in I$ 有 $M(\alpha\beta)=M(\alpha)M(\beta)$。

2. 范数

记$det\,M(\alpha)=D(\alpha)$ 而称$|D(\alpha)|=N(\alpha)$为α的范数，则显有

---

* b_1,b_2,b_3 的定义见后文(α)的元素形式一节。

系 1 对 $\forall\alpha\in I$, $0\leqslant N(\alpha)\subset \boldsymbol{Z}$, 又 $N(0)=0$

系 2 对 $\forall\alpha,\beta\in I$, $N(\alpha\beta)=N(\alpha)N(\beta)$. (3)

系 3 $I\ni\varepsilon$ 是一个单位 $\Longleftrightarrow N(\varepsilon)=1$

系 4 对 $\forall\alpha\in I$, $m\in\boldsymbol{Z}$, 有 $D(m\alpha)=m^nD(\alpha)$, $\therefore D(m)=m^n$. (4)

3.拟本原化

对 I 的任一元 $\alpha=a_0+a_1\theta+\cdots+a_{n-1}\theta^{n-1}$, 记 $d_\alpha=(a_0, a_1, \cdots, a_{n-1})$, 它就是 α 的坐标的 $.c.d$. 于是可写 $a_i=\bar{a}_i d_\alpha$, $(i=0, 1, \cdots, n-1)$, 及 $\alpha=\bar{\alpha}\,d_\alpha$, 其中 $\bar{\alpha}=\bar{a}_0+\bar{a}_1\theta+\cdots+\bar{a}_{n-1}\theta^{n-1}$ 叫作 α **的拟本原化**.* 显有 $d_{\bar{\alpha}}=1$, 当 $m\in\boldsymbol{Z}$ 时 $d_m=m$, $\overline{m}=1$ 以及

$$D(\alpha)=d_\alpha^n D(\bar{\alpha}),\quad M(\alpha)=d_\alpha M(\bar{\alpha}) \tag{5}$$

4.整化因子

I 的任一元 $\alpha=a_0+a_1\theta+\cdots+a_{n-1}\theta^{n-1}$ 可表为长方阵乘积的形式:

$$\alpha=(1,\theta,\cdots,\theta^{n-1})\begin{pmatrix}a_0\\a_1\\\vdots\\a_{n-1}\end{pmatrix}$$

则利用 (1) 式可表 I 中乘法如下: 又若 $\beta=\sum_{i=0}^{n-1}b_i\theta^i\in I$, 则

$$\alpha\beta=\alpha(1,\theta,\cdots,\theta^{n-1})\begin{pmatrix}b_0\\b_1\\\vdots\\b_{n-1}\end{pmatrix}=(1,\theta,\cdots,\theta^{n-1})M(\alpha)\begin{pmatrix}b_0\\b_1\\\vdots\\b_{n-1}\end{pmatrix}$$

就是积 $\alpha\beta$ 的坐标列是

$$M(\alpha)\begin{pmatrix}b_0\\b_1\\\vdots\\b_{n-1}\end{pmatrix}$$

若取 $b_i=D_{1,i+1}(\alpha)$ 为行列式 $D(\alpha)$ 第一行第 i 列位置的代数余子式, $(i=0, 1, 2, \cdots, n-1)$ 而记 $\beta=\tilde{\alpha}$ 则

$$\alpha\tilde{\alpha}=(1,\theta,\cdots,\theta^{n-1})M(\alpha)\begin{pmatrix}D_{11}(\alpha)\\D_{12}(\alpha)\\\vdots\\D_{1n}(\alpha)\end{pmatrix}=(1,\theta,\cdots,\theta^{n-1})\begin{pmatrix}D(\alpha)\\0\\\vdots\\0\end{pmatrix}=D(\alpha)\in\boldsymbol{Z}$$

故称 $\tilde{\alpha}$ 为 α 的**标准整化因子**. 为了简化符号写成 $D_{1,i+1}(\alpha)=\tilde{\alpha}_i=\overline{\tilde{\alpha}}_i d_{\tilde{\alpha}}$. $\overline{\tilde{\alpha}}=\sum_{i=0}^{n-1}\overline{\tilde{\alpha}}_i\theta^i$ 是 $\tilde{\alpha}=\sum_{i=0}^{n-1}\tilde{\alpha}_i\theta^i$ 的拟本原化.

显然, 对 $\forall m\in\boldsymbol{Z}$, $m\overline{\tilde{\alpha}}$ 都是 α 的整化因子, 乃称 $\overline{\tilde{\alpha}}$ 为 α 的**拟本原整化因子**. 可证: 它是 α 的范数最小的整化因子. 为此先要证下之

* 前缀"拟"字是鉴于 θ 不是 $\boldsymbol{Z}$ 上的未定元。

引理　若 $\alpha\in I$　使 $N(\alpha)=0$　则 $\alpha=0$

证　$I=\boldsymbol{Z}[\sqrt[n]{d}]\subset\boldsymbol{Q}[\sqrt[n]{d}]$——$\boldsymbol{Q}$ 上单纯的二项扩域，是 $\boldsymbol{Q}$ 上 n 维向量空间亦以 $\{1,\ \theta=\sqrt[n]{d},\cdots,\theta^{n-1}\}$ 为一基，在此基下，扩域的正则表示(也是切实的)所对应的矩阵表示限止于 I 就是 M。因扩域的非零元均可逆，故对 $\forall\alpha\in I^*=I-\{0\}$ 来说 $M(\alpha)$ 均是 $M_n(\boldsymbol{Q})$ 里可逆矩阵，因而 $D(\alpha)\neq0$，进一步便有 $N(\alpha)\neq0$。▮

系 5.　在 I 内，元 $\alpha=0\Longleftrightarrow$ 范数 $N(\alpha)=0$　　(6)

系 6.　I 的主理想 (α) 是真的 $\Longleftrightarrow N(\alpha)>1$。

命题　$0\neq\alpha\in I$ 的任一整化因子 β 必为 $\bar{\tilde{\alpha}}$ 的整数倍。

证　因 $$\alpha\beta=(1,\ \theta,\ \cdots,\ \theta^{n-1})M(\alpha)\begin{pmatrix}b_0\\ b_1\\ \vdots\\ b_{n-1}\end{pmatrix}=(1,\ \theta,\ \cdots,\ \theta^{n-1})\begin{pmatrix}m'\\ 0\\ \vdots\\ 0\end{pmatrix}=m'\in\boldsymbol{Z}$$

故 $M(\alpha)$ 的后 $n-1$ 个行向量均与 $(b_0,\ b_1,\ \cdots,\ b_{n-1})$ 正交，这 $n-1$ 个行向量是线性无关的，盖 $D(\alpha)\neq0$。故 $(b_0,\ b_1,\ \cdots,\ b_{n-1})$ 与 $(D_{11}(\alpha),\ D_{12}(\alpha),\ \cdots,\ D_{1n}(\alpha))$ 线性相关[7]，从而与 $(\bar{\tilde{a}}_0,\bar{\tilde{a}}_1,\cdots,\bar{\tilde{a}}_{n-1})$ 线性相关 $\therefore\beta=m\bar{\tilde{\alpha}}$，$m\in\boldsymbol{Z}$。▮

显然　$D(\alpha)=\alpha\tilde{\alpha}=d_\alpha d_{\tilde{\alpha}}(\bar{\alpha}\bar{\tilde{\alpha}})$ 而 $\bar{\alpha}\bar{\tilde{\alpha}}\in\boldsymbol{Z}$　　(7)

从而

$$M(\alpha)M(\tilde{\alpha})=M(\alpha\tilde{\alpha})=M(\tilde{\alpha}\alpha)=M(\tilde{\alpha})M(\alpha)=M(D(\alpha))=D(\alpha)E_n$$

$$\therefore\quad M(\tilde{\alpha})=M(\alpha)^*\ (\text{——}M(\alpha)\text{的伴随矩阵})\tag{8}$$

$$D(\tilde{\alpha})=D(\alpha)^{n-1}\tag{9}$$

又从 $\tilde{a}$ 的定义得 $d_\alpha^{n-1}|d_{\tilde{\alpha}}$

因 $\bar{\tilde{a}}$ 也是 α 的一个整化因子，故是 $\tilde{a}$ 的整数倍 $\therefore\bar{\tilde{\alpha}}=\tilde{\bar{\alpha}}\,d_{\tilde{\alpha}}$。于是

$$D(\bar{\alpha})=\bar{\alpha}\,\tilde{\bar{\alpha}}=\bar{\alpha}\,\tilde{\tilde{\alpha}}\cdot d_{\tilde{\alpha}}\tag{10}$$

由(5)(7)(10)得

$$d_{\tilde{\alpha}}=d_\alpha^{n-1}d_{\tilde{\alpha}}\tag{11}$$

再由 $\bar{\tilde{\alpha}}$ 是 $\tilde{\bar{\alpha}}$ 的整化因子，自然也是 $\tilde{\tilde{\alpha}}=\tilde{\bar{\alpha}}\,d_{\tilde{\alpha}}$ 的整化因子，故必为 $\bar{\alpha}$ 的整数倍，即 $\tilde{\tilde{\alpha}}=\bar{\alpha}\,d_{\tilde{\tilde{\alpha}}}$。乃有

$$D(\tilde{\bar{\alpha}})=\tilde{\bar{\alpha}}\,\tilde{\tilde{\bar{\alpha}}}=\tilde{\bar{\alpha}}\bar{\alpha}\,d_{\tilde{\tilde{\alpha}}}.\tag{13}$$

于是 $D(\alpha)^{n-1}=D(\tilde{\alpha})=d_{\tilde{\alpha}}^n\,D(\tilde{\bar{\alpha}})=d_{\tilde{\alpha}}^n\,d_{\tilde{\tilde{\alpha}}}\,\bar{\alpha}\tilde{\bar{\alpha}}$，利用(7)、(11)得

$$(\bar{\alpha}\tilde{\bar{\alpha}})^{n-2}=d_{\tilde{\alpha}}\,d_{\tilde{\tilde{\alpha}}}\tag{14}$$

特别地在 $n=3$ 时代入(7)得

$$D(\alpha)=d_\alpha d_{\tilde{\alpha}}d_{\tilde{\alpha}}d_{\tilde{\tilde{\alpha}}}\tag{15}$$

当 $n=2$ 时则按(14)与(11)有

$$d_{\tilde{\alpha}}=d_{\tilde{\tilde{\alpha}}}=1,\ d_{\tilde{\alpha}}=d_\alpha\ D(\alpha)=d_\alpha^2\,D(\bar{\alpha})\tag{16}$$

三、主理想(α)内元素形式

设$I=\mathbf{Z}[\sqrt[n]{d}]\ni\alpha=a_0+a_1\theta+\cdots+a_{n-1}\theta^{n-1}\neq 0$, $\theta=\sqrt[n]{d}$，则由《近世代数》知，$(\alpha)=\{\alpha\zeta|\zeta\in I\}$。于是

$x_i\in\mathbf{Z}$, $i=0,1,\cdots,n-1$, 的 $\zeta=\sum_{i=0}^{n-1}x_i\theta^i\in(\alpha)\Longleftrightarrow$存在$m_i\in\mathbf{Z}$, $i=0,1,\cdots,n-1$

使 $x_0+x_1\theta+\cdots+x_{n-1}\theta^{n-1}=\alpha(1,\theta,\cdots,\theta^{n-1})\begin{pmatrix}m_0\\m_1\\\vdots\\m_{n-1}\end{pmatrix}=(1,\theta,\cdots,\theta^{n-1})M(\alpha)\begin{pmatrix}m_0\\m_1\\\vdots\\m_{n-1}\end{pmatrix}$

即

$$\begin{pmatrix}x_0\\x_1\\\vdots\\x_{n-1}\end{pmatrix}=M(\alpha)\begin{pmatrix}m_0\\m_1\\\vdots\\m_{n-1}\end{pmatrix}$$

这又当且仅当

$$M(\tilde{\alpha})\begin{pmatrix}x_0\\x_1\\\vdots\\x_{n-1}\end{pmatrix}=\begin{pmatrix}D(\alpha)m_0\\D(\alpha)m_1\\\vdots\\D(\alpha)m_{n-1}\end{pmatrix}\equiv\begin{pmatrix}0\\0\\\vdots\\0\end{pmatrix}\pmod{N(\alpha)}\tag{1}$$

这是因为$M(\bar{\alpha})=M(\alpha)^*$,证充分性时可用$M(\alpha)$去左乘等式二边，然后消去非0因子$D(\alpha)$就够了。

在同余组(1)里可消去公因子$d_{\tilde{\alpha}}$得等价的

$$M(\tilde{\tilde{\alpha}})\begin{pmatrix}x_0\\x_1\\\vdots\\x_{n-1}\end{pmatrix}\equiv\begin{pmatrix}0\\0\\\vdots\\0\end{pmatrix}\pmod{d_\alpha|\bar{\alpha}\tilde{\tilde{\alpha}}|}\tag{2}$$

这里用了上段的(7)式。

接下去要寻找一个整数表值的可逆矩阵C,使$CM(\tilde{\tilde{\alpha}})$成为主对角线上都是1的高三角矩阵，这对$n=2$的情形毋需上一段知识就可轻而易举地作出。对$n>3$，我们还没有能够把$C$作出，而对$n=3$的情形我们能够作出这样的$C$。

1．$n=2$的情形 $d_{\tilde{\alpha}}=d_\alpha$故

$d_\alpha^2\bar{\alpha}\tilde{\tilde{\alpha}}=D(\alpha)=d_\alpha^2D(\bar{\alpha})$ 而(2)式就是

$$\begin{pmatrix}\overline{a_0} & -d\overline{a_1}\\-\overline{a_1} & \overline{a_0}\end{pmatrix}\begin{pmatrix}x_0\\x_1\end{pmatrix}\equiv\begin{pmatrix}0\\0\end{pmatrix}\pmod{d_\alpha N(\bar{\alpha})}$$

因$(\overline{a_0},-\overline{a_1})=d_{\bar{\alpha}}=1$故有$u_0,u_1\in Z$使得$u_0\overline{a_0}-u_1\overline{a_1}=1$。置

$$C=\begin{pmatrix} u_0 & u_1 \\ \bar{a}_1 & \bar{a}_0 \end{pmatrix}$$

则 $\det C=\begin{vmatrix} u_0 & u_1 \\ \bar{a}_1 & \bar{a}_0 \end{vmatrix}=u_0\bar{a}_0-u_1\bar{a}_1=1$ 是 $\boldsymbol{Z}$ 内正则元，所以 C^{-1} 也是整数矩阵，于是（2）式等价于

$$CM(\tilde{\alpha})\begin{pmatrix} x_0 \\ x_1 \end{pmatrix}=\begin{pmatrix} 1 & \bar{a}_0u_1-d\bar{a}_1u_0 \\ 0 & D(\bar{\alpha}) \end{pmatrix}\begin{pmatrix} x_0 \\ x_1 \end{pmatrix}\equiv 0 \pmod{d_\alpha N(\bar{\alpha})}$$

这可分写成

$$\begin{cases} x_0+(\bar{a}_0u_1-d\bar{a}_1u_0)x_1\equiv 0 \pmod{d_\alpha N(\bar{\alpha})} \\ \qquad\qquad\qquad\qquad x_1\equiv 0 \pmod{d_\alpha} \end{cases} \tag{3}$$

其中第二式已消去因子 $D(\bar{\alpha})$。

故在 $n=2$ 的情形即对 $I=\boldsymbol{Z}[\sqrt{d}]$ 来说 $\alpha\neq 0$ 所生成的主理想

$$(\alpha)=\left\{x_0+x_1\sqrt{d}\in I \;\middle|\; \begin{matrix} x_0+(\bar{a}_0u_1-d\bar{a}_1u_0)x_1\equiv 0 \pmod{d_\alpha N(\bar{\alpha})} \\ x_1\equiv 0 \pmod{d_\alpha} \end{matrix}\right\} \tag{4}$$

2．　$n=3$ 的情形　　$D(\alpha)=d_\alpha d_{\tilde{\alpha}} d_{\tilde{\tilde{\alpha}}}$，(2)式成为

$$M(\tilde{\alpha})\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}\equiv\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \pmod{d_\alpha d_{\tilde{\alpha}} d_{\tilde{\tilde{\alpha}}}}$$

因 $(\tilde{\tilde{a}}_0,\tilde{\tilde{a}}_1,\tilde{\tilde{a}}_2)=d_{\tilde{\tilde{\alpha}}}=1$。故有 $u_0, u_1, u_2\in\boldsymbol{Z}$ 使得

$$u_0\tilde{\tilde{a}}_0+u_1\tilde{\tilde{a}}_1+u_2\tilde{\tilde{a}}_2=1$$

同理因 $(\bar{a}_2,\bar{a}_1,\bar{a}_0)=d_{\bar{\alpha}}=1$，故有 $c_0, c_1, c_2\in\boldsymbol{Z}$ 使得

$$c_0\bar{a}_2+c_1\bar{a}_1+c_2\bar{a}_0=1$$

再取 $v_0, v_1, v_2\in\boldsymbol{Z}$ 使

$$v_0\boldsymbol{i}+v_1\boldsymbol{j}+v_2\boldsymbol{k}=\begin{vmatrix} \boldsymbol{i} & \boldsymbol{j} & \boldsymbol{k} \\ c_0 & c_1 & c_2 \\ \tilde{\tilde{a}}_0 & \tilde{\tilde{a}}_1 & \tilde{\tilde{a}}_2 \end{vmatrix}$$

这右边3阶行列式只许按第1行展开，设 $\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$ 为线性无关的三个向量，即

$$v_0=\begin{vmatrix} c_1 & c_2 \\ \tilde{\tilde{a}}_1 & \tilde{\tilde{a}}_2 \end{vmatrix},\quad v_1=\begin{vmatrix} c_2 & c_0 \\ \tilde{\tilde{a}}_2 & \tilde{\tilde{a}}_0 \end{vmatrix},\quad v_2=\begin{vmatrix} c_0 & c_1 \\ \tilde{\tilde{a}}_0 & \tilde{\tilde{a}}_1 \end{vmatrix}$$

则有

1）　$$\tilde{\tilde{a}}_0v_0+\tilde{\tilde{a}}_1v_1+\tilde{\tilde{a}}_2v_2=\begin{vmatrix} \tilde{\tilde{a}}_0 & \tilde{\tilde{a}}_1 & \tilde{\tilde{a}}_2 \\ c_0 & c_1 & c_2 \\ \tilde{\tilde{a}}_0 & \tilde{\tilde{a}}_1 & \tilde{\tilde{a}}_2 \end{vmatrix}=0$$

2）　$$d\tilde{\tilde{a}}_2v_0+\tilde{\tilde{a}}_0v_1+\tilde{\tilde{a}}_1v_2=\begin{vmatrix} d\tilde{\tilde{a}}_2 & \tilde{\tilde{a}}_0 & \tilde{\tilde{a}}_1 \\ c_0 & c_1 & c_2 \\ \tilde{\tilde{a}}_0 & \tilde{\tilde{a}}_1 & \tilde{\tilde{a}}_2 \end{vmatrix}=\begin{vmatrix} c_2 & c_1 & c_0 \\ \tilde{\tilde{a}}_1 & \tilde{\tilde{a}}_0 & d\tilde{\tilde{a}}_2 \\ \tilde{\tilde{a}}_2 & \tilde{\tilde{a}}_1 & \tilde{\tilde{a}}_0 \end{vmatrix}=$$

$$=d'_{\tilde{a}}(c_2\overline{a_0}+c_1\overline{a_1}+c_0 a_2)=d_{\tilde{a}}^{\sim}$$

3) $$d\widetilde{\widetilde{a_1}}v_0+d\widetilde{\widetilde{a_2}}v_1+\widetilde{\widetilde{a_0}}v_2=\begin{vmatrix} d\widetilde{a_1} & d\widetilde{\widetilde{a_2}} & \widetilde{\widetilde{a_0}} \\ c_0 & c_1 & c_2 \\ \widetilde{\widetilde{a_0}} & \widetilde{\widetilde{a_1}} & \widetilde{\widetilde{a_2}} \end{vmatrix}=\begin{vmatrix} c_0 & c_1 & c_2 \\ \widetilde{\widetilde{a_0}} & \widetilde{\widetilde{a_1}} & \widetilde{\widetilde{a_2}} \\ d\widetilde{\widetilde{a_1}} & d\widetilde{\widetilde{a_2}} & \widetilde{\widetilde{a_0}} \end{vmatrix}=-\begin{vmatrix} c_1 & c_0 & c_2 \\ \widetilde{\widetilde{a_1}} & \widetilde{\widetilde{a_0}} & \widetilde{\widetilde{a_2}} \\ d\widetilde{\widetilde{a_2}} & d\widetilde{\widetilde{a_1}} & \widetilde{\widetilde{a_0}} \end{vmatrix}=$$

$$=-\begin{vmatrix} c_1 & c_0 & dc_2 \\ \widetilde{\widetilde{a_1}} & \widetilde{\widetilde{a_0}} & d\widetilde{\widetilde{a_2}} \\ \widetilde{\widetilde{a_2}} & \widetilde{\widetilde{a_1}} & \widetilde{\widetilde{a_0}} \end{vmatrix}=-d_{\tilde{a}}(c_1\overline{a_0}+c_0\overline{a_1}+c_2 d\overline{a_2})=-b_3 d_{\tilde{\tilde{a}}}.$$

其中 $b_3=c_1\overline{a_0}+c_0\overline{a_1}+c_2 d\overline{a_2}$。

令

$$C=\begin{pmatrix} u_0 & u_1 & u_2 \\ v_0 & v_1 & v_2 \\ \overline{a_2} & \overline{a_1} & \overline{a_0} \end{pmatrix}$$

则按上面的 1), 2), 3) 以及上段的(14)式与$M(\bar{\alpha})M(\tilde{c})=\alpha\tilde{\alpha}E_3$得

$$CM(\tilde{\tilde{\alpha}})=\begin{pmatrix} u_0 & u_1 & u_2 \\ v_0 & v_1 & v_2 \\ \overline{a_2} & \overline{a_1} & \overline{a_0} \end{pmatrix}\begin{pmatrix} \widetilde{\widetilde{a_0}} & d\widetilde{\widetilde{a_2}} & d\widetilde{\widetilde{a_1}} \\ \widetilde{\widetilde{a_1}} & \widetilde{\widetilde{a_0}} & d\widetilde{\widetilde{a_2}} \\ \widetilde{\widetilde{a_2}} & \widetilde{\widetilde{a_1}} & \widetilde{\widetilde{a_0}} \end{pmatrix}=\begin{pmatrix} 1 & b_1 & b_2 \\ 0 & d_{\tilde{\tilde{a}}} & -b_3 d_{\tilde{\tilde{a}}} \\ 0 & 0 & d_{\tilde{a}} d_{\tilde{\tilde{a}}} \end{pmatrix}$$

其中 $b_1=u_0 d\widetilde{\widetilde{a_2}}+u_1\widetilde{\widetilde{a_0}}+u_2\widetilde{\widetilde{a_1}}$, $b_2=u_0 d\widetilde{\widetilde{a_1}}+u_1 d\widetilde{\widetilde{a_2}}+u_2\widetilde{\widetilde{a_0}}$。

计算二边的行列式得

$$d_{\tilde{a}} d^2_{\tilde{\tilde{a}}}=\det(CM(\tilde{\tilde{\alpha}}))=\det C\cdot\det M(\tilde{\tilde{\alpha}})=D(\bar{\alpha})\det C$$

据上一段的(13)、(14)式，$D(\tilde{\tilde{\alpha}})=\bar{\alpha}\tilde{\alpha}d_{\tilde{\tilde{a}}}=d_{\tilde{a}}d^2_{\tilde{\tilde{a}}}$, $\therefore\det C=1$ 从而 $C^{-1}=C^*$ 是整数矩阵，于是组(2)等价于

$$CM(\tilde{\tilde{\alpha}})\begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}\equiv\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}\pmod{d_a d_{\tilde{a}} d_{\tilde{\tilde{a}}}}$$

分开写出消去因子就得等价的

$$\begin{cases} x_0+b_1x_1+b_2x_2\equiv 0 & \pmod{d_a d_{\tilde{a}} d_{\tilde{\tilde{a}}}} \\ x_1-b_3x_2\equiv 0 & \pmod{d_a d_{\tilde{\tilde{a}}}} \\ x_2\equiv 0 & \pmod{d_a} \end{cases}\tag{5}$$

于是在 $n=3$ 的情形即 $I=\mathbf{Z}[\sqrt[3]{d}]$的非零元 α 所生成的主理想

$$(\alpha)=\left\{x_0+x_1\sqrt[3]{d}+x_2\sqrt[3]{d^2}\in I\ \middle|\ \begin{aligned} x_0+b_1x_1+b_2x_2&\equiv 0\pmod{d_a d_{\tilde{a}} d_{\tilde{\tilde{a}}}} \\ x_1-b_3x_2&\equiv 0\pmod{d_a d_{\tilde{a}}} \\ x_2&\equiv 0\pmod{d_a} \end{aligned}\right\}\tag{6}$$

四、n=2,3 时剩余类环 $Z[\sqrt[n]{d}]/(\alpha)$ 的结构

1．$n=2$ 的情形

(i) 对 $\forall i,j\in Z$

$$I_{i,j}=\left\{x_0+x_1\sqrt{d}\in I\;\middle|\;\begin{array}{ll}x_0+bx_1\equiv i & (\bmod\ d_\alpha N(\bar{\alpha}))\\ x_1\equiv j & (\bmod\ d_\alpha)\end{array}\right\}$$

$$=i-bj+j\sqrt{d}+(\alpha)=iI_{1,0}+jI_{0,1}\tag{1}$$

都是模(α)的剩余类，其中 $b=\overline{a_0}u_1-d\overline{a_1}u_0$。证明甚易，无非是证二个集合相等。

(ii) 若 $i_1, i_2\in\{0,1,2,\cdots,d_\alpha N(\bar{\alpha})-1\}$，$j_1, j_2\in\{0,1,2,\cdots,d_\alpha-1\}$使得 $(i_1,j_1)\neq(i_2,j_2)$ 则 $I_{\bar{i}_1,\bar{j}_1}\cap I_{\bar{i}_2,\bar{j}_2}=\phi$。即剩余类 $I_{\bar{i}_1,\bar{j}_1}\neq I_{\bar{i}_2,\bar{j}_2}$

(iii) $Z[\sqrt{d}]/(\alpha)=\{I_{i,j}\,|\,i=0,1,2,\cdots,d_\alpha N(\bar{\alpha})-1;\ j=0,1,2,\cdots,d_\alpha-1\}$，它恰含$N(\alpha)$个元，按剩余类加法和乘法得

$$I_{\bar{i}_1,\bar{j}_1}+I_{\bar{i}_2,\bar{j}_2}=I_{\overline{i_1+i_2},\overline{j_1+j_2}}$$

$I_{0,0}$是加法零元，$I_{1,0}$是乘法单位元而

$$I_{0,1}^2=(d-b^2)I_{1,0}-2bI_{0,1}$$

$$\therefore I_{i_1,j_1}\cdot I_{i_2,j_2}=(i_1I_{1,0}+j_1I_{0,1})(i_2I_{1,0}+j_2I_{0,1})=$$
$$=(i_1i_2+j_1j_2(d-b^2))I_{1,0}+(i_1j_2+i_2j_1-2bj_1j_2)I_{0,1}.$$

故 $\Pi=\{I_{i,0}\,|\,i=0,1,2,\cdots,d_\alpha N(\bar{\alpha})-1\}$是一个子环，它同构于 $Z/(d_\alpha N(\bar{\alpha}))$。

2．$n=3$ 的情形

(i) 对 $\forall i,j,k\in Z$

$$I_{i,j,k}=\left\{x_0+x_1\sqrt[3]{d}+x_2\sqrt[3]{d^2}\in I\;\middle|\;\begin{array}{ll}x_0+b_1x_1+b_2x_2\equiv i & (\bmod\ d_\alpha d_{\tilde{\alpha}}d_{\tilde{\tilde{\alpha}}})\\ x_1-b_3x_2\equiv j & (\bmod\ d_\alpha d_{\tilde{\alpha}})\\ x_2\equiv k & (\bmod\ d_\alpha)\end{array}\right\}=$$

$$=(i-b_1j-b_2k-b_1b_3k)+(j+b_3k)\sqrt[3]{d}+k\sqrt[3]{d^2}+(\alpha)$$

都是模(α)的剩余类，且$I_{i,j,k}=iI_{1,0,0}+jI_{0,1,0}+kI_{0,0,1}$

(ii) 若 $i_1,i_2\in\{0,1,2\cdots,d_\alpha d_{\tilde{\alpha}}d_{\tilde{\tilde{\alpha}}}-1\}$，$j_1,j_2\in\{0,1,2,\cdots,d_\alpha d_{\tilde{\alpha}}-1\}$；$k_1,k_2\in\{0,1,2,\cdots,d_\alpha-1\}$使得$(i_1,j_1,k_1)\neq(i_2,j_2,k_2)$则$I_{\bar{i}_1,\bar{j}_1,\bar{k}_1}\cap I_{\bar{i}_2,\bar{j}_2,\bar{k}_2}=\phi$，即$I_{\bar{i}_1,\bar{j}_1,\bar{k}_1}\neq I_{\bar{i}_2,\bar{j}_2,\bar{k}_2}$

(iii) $Z[\sqrt[3]{d}]/(\alpha)=\{I_{i,j,k}\,|\,i=0,1,2,\cdots,d_\alpha d_{\tilde{\alpha}}d_{\tilde{\tilde{\alpha}}}-1;\ j=0,1,2,\cdots,d_\alpha d_{\tilde{\alpha}}-1;\ k=0,1,\cdots,d_\alpha-1\}$恰含$N(\alpha)$个元，其中加法为

$$I_{\bar{i}_1,\bar{j}_1,\bar{k}_1}+I_{\bar{i}_2,\bar{j}_2,\bar{k}_2}=I_{\overline{i_1+i_2},\overline{j_1+j_2},\overline{k_1+k_2}}$$

$I_{0,0,0}=(\alpha)$是加法零元，$I_{1,0,0}=1+(\alpha)$是乘法单位元，因 $I_{0,1,0}=-b_1+\sqrt[3]{d}+(\alpha)$，故$I_{0,1,0}^2=b_1^2-2b_1\sqrt[3]{d}+\sqrt[3]{d^2}+(\alpha)=(b_2-b_1^2)I_{1,0,0}-(2b_1+b_3)I_{0,1,0}+I_{0,0,1}$；

$I_{0,0,1}=-(b_2+b_1b_3)+b_3\sqrt[3]{d}+\sqrt[3]{d^2}+(\alpha)$，$I_{0,0,1}^2=(db_1+2b_3+b_2b_3-(b_2+b_1b_3)^2)I_{1,0,0}+(d-b_3^2)I_{0,1,0}+(b_3-2b_2-2b_1b_3)I_{0,0,1}$，又 $I_{0,1,0}\cdot I_{0,0,1}=(1-b_1b_2+b_2b_3-b_1^2b_3)I_{1,0,0}-(b_2+b_1b_3-b_3^2)I_{0,1,0}+(b_3-b_1)I_{0,0,1}$。于是乘法表完全确定。又它含子环

$$\Pi=\{I_{i,0,0}\,|\,i=0,1,2,\cdots,d_\alpha d_{\tilde{\alpha}}d_{\tilde{\tilde{\alpha}}}-1\}\cong Z/(d_\alpha d_{\tilde{\alpha}}d_{\tilde{\tilde{\alpha}}}).$$

五、$I=\mathbf{Z}[\sqrt{d}]$ 的所有素元

已知$I=\mathbf{Z}[\sqrt{d}]$的不是单位的非零元α是素元的充要条件是$\mathbf{Z}[\sqrt{d}]/(\alpha)$，为$N(\alpha)$元域。

有限域的元素个数应为某个素数幂，所以α为素元的一个必要条件是$N(\alpha)$是素数幂。问题在于$N(\alpha)$是什么样的素数幂时$I/(\alpha)$才是域。

对素数幂$N(\alpha)$的α只有两种可能情形：(i) $d_\alpha=1$，(ii) $d_\alpha>1$。

(i) 当$d_\alpha=1$时，$N(\bar{\alpha})=N(\alpha)>1$，三中的(4)式成为

$$(\alpha)=\{x_0+x_1\sqrt{d}\in I\,|\,x_0+bx_1\equiv 0\pmod{N(\alpha)}\}$$

而四中的(1)式成为

$$I_i=I_{i,0}=\{x_0+x_1\sqrt{d}\in I\,|\,x_0+bx_1\equiv i\pmod{N(\alpha)}\},i=0,1,2,\cdots,N(\alpha)-1$$

又$\mathbf{Z}[\sqrt{d}]/(\alpha)=\Pi\cong\mathbf{Z}/(N(\alpha))$。当且仅当$N(\alpha)$为素数时它才是域。

(ii) 当$d_\alpha>1$时，$\alpha=\bar{\alpha}d_\alpha$要是素元必不可约，应有$\bar{\alpha}$是单位，即$N(\bar{\alpha})=1$，于是$N(\alpha)=d_\alpha^2$。故若此时$\alpha$是素元必须$d_\alpha$是素数，与$\alpha$相伴(因$\alpha$不可约，故$d_\alpha$不能是素数的高次幂)。此时在四中

$$\mathbf{Z}[\sqrt{d}]/(\alpha)=\{I_{i,j}\,|\,i,j=0,1,2,\cdots,d_\alpha-1\}=\Pi[\sqrt{d}+(\alpha)]$$

其中子环$\Pi\cong\mathbf{Z}/(d_\alpha)$是域。要$I/(\alpha)$是域当且仅当$\sqrt{d}+(\alpha)$在$\Pi$上的最小多项式在$\Pi(x)$内不可约。这个最小多项式是$x^2-(d+(\alpha))$

反映到同构的素域$\mathbf{Z}/(d_\alpha)=\Pi_1$上添加$x^2-(d+(d_\alpha))$的一根来看

$x^2-(d+(d_\alpha))$在Π_1内不可约$\Longleftrightarrow x^2\equiv d\pmod{d_\alpha}$在$\mathbf{Z}$内无解(此时自然$(d_1,d_\alpha)=1$。且素数$d_\alpha>2$，否则有解)。

故在$d_\alpha>1=N(\bar{\alpha})$时$\alpha$是素元当且仅当$d_\alpha$是奇素数且$d$是模$d_\alpha$之一平方非剩余此时$N(\alpha)=d_\alpha^2$。

综合上述所有两种情形乃得一所述的

定理 1　整数$d\neq 0.1$且无平方真因子时，$\mathbf{Z}[\sqrt{d}]$的元$\alpha=a_0+a_1\sqrt{d}$是素元的充要条件

或者(1)　$N(\alpha)>1=d_\alpha$是一个素数

或者(2)　$d_\alpha>1=N(\bar{\alpha})$是一个奇素数且$d$是模$d_\alpha$之一平方非剩余(此时$N(\alpha)=d_\alpha^2$，$(d,d_\alpha)=1$)。

六、$I=\mathbf{Z}[\sqrt[3]{d}]$ 的所有素元

$I=\mathbf{Z}[\sqrt[3]{d}]$的不是单位的非零元$\alpha$是素元$\Longleftrightarrow I/(\alpha)$是$N(\alpha)$元域。由此推出$N(\alpha)$应为素数幂。

范数$(N\alpha)$为素数幂的素元$\alpha=\bar{\alpha}d_\alpha$有两种可能。(i) $d_\alpha>1=N(\bar{\alpha})$，此时$N(\alpha)=d_\alpha^3$，(ii) $d_\alpha=1<N(\alpha)=N(\alpha)$。

(i) $d_\alpha>1$ 时,因 α 不可约，故 $\bar{\alpha}$ 为单位,从而 $N(\bar{\alpha})=1$，α 与 d_α 相伴。据二中 (10) 式和 (14)式有

$$D(\bar{\alpha})=\bar{\alpha}\tilde{\tilde{\alpha}}d_{\tilde{\alpha}}=d_{\tilde{\alpha}}^2 d_{\tilde{\alpha}}$$

由 $N(\bar{\alpha})=1$ 推出 $d_{\tilde{\alpha}}=d_{\tilde{\tilde{\alpha}}}=1$。于是三中(6)式成为

$$(\alpha)=\left\{x_0+x_1\sqrt[3]{d}+x_2\sqrt[3]{d^2}\in I\;\middle|\;\begin{array}{r}x_0+b_1x_1+b_2x_2\equiv 0\quad(\mathrm{mod}\;\; d_\alpha)\\ x_1-b_3x_2\equiv 0\quad(\mathrm{mod}\;\; d_\alpha)\\ x_2\equiv 0\quad(\mathrm{mod}\;\; d_\alpha)\end{array}\right\}$$

而　$I/(\alpha)=\{I_{i,j,k}\,|\,i,j,k=0,1,2,\cdots,d_\alpha-1\}=\Pi[\sqrt[3]{d}+(\alpha)]$

恰含 d_α^3 个元，要它是域必须 d_α 是一个素数且 $\sqrt[3]{d}+(\alpha)$ 在 Π 上的最小多项式不可约。或藉 $\Pi\cong \boldsymbol{Z}/(d_\alpha)$ 来看应有 $\sqrt[3]{d}+(d_\alpha)$ 的最小多项式 $x^3-(d+(d_\alpha))$ 在 $\boldsymbol{Z}/(d_\alpha)$ 上不可约，也就是在 $\boldsymbol{Z}$ 内同余方程 $x^3\equiv d\ (\mathrm{mod}\;\; d_\alpha)$ 无解,亦即 d 是模 d_α 的一个立方非剩余，故必 $(d,\ d_\alpha)=1$。且素数 $d_\alpha>2$，(否则同余方程将有解)。

(ii) $d_\alpha=1$ 时，$\bar{\alpha}=\alpha$，从而 $N(\bar{\alpha})=N(\alpha)=d_{\tilde{\alpha}}^2 d_{\tilde{\tilde{\alpha}}}$，此时

$$(\alpha)=\left\{x_0+x_1\sqrt[3]{d}+x_2\sqrt[3]{d^2}\in I\;\middle|\;\begin{array}{r}x_0+b_1x_1+b_2x_2\equiv 0\quad(\mathrm{mod}\;\; d_{\tilde{\alpha}}d_{\tilde{\tilde{\alpha}}})\\ x_1-b_3x_2\equiv 0\quad(\mathrm{mod}\;\; d_{\tilde{\alpha}})\end{array}\right\}$$

而　$I/(\alpha)=\{I_{i,j,0}\,|\,i=0,1,2,\cdots,\ d_{\tilde{\alpha}}d_{\tilde{\tilde{\alpha}}}-1;\ j=0,1,2,\cdots,d_{\tilde{\alpha}}-1\}$

恰含 $d_{\tilde{\alpha}}^2 d_{\tilde{\tilde{\alpha}}}$ 个元，要它是域，必须 $d_{\tilde{\alpha}}^2 d_{\tilde{\tilde{\alpha}}}$ 是素数幂且自然数 $d_{\tilde{\alpha}}$ 与 $\tilde{\tilde{\alpha}}$ 不能二者都大于1，否则有

$I\,d_{\tilde{\alpha},0,0}\neq\bar{0}\neq I d_{\tilde{\tilde{\alpha}},0,0}$ 而

$$Id_{\tilde{\alpha},0,0}\cdot Id_{\tilde{\tilde{\alpha}},0,0}=(d_{\tilde{\alpha}}+(\alpha))(d_{\tilde{\tilde{\alpha}}}+(\alpha))=d_{\tilde{\alpha}}d_{\tilde{\tilde{\alpha}}}+(\alpha)=(\alpha)=\bar{0}$$

这与域无非零零因子相矛盾，因此这里又有两种可能情形：1) $d_{\tilde{\alpha}}=1<d_{\tilde{\tilde{\alpha}}}$　2) $d_{\tilde{\tilde{\alpha}}}=1<d_{\tilde{\alpha}}$

1) $d_{\tilde{\alpha}}=1<d_{\tilde{\tilde{\alpha}}}$ 时 $N(\alpha)=d_{\tilde{\tilde{\alpha}}}$

$$(\alpha)=\{x_0+x_1\sqrt[3]{d}+x_2\sqrt[3]{d^2}\,|\,x+b_1x_1+b_2x_2\equiv 0\ (\mathrm{mod}\; d_{\tilde{\tilde{\alpha}}})\}$$

而要 $I/(\alpha)=\{I_{i,0,0}\,|\,i=0,1,2,\cdots,d_{\tilde{\tilde{\alpha}}}-1\}\cong\boldsymbol{Z}/(d_{\tilde{\tilde{\alpha}}})$ 是域，必须且只须 $N(\alpha)=d_{\tilde{\tilde{\alpha}}}$ 是一个素数。

2) $d_{\tilde{\tilde{\alpha}}}=1<d_{\tilde{\alpha}}$ 时，$N(\alpha)=d_{\tilde{\alpha}}^2$

$$(\alpha)=\left\{x_0+x_1\sqrt[3]{d}+x_2\sqrt[3]{d^2}\in I\;\middle|\;\begin{array}{r}x_0+b_1x_1+b_2x_2\equiv 0\quad(\mathrm{mod}\;\; d_{\tilde{\alpha}})\\ x_1-b_3x_2\equiv 0\quad(\mathrm{mod}\;\; d_{\tilde{\alpha}})\end{array}\right\}$$

而　$I/(\alpha)=\{I_{i,j,0}\,|\,i,j=0,1,2,\cdots,d_{\tilde{\alpha}}-1\}$

恰含 $d_{\tilde{\alpha}}^2$ 个元，子环 $\Pi=\{I_{i,0,0}\,|\,i=0,1,\cdots,d_{\tilde{\alpha}}-1\}\cong\boldsymbol{Z}/(d_{\tilde{\alpha}})$

由此可见 $d_{\tilde{\alpha}}$ 不能是合数，否则 Π 有零因子而 $I/(\alpha)$ 非域，故要 $I/(\alpha)$ 是域必须 $d_{\tilde{\alpha}}$ 是素数，即 $N(\alpha)=d_{\tilde{\alpha}}^2$ 是素数的平方，$I/(\alpha)$ 是素域 Π 上二次扩域：

$$I/(\alpha)=\Pi[I_{0,1,0}].$$

此时 $I_{0,0,1}=I_{0,0,0}$，故 $I_{0,1,0}^2=-(2b_1+b_3)I_{0,1,0}-(b_1^2-b_2)I_{1,0,0}$

所以 $I_{0,1,0}$ 在 Π 上的最小多项式是

$$x^2+(2b_1+b_3)x+(b_1^2-b_2).$$

它不可约的充要条件是二次同余方程

$$x^2+(2b_1+b_3)x+(b_1^2-b_2)\equiv 0 \pmod{d_{\tilde{\alpha}}} \tag{*}$$

无解，这又有两种可能：①$d_{\tilde{\alpha}}=2$，②$d_{\tilde{\alpha}}$是奇素数

①当$d_{\tilde{\alpha}}=2$时，(*)无解$\Longleftrightarrow(2b_1+b_3)$与$(b_1^2-b_2)$均为奇数$\Longleftrightarrow b_3$为奇数且$b_1$与$b_2$奇偶性不同。

②$d_{\tilde{\alpha}}$为奇素数时，(*)等价于

$$4x^2+4(2b_1+b_3)x+4(b_1^2-b_2)\equiv 0 \pmod{d_{\tilde{\alpha}}}$$

即

$$(2x+2b_1+b_3)^2\equiv(2b_1+b_3)^2-4(b_1^2-b_2) \pmod{d_{\tilde{\alpha}}}$$

故(*)无解当且仅当上式右端$4(b_1b_3+b_2)+b_3^2$是模$d_{\tilde{\alpha}}$之一平方非剩余。

综上所述性得到一中所提出的

定理2 整数$d\neq 0,\pm1$且无立方真因子时$\boldsymbol{Z}[\sqrt[3]{d}]$的元$\alpha=x_0+x_1\sqrt[3]{d}+x_2\sqrt[3]{d^2}$是素元的充要条件当且仅当下列互斥的四个条件有且只有一个成立：

(i) $N(\alpha)=d_\alpha^3$，d_α是与d互素的奇素数且d是模d_α之一立方非剩余。

(ii) 素数 $N(\alpha)=d_{\tilde{\alpha}}>1=d_\alpha=d_{\tilde{\alpha}}$。

(iii) $N(\alpha)=d_{\tilde{\alpha}}^2$，$d_{\tilde{\alpha}}>1=d_\alpha=d_{\tilde{\alpha}}$为一奇素数且整数$4(b_1b_3+b_2)+b_3^2$是模$d_{\tilde{\alpha}}$之一平方非剩余。

(iv) $N(\alpha)=d_{\tilde{\alpha}}^2=4$，$d_\alpha=d_{\tilde{\alpha}}=1$，且$2\nmid b_3$而$b_1\not\equiv b_2 \pmod 2$。

参 考 文 献

[1] N. Jacobson. Basic Algebia I.

[2] Erich Hecke, Lectures on the Theory of Algebraic Numbers, Chaptes V.

[3] B. L. Van der Waerden, Algebra I, 丁石孙等译，80～81。

[4] 沈明刚，Gauss整数环$\boldsymbol{Z}[i]$关于主理想$(a+b\sqrt{-1})$的分类，高师数学教学，1983，(7)，29～32。

[5] 赵嗣元，$\boldsymbol{Z}[\sqrt{d}]$对主理想$(a+b\sqrt{d})$的剩余类环，高师数学教学，1985，(11)，6-1～6-8，211.

[6] N. Jacobson, Basic Algebra II, 211.

[7] 北京大学代数组编，高等代数，355～356。

Determination of All Prime Elements of the Two Kinds of Domains of Algebraic Integers $Z[\sqrt{d}]$ and $Z[\sqrt[3]{d}]$

Zhao Siyuan

Abstract

In this paper, we have determined, by using the elementary method, all prime elements of the two kinds of domains of algebraic integers $\boldsymbol{Z}[\sqrt{d}]$ and $\boldsymbol{Z}[\sqrt[3]{d}]$ in terms of the notions of norm, primitization and integralized factor of an algebraic integers. The result obtained in the case of $\boldsymbol{Z}[\sqrt{d}]$ is especially simple. We have obtained the follwing theorem:

Theorem 1. Let the rational integer $d \neq 0, 1$ and be square free. Then $\alpha = a_0 + a_1\sqrt{d} \in \boldsymbol{Z}[\sqrt{d}]$ is a prime element if and only if:

either (i) $N(\alpha) > 1 = d_\alpha$ and $N(\alpha)$ is a prime number, where $N(\alpha) = |a_0^2 - da_1^2|$ is the norm of α, and $d_\alpha = (a_0, a_1)$ is the *g.c.d.* of its coordinates a_0, a_1;

or (ii) $d_\alpha > 1 = N(\bar{\alpha})$ and d_α is an odd prime number such that $(d, d_\alpha) = 1$ and d is a square non-residue modulo-d_α. (in this case, $N(\alpha) = d_\alpha^2$.), where $\bar{\alpha} = \alpha d_\alpha^{-1}$ is the primitization of α.

Theorem 2. If the rational integer $d \neq 0$、± 1 and is cubic free, then $\alpha = a_0 + a_1\sqrt[3]{d} + a_2\sqrt[3]{d^2} \in \boldsymbol{Z}[\sqrt[3]{d}]$ is a prime element if and only if one and only one of the following four mutually independent conditions is valid:

(i) $N(\alpha) = d_\alpha^3$ and d_α is an odd prime number such that $(d, d_\alpha) = 1$ and d_α is a cubic non-residue mod-d_α (in this case $\alpha \sim d_\alpha$)

(ii) $d_\alpha = d_{\tilde{\bar{\alpha}}} = 1 < d_{\overset{\approx}{\alpha}} = N(\alpha)$ and $N(\alpha)$ is a prime number, where $\bar{\alpha}$, $\tilde{\bar{\alpha}}$ are respectively the primitization of α, $\tilde{\alpha}$, and $\tilde{\alpha}$、$\overset{\simeq}{\alpha}$、$\overset{\approx}{\alpha}$ are respectively the normal integralized factors of α、$\bar{\alpha}$、$\tilde{\bar{\alpha}}$, and again d_α、$d_{\overset{\simeq}{\alpha}}$、$d_{\overset{\approx}{\alpha}}$ are respectively the g、c、d. of coordinates of α、$\overset{\simeq}{\alpha}$、$\overset{\approx}{\alpha}$;

(iii) $d_\alpha = d_{\overset{\simeq}{\alpha}} = 1 < 2 = d_{\tilde{\alpha}}$、$2 \nmid b_3$ and $b_1 \not\equiv b_2 \pmod 2$, where $b_1 = u_0 d\widetilde{\overline{a}}_2 + u_1\widetilde{\overline{a}}_0 + u_2\widetilde{\overline{a}}_1$, $b_2 = u_0 d\widetilde{\overline{a}}_1 + u_1 d\widetilde{\overline{a}}_2 + u_2\widetilde{\overline{a}}_0$, $b_3 = c_1\overline{a}_0 + c_0\overline{a}_1 + dc_2\overline{a}_2$ and $u_i, c_i \in \boldsymbol{Z}$ $(i = 0, 1, 2)$ are chosen such that

$$u_0\widetilde{\overline{a}}_0 + u_1\widetilde{\overline{a}}_1 + u_2\widetilde{\overline{a}}_2 = 1, \quad c_2\overline{a}_0 + c_1\overline{a}_1 + c_0\overline{a}_2 = 1$$

since $(\widetilde{\overline{a}}_0, \widetilde{\overline{a}}_1, \widetilde{\overline{a}}_2) = d_{\overset{\simeq}{\alpha}} = 1$, $(\overline{a}_0, \overline{a}_1, \overline{a}_2) = d_{\bar{\alpha}} = 1$. (in this case $N(\alpha) = 2^2$).

(iv) $d_\alpha = d_{\overset{\approx}{\alpha}} = 1 < d_{\overset{\simeq}{\alpha}}$ and $d_{\overset{\simeq}{\alpha}}$ is an odd prime. number such that $4(b_1b_3 + b_2) + b_3^2$ is a square residue mod-$d_{\tilde{\alpha}}$ and so is mutually prime with $d_{\overset{\simeq}{\alpha}}$ (in this case $N(\alpha) = d_{\overset{\simeq}{\alpha}}^2$).