数理解析研究所講究録
1154巻 2000年 165-174

$\langle a\theta+b, c\theta+d\rangle$ の型の単数群をもつ総実3次の整環について

峯村健二 (Kenji Minemura)

(名古屋大学大学院人間情報学研究科ＤＣ)

1 Introduction

代数的整数論の大きな問題として類数問題があるが, 類数問題を扱う際に必要になってくるパラメータの1つとして単数規準が挙げられる. すなわち基本単数系を調べることが重要な課題となる. ここでは代数体として総実3次体を扱うが, 一般的に体の判別式が大きいほど基本単数を求めるのも難しくなってしまう. そこで, 逆に基本単数系の型を最初に決め, その型の総実3次体を無限個求めるというアプローチが1つの手段として確立している. それにより今までどのような結果が得られているか, 以下に触れてみたい.

まずは記号の定義から. $\phi(x)\in\mathbf{Z}[X]$ を総実既約3次多項式, $\phi(x)=0$ の3実根を$\theta=\theta^{(0)}>\theta^{(1)}>\theta^{(2)}$ とし, そのうちの1つを有理数体 $\mathbf{Q}$ に添加して総実3次体 $\mathbf{Q}(\theta)$ を作る. ここで, 各根を添加してできたどの体もお互いに同型となることに注意. また, $E_K=\langle -1\rangle\times E_K^+$ を Kの単数群, ただし E_K^+ はノルムが1の単数のなす群とする. 類数問題においては単数群の基底を求めることが重要になるのだが, ここでは整環 $\mathfrak{o}_\theta=\mathbf{Z}[\theta]$ における単数群, つまり $E_K^+\cap\mathfrak{o}_\theta$ の基底について調べる. 体の判別式が square-free であるという条件をつければ整環 $\mathfrak{o}_\theta$は体 K の整数環となり, 類数問題にそのまま適用できるし, 最近では整環 $\mathfrak{o}_\theta$ のままの議論でも不定方程式論に応用できることがわかっている. 実際, 後に2元3次の不定方程式 (Thue 方程式の一種) として見ることのできる式がいくつか出てくるので, その様子も少しながらうかがうことができるであろう.

さて, 今後よく使う有理整数 a,b,c,d を用意しておく. 1972年, Stender は $E_K^+\cap\mathfrak{o}_\theta=\langle\theta+b,\theta+d\rangle$, $\left\langle\frac{\theta+ab}{\theta},\frac{\theta+ad}{\theta}\right\rangle$ なる型の整環 $\mathfrak{o}_\theta$ の族を見つけた. 1979年, Thomas $E_K^+\cap\mathfrak{o}_\theta=\langle a\theta+1,\theta+d\rangle, \langle a\theta+1,c\theta+1\rangle$ なる型の $\mathfrak{o}_\theta$ の族を見つけた. 1995年, Grundman は Thomas の用いた方法をアルゴリズム化し, 例として $E_K^+\cap\mathfrak{o}_\theta=\langle a\theta+1,2\theta+3\rangle$ なる型の $\mathfrak{o}_\theta$ の族を見つけた. このアルゴリズムを利用し, 最近では $E_K^+\cap\mathfrak{o}_\theta=\langle a\theta+b,\theta\rangle$ $(|a|,|b|\geq 2)$ なる型の $\mathfrak{o}_\theta$ の族を得ることができたのだが, ここではそれを拡張した $E_K^+\cap\mathfrak{o}_\theta=\langle a\theta+b,c\theta+d\rangle$, $(|a|,|c|\geq 2,|b|,|d|\geq 1)$ なる型の $\mathfrak{o}_\theta$ の族を求めてみる.

まず, $a\theta+b, c\theta+d\in E_K^+$ をみたすような$\phi(x)=x^3+ex^2+fx+g$ の候補を得たいのだが, それについて以下の2つの命題が得られる.

命題 1 $a\theta+b, c\theta+d\in E_K^+$ ならば

$$b^3-eab^2+fa^2b-ga^3=1,\quad d^3-ecd^2+fc^2d-gc^3=1. \tag{1}$$

証明 (1) の両式はそれぞれ $N_{K/\mathbf{Q}}(a\theta+b)=+1$ と $N_{K/\mathbf{Q}}(c\theta+d)=+1$ から得られる. □

命題 2 与えられた a,b,c,d に対し, ある有理整数の組 (e,f,g) が (1) をみたすとする. このとき (e_0,f_0,g_0) が

$$b^3 - e_0ab^2 + f_0a^2b - g_0a^3 = 1, \quad d^3 - e_0cd^2 + f_0c^2d - g_0c^3 = 1. \tag{2}$$

をみたすための必要十分条件は, ある有理整数 t,t' が存在して,

$$e = e_0 + \frac{ac}{(a,c)}t, \quad g = g_0 + \frac{bd}{(b,d)}t', \quad f = f_0 + \frac{bc}{(a,c)}t + \frac{ad}{(b,d)}t'. \tag{3}$$

をみたすことである.

証明 (2) が成り立つとすると $(1)-(2)$ より

$$-(e-e_0)b^2 + (f-f_0)ab - (g-g_0)a^2, \quad -(e-e_0)d^2 + (f-f_0)cd - (g-g_0)c^2.$$

よってある有理整数 t_1,t_2,t_3,t_4 が存在して

$$e - e_0 = at_1 = ct_2, \quad g - g_0 = bt_3 = dt_4.$$

従って

$$t_1 = \frac{c}{(a,c)}t, \quad t_2 = \frac{a}{(a,c)}t, \quad t_3 = \frac{b}{(b,d)}t', \quad t_4 = \frac{d}{(b,d)}t'$$

というように t,t' をとれば (3) がみたされる.
逆に (3) を仮定すれば (2) が成り立つことは明らか. □

ここで $\frac{b}{a} > \frac{d}{c}$ としても一般性を失わないことに注意し, 以下の定理を得る.

主定理 $|a|,|c| \geq 2$, $|b|,|d| \geq 1$, $\frac{b}{a} - \frac{d}{c} > 3$ とする. またある有理整数 e_0,f_0,g_0 で

$$b^3 - e_0ab^2 + f_0a^2b - g_0a^3 = 1, \quad d^3 - e_0cd^2 + f_0c^2d - g_0c^3 = 1$$

をみたすものが存在するとして, 有理整数 t,t' に対し

$$e = e_0 + \frac{ac}{(a,c)}t, \quad g = g_0 + \frac{bd}{(b,d)}t', \quad f = f_0 + \frac{bc}{(a,c)}t + \frac{ad}{(b,d)}t',$$

$$\phi(x) = x^3 + ex^2 + fx + g$$

とおく. このとき,

$$\left|e - \frac{a^2}{b^2}g - 2\frac{b}{a} - \frac{1}{ab^2}\right| > 5|ag|, \quad \left|e - \frac{c^2}{d^2}g - 2\frac{d}{c} - \frac{1}{cd^2}\right| > 5|cg|$$

かつ

$$\left|e - \frac{b}{a} - 2\frac{d}{c}\right| > 3|a|, \quad \left|e - \frac{d}{c} - 2\frac{b}{a}\right| > 3|c|$$

ならば $\mathfrak{o}_\theta \cap E_K^+ = \langle a\theta + b, c\theta + d \rangle$.

2 Berwick, Grundman の定理

まず $i, i', i'' \in \{0,1,2\}$, $i \neq i' \neq i'' \neq i$, $m, n \in \mathbf{Z}$, $m > 0$, $n \geq 0$ に対し, 主定理の証明に使われる記号を以下のように定義しておく.

$$\begin{array}{rcl}
[e_{i,0}, e_{i,1}, \cdots] & : & |\theta^{(i)}| \text{ の連分数展開}, \\
\dfrac{p_{i,n}}{q_{i,n}} & : & |\theta^{(i)}| \text{ の } n \text{ 次近似分数}, \\
\lambda_i & := & \dfrac{1}{|\theta^{(i')} - \theta^{(i'')}|}, \\
\delta_i & := & \lambda_i(\lambda_{i'} + \lambda_{i''}), \\
M_{i,n} & := & \lceil e_{i,n+1} - 2\lambda_i q_{i,n+1} \rceil, \\
N_i & := & \left\{ \begin{array}{cl} \lceil 2\lambda_i \theta^{(i)} + 1 \rceil & \text{if } \theta^{(i')}\theta^{(i'')} > 0 \\ 1 & \text{otherwise} \end{array} \right. , \\
\Delta_i & := & \mathrm{sign}(\theta^{(i)}), \\
\eta_{i,m,n} & := & m q_{i,n} \theta^2 + m(q_{i,n} e - \Delta_i p_{i,n})\theta - \left\lfloor \dfrac{m g q_{i,n}}{\theta^{(i)}} \right\rfloor \\
 & & (\lfloor * \rfloor \text{ は } * \text{ 以下の整数で一番大きいものを表す記号}), \\
C_i & := & \{ \eta \in \mathfrak{o}_\theta \ : \ \eta^{(i)} > 1 \text{ and } |\eta^{(j)}| < 1 \text{ for each } j \in \{0,1,2\}, j \neq i \}, \\
S_{i,n} & := & \{ \gamma \in C_i \cap E_K : \ \gamma = (-1)^i(\eta_{i,m,n} + l) \text{ with } 1 \leq m \leq M_{i,n}, \\
 & & -N_i \leq l < N_i, \ m, l \in \mathbf{Z} \}.
\end{array}$$

主定理の証明のために, 以下の 2 つの定理を使う.

定理 (Berwick[1]) (1) 各 C_i $(i = 0,1,2)$ には必ず単数が存在する.
(2) C_i の単数で, i 番目の共役が最小となるものが存在し, それを ε_i とすると, $\varepsilon_0, \varepsilon_1, \varepsilon_2$ のうちの任意の 2 つが $\mathfrak{o}_\theta$ に関する基本単数系をなす.

Berwick の定理に現れる ε_i をここでは fundamental C_i unit と呼ぶ.

定理 (Grundman[3]) $i = 0,1,2$ に対し $e_{i,n_i+1} \leq \dfrac{1}{2} q_{i,n_i+1}$ かつ $S_{i,n_i} \neq \emptyset$ なる $n_i \geq 1$ が存在するとし,

$$m_i := \min\{ \ m \ : \ (-1)^i(\eta_{i,m,n_i} + l) \in S_{i,n_i} \text{ for some } l \ \},$$

$$l_i := \min\{ \ l \ : \ (-1)^i(\eta_{i,m_i,n_i} + l) \in S_{i,n_i} \ \}$$

とする. このとき, もし $\delta_i < \dfrac{1}{2}$ ならば $(-1)^i(\eta_{i,m_i,n_i} + l_i)$ は fundamental C_i unit である.

3　主定理の証明

主定理の証明に入るが, $|a|<|b|$, $|c|<|d|$ と仮定して良い. 他の場合は適当な変数変換 $\theta := \theta + T$ $(T \in \mathbf{Z})$ によってこの場合に帰着できるからである.

また, 以下でよく用いる次の値を用意しておく：

$$\phi\left(-\frac{b}{a}\right) = -\frac{1}{a^3},$$

$$\phi'\left(-\frac{b}{a}\right) = 3\frac{b^2}{a^2} - 2e\frac{b}{a} + f = 2\frac{b^2}{a^2} - e\frac{b}{a} + g\frac{a}{b} + \frac{1}{a^2b},$$

$$\phi''\left(-\frac{b}{a}\right) = -6\frac{b}{a} + 2e = -2\left(\frac{a}{b}\phi'\left(-\frac{b}{a}\right) + \frac{b}{a} - g\frac{a^2}{b^2} - \frac{1}{ab^2}\right).$$

補題 1　ある $n_i \in \mathbf{Z}_{>0}$ に対して $p_{i,n_i} = |a|$, $q_{i,n_i} = |b|$ となる $\theta^{(i)}$ が存在する.

証明　$\left|\theta^{(i)} - \left(-\frac{b}{a}\right)\right| < \frac{1}{2a^2}$ なる $\theta^{(i)}$ が存在することを示せば, 連分数についてのよく知られた結果から 補題 1 が得られる. しかし, ここでは後のためにより強い結論$\left|\theta^{(i)} - \left(-\frac{b}{a}\right)\right| < \frac{1}{2a^2|g|}$ を導くことにする.

$\Delta' = \mathrm{sign}\left(a\phi'\left(-\frac{b}{a}\right)\right)$ とおくと,

$$\begin{aligned}
&\phi\left(-\frac{b}{a} + \Delta'\frac{1}{2a^2|g|}\right) \Big/ \phi\left(-\frac{b}{a}\right) \\
&= \phi\left(-\frac{b}{a}\right) + \phi'\left(-\frac{b}{a}\right)\left(\Delta'\frac{1}{2a^2|g|}\right) + \frac{\phi''\left(-\frac{b}{a}\right)}{2}\left(\Delta'\frac{1}{2a^2|g|}\right)^2 + \left(\Delta'\frac{1}{2a^2|g|}\right)^3 \Big/ \phi\left(-\frac{b}{a}\right) \\
&= 1 - \frac{|a|}{2|g|}\left|\phi'\left(-\frac{b}{a}\right)\right| - \frac{1}{8ag^2}\phi''\left(-\frac{b}{a}\right) - \Delta'\frac{1}{8a^3|g|^3} \\
&= 1 - \frac{|a|}{2|g|}\left|\phi'\left(-\frac{b}{a}\right)\right| + \frac{1}{4ag^2}\left(\frac{a}{b}\phi'\left(-\frac{b}{a}\right) + \frac{b}{a} - g\frac{a^2}{b^2} - \frac{1}{ab^2}\right) - \Delta'\frac{1}{8a^3|g|^3} \\
&= \left(-\frac{|a|}{2|g|} + \frac{1}{4gb^2}\frac{\phi'\left(-\frac{b}{a}\right)}{\left|\phi'\left(-\frac{b}{a}\right)\right|}\right)\left|\phi'\left(-\frac{b}{a}\right)\right| + \frac{b}{4a^2g^2} - \frac{a}{4b^2|g|} - \frac{1}{4a^2b^2g^2} - \Delta'\frac{1}{8a^3|g|^3} + 1 \\
&< \left(-\frac{|a|}{2|g|} + \frac{1}{4|b|g^2}\right)\left|\phi'\left(-\frac{b}{a}\right)\right| + \frac{b}{4a^2g^2} - \frac{a}{4b^2|g|} - \Delta'\frac{1}{8a^3|g|^3} + 1 \\
&< -\frac{7|a|}{16|g|}\left|\phi'\left(-\frac{b}{a}\right)\right| + \frac{b}{4a^2g^2} - \frac{a}{4b^2|g|} + \frac{1}{8a^3|g|^3} + 1 \\
&< -\frac{7|a|}{16|g|}\left(\left|\phi'\left(-\frac{b}{a}\right)\right| - \frac{4|b|}{7|a|^3|g|} - \frac{4}{7b^2} - \frac{16|g|}{7|a|} - \frac{2}{7|a|a^3g^2}\right) \\
&< -\frac{7|a|}{16|g|}\left(\left|\phi'\left(-\frac{b}{a}\right)\right| - 2|g| - \frac{4}{7b^2}\right).
\end{aligned}$$

$\left|\phi'\left(-\frac{b}{a}\right)\right| > 5|gb|$ より, 上の値は負となり, 従ってある $\theta^{(i)}$ が $-\frac{b}{a}$ と $-\frac{b}{a} + \Delta'\frac{1}{2a^2|g|}$ の間にあることがわかる. よって $\left|\theta^{(i)} - \left(-\frac{b}{a}\right)\right| < \frac{1}{2a^2|g|}$ となり, 補題 1 が得られる. □

以下, 補題 1 の n_i を固定しておく.

補題 2 $e_{i,n_i+1} > 4|ab|$.

証明 $\Delta' := \mathrm{sign}\left(a\phi\left(-\frac{b}{a}\right)\right)$, $S := \left|a\phi'\left(-\frac{b}{a}\right)\right| - \frac{3q_{i,n_i-1}}{|a|}$ とおくと,

$$\begin{aligned} S &= \Delta' a\phi'\left(-\frac{b}{a}\right) - \frac{3q_{i,n_i-1}}{|a|} \\ &= \Delta'\left(-eb + \frac{2b^3+ga^3+1}{ab}\right) - \frac{3q_{i,n_i-1}|b|}{|a||b|} \end{aligned}$$

より, 各分数の分子は b で割り切れ, さらに

$$\begin{aligned} S &= \Delta'\left(-eb + \frac{2b^3+ga^3+1}{ab}\right) + \frac{3(|a|p_{i,n_i-1} - \Delta'\Delta_i)}{\Delta_i ab} \\ &= \Delta'\left(-eb + \frac{2(b^3-1)+ga^3}{ab}\right) + \frac{3|a|p_{i,n_i-1}}{\Delta_i ab} \end{aligned}$$

より, 各分数の分子は a でも割り切れるから, $S \in \mathbf{Z}$. また

$$\begin{aligned} q_{i,n_i}p_{i,n_i-1} - p_{i,n_i}q_{i,n_i-1} &= |a|p_{i,n_i-1} - |b|q_{i,n_i-1} \\ &= \mathrm{sign}\left(|\theta^{(i)}| - \left|-\frac{b}{a}\right|\right) \\ &= \mathrm{sign}\left(-\phi\left(-\frac{b}{a}\right)\right)\mathrm{sign}\left(\phi'\left(-\frac{b}{a}\right)\right)\mathrm{sign}\left(\theta^{(i)}\right) \\ &= \mathrm{sign}(a)\mathrm{sign}\left(\phi'\left(-\frac{b}{a}\right)\right)\mathrm{sign}\left(\theta^{(i)}\right) \\ &= \Delta_i\Delta' \end{aligned}$$

より

$$\begin{aligned} \Delta_i\frac{|b|S + p_{i,n_i-1}}{|a|S + q_{i,n_i-1}} &= -\frac{b}{a} + \Delta_i\frac{|a|p_{i,n_i-1} - |b|q_{i,n_i-1}}{|a|(|a|S + q_{i,n_i-1})} \\ &= -\frac{b}{a} + \Delta'\frac{1}{|a|(|a|S + q_{i,n_i-1})} \end{aligned}$$

であるから, $S > 5|gab| - 3 > 4|gab|$ などにより

$$\begin{aligned} &a^3(|a|S + q_{i,n_i-1})^3\phi\left(\Delta_i\frac{|b|S + p_{i,n_i-1}}{|a|S + q_{i,n_i-1}}\right) \\ &= a^3(|a|S + q_{i,n_i-1})^3\left\{\phi\left(-\frac{b}{a}\right) + \phi'\left(-\frac{b}{a}\right)\left(\frac{\Delta'}{|a|(|a|S + q_{i,n_i-1})}\right)\right. \\ &\quad \left. + \frac{\phi''\left(-\frac{b}{a}\right)}{2}\left(\frac{\Delta'}{|a|(|a|S + q_{i,n_i-1})}\right)^2 + \frac{\phi'''\left(-\frac{b}{a}\right)}{6}\left(\frac{\Delta'}{|a|(|a|S + q_{i,n_i-1})}\right)^3\right\} \\ &= -(|a|S + q_{i,n_i-1})^3 + a^2\left|\phi'\left(-\frac{b}{a}\right)\right|(|a|S + q_{i,n_i-1})^2 + \frac{a\phi''\left(-\frac{b}{a}\right)}{2}(|a|S + q_{i,n_i-1}) + \Delta'\frac{a}{|a|} \end{aligned}$$

$$
\begin{aligned}
&= 2q_{i,n_i-1}(|a|S+q_{i,n_i-1})^2+\frac{a\phi''\left(-\frac{b}{a}\right)}{2}(|a|S+q_{i,n_i-1})+\Delta'\frac{a}{|a|}\\
&> (|a|S+q_{i,n_i-1})\left\{2q_{i,n_i-1}(|a|S+q_{i,n_i-1})-\frac{\left|a\phi''\left(-\frac{b}{a}\right)\right|}{2}\right\}+\Delta'\frac{a}{|a|}\\
&> (|a|S+q_{i,n_i-1})\left\{2q_{i,n_i-1}(|a|S+q_{i,n_i-1})-|a|\left|\frac{a}{b}\phi'\left(-\frac{b}{a}\right)+\frac{b}{a}-g\frac{a^2}{b^2}-\frac{1}{ab^2}\right|\right\}+\Delta'\frac{a}{|a|}\\
&> (|a|S+q_{i,n_i-1})\left\{2q_{i,n_i-1}(|a|S+q_{i,n_i-1})-\frac{1}{|b|}(|a|S+3q_{i,n_i-1})-\left|\frac{b}{a}-g\frac{a^2}{b^2}-\frac{1}{ab^2}\right|\right\}+\Delta'\frac{a}{|a|}\\
&> (|a|S+q_{i,n_i-1})\left\{\left(2q_{i,n_i-1}-\frac{1}{|b|}\right)(|a|S+q_{i,n_i-1})-\frac{2q_{i,n_i-1}}{|b|}-\left|\frac{b}{a}-g\frac{a^2}{b^2}-\frac{1}{ab^2}\right|\right\}+\Delta'\frac{a}{|a|}\\
&> 0.
\end{aligned}
$$

よって $\mathrm{sign}\Big(\phi\left(\Delta_i\frac{|b|S+p_{i,n_i-1}}{|a|S+q_{i,n_i-1}}\right)\Big)$ は $\mathrm{sign}(a)$ に等しい. 同様に

$$
\begin{aligned}
&a^3(|a|(S+2)+q_{i,n_i-1})^3\phi\left(\Delta_i\frac{|b|(S+2)+p_{i,n_i-1}}{|a|(S+2)+q_{i,n_i-1}}\right)\\
&\quad= -(|a|(S+2)+q_{i,n_i-1})^3+a^2\left|\phi'\left(-\frac{b}{a}\right)\right|(|a|(S+2)+q_{i,n_i-1})^2\\
&\qquad+\frac{a\phi''\left(-\frac{b}{a}\right)}{2}(|a|(S+2)+q_{i,n_i-1})+\Delta'\frac{a}{|a|}\\
&\quad= -2(|a|-q_{i,n_i-1})(|a|(S+2)+q_{i,n_i-1})^2+\frac{a\phi''\left(-\frac{b}{a}\right)}{2}(|a|(S+2)+q_{i,n_i-1})+\Delta'\frac{a}{|a|}\\
&\quad< 0
\end{aligned}
$$

となり, $\mathrm{sign}\Big(\phi\left(\Delta_i\frac{|b|(S+2)+p_{i,n_i-1}}{|a|(S+2)+q_{i,n_i-1}}\right)\Big)$ は $-\mathrm{sign}(a)$ に等しいことが言える. 従って

$$
\phi\left(\Delta_i\frac{|b|S+p_{i,n_i-1}}{|a|S+q_{i,n_i-1}}\right)\phi\left(\Delta_i\frac{|b|(S+2)+p_{i,n_i-1}}{|a|(S+2)+q_{i,n_i-1}}\right)<0
$$

となり, $|\theta^{(i)}|$ は $\frac{|b|S+p_{i,n_i-1}}{|a|S+q_{i,n_i-1}}$ と $\frac{|b|(S+2)+p_{i,n_i-1}}{|a|(S+2)+q_{i,n_i-1}}$ の間にあることがわかる. 故に $S+2\geq e_{i,n_i+1}\geq S>4|ab|$. □

補題 3 $(-1)^i(a\theta+b)^{-1}\in S_{i,n_i}$.

証明 補題 1 より

$$
\begin{aligned}
\eta_{i,m,n_i} &= mq_{i,n_i}\theta^2+m(q_{i,n_i}e-\Delta_i p_{i,n_i})\theta-\left\lfloor\frac{mgq_{i,n_i}}{\theta^{(i)}}\right\rfloor\\
&= m|a|\theta^2+m(|a|e-\Delta_i|b|)\theta-\left\lfloor\frac{mg|a|}{\theta^{(i)}}\right\rfloor.
\end{aligned}
$$

一方,

$$
(a\theta+b)^{-1}=a^2\theta^2+(a^2e-ab)\theta+\frac{a^3g+1}{b}.
$$

$M_{i,n_i} > |a|$ をいう. $\lambda_i = \frac{1}{|\theta^{(i')}-\theta^{(i'')}|} < \frac{1}{\left|e-\frac{b}{a}-2\frac{d}{c}\right|-\frac{1}{2a^2}-\frac{1}{c^2}} < \frac{2}{5|a|}$ より,

$$\begin{aligned}
M_{i,n_i} &= \lceil e_{i,n_i+1} - 2\lambda_i q_{i,n_i+1} \rceil \\
&= \lceil e_{i,n_i+1} - 2\lambda_i (e_{i,n_i+1}|a| + q_{i,n_i-1}) \rceil \\
&> \lceil e_{i,n_i+1} - 2\lambda_i (e_{i,n_i+1}|a| + |a|) \rceil \\
&= \lceil (e_{i,n_i+1}+1)(1-2\lambda_i|a|) - 1 \rceil \\
&> \left\lceil (4|gab|+1)\left(1-\frac{4}{5|a|}|a|\right) - 1 \right\rceil \\
&= \left\lceil \frac{4}{5}|gab| - \frac{4}{5} \right\rceil \\
&> |a|.
\end{aligned}$$

あとは $-N_i \leq -1 \leq (a\theta+b)^{-1} - \eta_{i,|a|,n_i} < 1 \leq N_i$ をいえばよい. 実際, 補題 1 の証明より, ある $|\alpha| < \frac{1}{|ag|}$ を用いて $\theta^{(i)} = -\dfrac{b}{a+\alpha}$ と書けるから,

$$(a\theta+b)^{-1} - \eta_{i,|a|,n_i} = \frac{a^3g+1}{b} + \left\lfloor \frac{a^2g}{\theta^{(i)}} \right\rfloor = \left\lfloor \frac{a^3g+1}{b} - \frac{a^3g+\alpha a^2 g}{b} \right\rfloor = \left\lfloor \frac{-\alpha a^2 g+1}{b} \right\rfloor = 0 \text{ or } -1.$$

以上より $(-1)^i(a\theta+b)^{-1} \in S_{i,n_i}$. $\square$

補題 4 $m_i = a$.

証明 $c := -\left\lfloor \dfrac{-m|a|}{\theta^{(i)}} \right\rfloor + d$ とおくと, 補題 1 より

$$\begin{aligned}
(a\theta+b)(\eta_{i,m,n_i}+d) &= (a\theta+b)(m|a|\theta^2 + m(|a|e - \Delta_i|b|)\theta + c) \\
&= \left(m|a|\frac{-ga^3-1}{ab} + ac\right)\theta - gma|a| + bc.
\end{aligned}$$

ここで $A = m|a|\frac{-ga^3-1}{ab} + ac$ とおくと

$$(a\theta+b)(\eta_{i,m,n_i}+d) = A\theta + \frac{m}{|a|} + \frac{bA}{a}$$

$\eta_{i,m,n_i}+d$ が単数であると仮定すると, $a\theta+b$ は単数であるから $A\theta + \frac{m}{|a|} + \frac{bA}{a}$ も単数となり, ノルムの計算から

$$A^3 + m|a|a\phi'\left(-\frac{b}{a}\right)A^2 - \frac{m^2a}{2}\phi''\left(-\frac{b}{a}\right)A + \frac{a}{|a|}m^3 - a^3 = 0.$$

左辺を A の多項式と見て $\psi(A)$ とおく. $1 \leq m \leq |a|-1$ のとき$\psi(A)=0$ が整数解をもたないことを示せばよい. 実際このとき

$$\psi(0)\psi(\pm1) < 0 \quad \text{または} \quad \psi(0)\psi(\pm1) > 0,\ |\psi(\pm1)| > |\psi(0)|$$

かつ

$$\psi\left(-m|a|a\phi'\left(-\frac{b}{a}\right)\right) \neq 0, \quad \psi\left(-m|a|a\phi'\left(-\frac{b}{a}\right)+1\right)\psi\left(-m|a|a\phi'\left(-\frac{b}{a}\right)-1\right) < 0$$

となることが, 以下の証明により示される. まず 0 付近については

$$-a\psi(0) \;=\; a^4 - m^3|a| \;>\; 0$$

となり, $\mathrm{sign}(\psi(0)) = -\mathrm{sign}(a)$ が言え, さらに$\left|\phi'\left(-\frac{b}{a}\right)\right| > 5|gb|$ より

$$\begin{aligned}
&a\phi'\left(-\frac{b}{a}\right)\psi(\pm1)\\
&= a\phi'\left(-\frac{b}{a}\right)\left(\pm1 + m|a|a\phi'\left(-\frac{b}{a}\right) \mp \frac{m^2a}{2}\phi''\left(-\frac{b}{a}\right) + \frac{a}{|a|}m^3 - a^3\right)\\
&= a\phi'\left(-\frac{b}{a}\right)\left(ma^2\left(\frac{|a|}{a} \pm \frac{m}{b}\right)\phi'\left(-\frac{b}{a}\right) \pm m^2b \mp g\frac{m^2a^3}{b^2} \mp \frac{m^2}{b^2} \pm 1 + \frac{a}{|a|}m^3 - a^3\right)\\
&> \left|a\phi'\left(-\frac{b}{a}\right)\right|\left(ma^2\left(1 - \frac{m}{|b|}\right)\phi'\left(-\frac{b}{a}\right) - \left|\pm m^2b \mp g\frac{m^2a^3}{b^2} \mp \frac{m^2}{b^2} \pm 1\right| - \left(|a|^3 - m^3\right)\right)\\
&> \left|a\phi'\left(-\frac{b}{a}\right)\right|\left(ma^2\left(1 - \frac{m}{m+2}\right)5|gb| - 2m^2|gb| - |a|^3\right)\\
&> \left|a\phi'\left(-\frac{b}{a}\right)\right|\left(\frac{10m}{m+2}a^2|gb| - 2m^2|gb| - |a|^3\right)\\
&> \left|a\phi'\left(-\frac{b}{a}\right)\right|\left(3a^2|gb| - 2m^2|gb| - |a|^3\right) \;>\; 0 \text{（復号同順）}
\end{aligned}$$

となり, もし $\phi'\left(-\frac{b}{a}\right) > 0$ ならば $\psi(0)\psi(\pm1) < 0$ が得られ, もし $\phi'\left(-\frac{b}{a}\right) < 0$ ならば $\psi(0)\psi(\pm1) > 0$ となるが, このときは $|\psi(\pm1)| - |\psi(0)| = -\mathrm{sign}(a)(\psi(\pm1) - \psi(0)) > 0$ が同様な計算によって得られる. 次に $-m|a|a\phi'\left(-\frac{b}{a}\right)$ 付近については

$$\begin{aligned}
\left|\psi\left(-m|a|a\phi'\left(-\frac{b}{a}\right)\right)\right| &= \left|\frac{1}{2}m^3|a|^3\phi'\left(-\frac{b}{a}\right)\phi''\left(-\frac{b}{a}\right) + \frac{a}{|a|}m^3 - a^3\right|\\
&> m^3|a|^3\left|\phi'\left(-\frac{b}{a}\right)\right|\left(\left|\frac{a}{b}\phi'\left(-\frac{b}{a}\right)\right| - \left|\frac{b}{a} - g\frac{a^2}{b^2} - \frac{1}{ab^2}\right|\right) - \left|\frac{a}{|a|}m^3 - a^3\right|\\
&> 0
\end{aligned}$$

が得られ, さらに, もし $\phi'\left(-\frac{b}{a}\right) > 0$ ならば

$$\begin{aligned}
&\pm\psi\left(-m|a|a\phi'\left(-\frac{b}{a}\right) \pm 1\right)\\
&= \pm\left(m^2|a^3|\phi'\left(-\frac{b}{a}\right) \mp ma\right)\left\{\pm|a|\phi'\left(-\frac{b}{a}\right) + \frac{m}{2}\phi''\left(-\frac{b}{a}\right)\right\} \pm \left(\frac{a}{|a|}m^3 - a^3\right)\\
&= m\left(m|a|^3\phi'\left(-\frac{b}{a}\right) \mp a\right)\left\{\left(|a| \mp \frac{ma}{b}\right)\phi'\left(-\frac{b}{a}\right) \mp \frac{mb}{a} \pm g\frac{ma^2}{b^2} \pm \frac{m}{ab^2}\right\} \pm \left(\frac{a}{|a|}m^3 - a^3\right)\\
&> m|a|\left(5ma^2|gb| - 1\right)\left\{5\left(|a| \mp \frac{ma}{b}\right)|gb| - \left|\mp\frac{mb}{a} \pm g\frac{ma^2}{b^2} \pm \frac{m}{ab^2}\right|\right\} - |a|(a^2 - m^2)\\
&> m|a|\left(5ma^2|gb| - 1\right) - |a|(a^2 - m^2) \;>\; 0 \text{（復号同順）}
\end{aligned}$$

となり, $\phi'\left(-\frac{b}{a}\right) < 0$ のときも同様となるため, $\psi\left(-m|a|a\phi'\left(-\frac{b}{a}\right) + 1\right)\psi\left(-m|a|a\phi'\left(-\frac{b}{a}\right) - 1\right) < 0$ が得られる. 以上により $1 \leq m \leq |a| - 1$ のとき $\psi(A) = 0$ は整数解をもたないことがわかり,

すなわち $1 \leq m \leq |a|-1$ かつ $\eta_{i,m,n_i}+d \in E_K$ となるような m は存在しないことがわかる. 従って $m_i = |a|$. □

補題 5 $l_i = (a\theta+b)^{-1} - \eta_{i,|a|,n_i}$.

証明 補題 4 より $\eta_{i,|a|,n_i}+l \in S_{i,n_i}$ をとることができる. $l' = (\eta_{i,|a|,n_i}+l)-(a\theta+b)^{-1}$ とおくと $(a\theta+b)^{-1}+l' \in E_K^+$ となり,

$$(a\theta+b)\{(a\theta+b)^{-1}+l'\} = al'\theta+bl'+1 \in E_K^+.$$

よって $N_{K/\mathbf{Q}}(al'\theta+bl'+1)=1$ より

$$l'^2 + a^2\phi'\left(-\frac{b}{a}\right)l' - a\frac{\phi''\left(-\frac{b}{a}\right)}{2} = 0 \quad \text{または} \quad l'=0.$$

左式の左辺を l' の多項式と見て $\psi_2(l')$ とおくと, $\psi_2(l')=0$ の 1 つの解は -1 と 1 の間, もう 1 つの解は $-a^2\phi'\left(-\frac{b}{a}\right)-1 \in \mathbf{Z}$ と $-a^2\phi'\left(-\frac{b}{a}\right)+1$ の間にあることがわかる. なぜなら,

$$\begin{aligned}\psi_2(\pm 1) &= \psi_2\left(-a^2\phi'\left(-\frac{b}{a}\right)\mp 1\right) = \pm a^2\phi'\left(-\frac{b}{a}\right) - a\frac{\phi''\left(-\frac{b}{a}\right)}{2}+1 \\ &= \left(\pm a^2+\frac{a^2}{b}\right)\phi'\left(-\frac{b}{a}\right)+b-\frac{a^3}{b^2}g-\frac{1}{b^2}+1\end{aligned}$$

であり, $\left|\phi'\left(-\frac{b}{a}\right)\right| > 5|b|-1$ より, この符号は $\mathrm{sign}\left(\pm\phi'\left(-\frac{b}{a}\right)\right)$ と一致するから (復号同順).

ところで $\eta_{i,|a|,n_i}+l \in S_{i,n_i}$ より $|l'| \leq |l+1| \leq N_i+1 \leq |b|$ であり, 一方 $\left|-a^2\phi'\left(-\frac{b}{a}\right)\right| > |b|+1$ であるから, $l'=0$ のとき以外に $\eta_{i,|a|,n_i}+l \in S_{i,n_i}$ をみたすことはできないことがわかる. 従って $l_i = (a\theta+b)^{-1}-\eta_{i,|a|,n_i}$. □

補題 6 $\delta_i < \frac{1}{2}$.

証明

$$\begin{aligned}\delta_i &= \frac{1}{|\theta^{(i')}-\theta^{(i'')}|}\left(\frac{1}{|\theta^{(i)}-\theta^{(i')}|}+\frac{1}{|\theta^{(i)}-\theta^{(i'')}|}\right) \\ &< \frac{1}{\left|e-\frac{b}{a}-2\frac{d}{c}\right|-\frac{1}{2a^2}-\frac{1}{c^2}}\left(\frac{1}{\left|e-2\frac{b}{a}-\frac{d}{c}\right|-\frac{1}{a^2}-\frac{1}{2c^2}}+\frac{1}{\left|\frac{b}{a}-\frac{d}{c}\right|-\frac{1}{2a^2}-\frac{1}{2c^2}}\right) \\ &< \frac{1}{\frac{5}{2}|a|}\left(\frac{1}{\frac{5}{2}|c|}+\frac{1}{2}\right) \\ &< \frac{1}{2}.\end{aligned}$$
□

補題 1 から 補題 6 により, 主定理の条件は Grundman の定理の条件をみたすことがわかり, よって $(-1)^i(a\theta+b)^(-1)$ が fundamental C_i unit となる. ある $j(\neq i)$ に対し $(-1)^j(c\theta+d)^(-1)$ が fundamental C_j unit となることも同様に示せ, 従って主定理を得るのである.

4 例を1つ

ここでは, こういったアプローチにより今までに扱われていなかった $b \not\equiv 1 \pmod{a}$ の場合の例を1つ挙げて終りとする.

例 $\phi(x) = x^3 + (b+1)\{(b^2+b+1)t - (b+2)\}x^2 + \{(2b^2+2b+1)t - (2b+3)\}x + bt - 1,\ t \in \mathbf{Z}$ のとき, b に依存する有限個の場合を除けば $\mathfrak{o}_K \cap E_K^+ = \langle (b^2+b+1)\theta + b, (b+1)\theta + 1 \rangle$.

参考文献

[1] W. E. H. Berwick, Algebraic number fields with two independent units, *Proc. London Math. Soc.* 34 (1932), 360-378.

[2] E. Thomas, Fundamental units for orders in certain cubic number fields, *J. Reine Angew. Math.* 310 (1979), 33-55.

[3] H. G. Grundman, Systems of fundamental units in cubic orders, *J. Number Theory* 50 (1995), 119-127.