UBasicによる純3次体のプログラム

— 基本単数，イデアル類群の構造について —

金山茂雄
細谷順二

A Program of Purely Cubic Field by UBasic

− Fundamental Units and the Structure of Ideal Class Group −

Shigeo Kanayama
Junji Hosoya

First we wrote how to get fundamental units and class number of ideal group of purely cubic field $k = Q(\sqrt[3]{m})$. Then we wrote the program. The program was written in UBasic. We got, then, fundamental unit and the structure of ideal class group of purely cubic field $k = Q(\sqrt[3]{m})$, $2 \leq m \leq 2000$. We used the expression (a, b, ..., c) to denote the type of finite abelian group which was the direct product of cyclic groups of order a, b, ..., c $aZ \subset bZ \subset \ldots \subset cZ$.

1．はじめに

有理数体Qに既約多項式$x^3-m=0$の根を添加した体、純3次体$k = Q(\sqrt[3]{m})$の基本単数およびイデアル類群の構造の求めるプログラムについて解説した。プログラムはUBasicという木田祐司氏（立教大学）が数学（教育）研究用に開発した多倍長計算用BASIC言語を使用した。

2．数学的背景

2.1 純3次体についての基本事項

純3次体においては3乗因子をもたない正の有理整数としてよく、互いに素で平方因子をもたない正の有理数f, gで$m = fg^2$の形に表すことができる。
このとき次の定理が知られている。

定理1

純3次体 $k = Q(\alpha), \alpha = \sqrt[3]{m}, m = fg^2$ において、

$d_k(\alpha) = -27m^2$

$M=(\frac{4}{\pi})\frac{3!}{3^3}=\frac{8}{9\pi}$ であり、

(i) $m\equiv\pm1(\mathrm{mod}9)$ でないとき、

整数底 $\left[1,\ \alpha,\ \frac{\alpha^2}{g}\right]$

$d(k)=-27f^2g^2$

$m(\alpha)=g$

$M_k=\frac{8\sqrt{3}}{3\pi}fg$

(ii) $m\equiv\pm1(\mathrm{mod}9)$ のとき、

整数底 $\left[1,\alpha,\frac{1}{3}(1+e_1\alpha+e_2\frac{\alpha^2}{g})\right]$

$f\equiv e_1=\pm1,\ g\equiv e_2=\pm1(\mathrm{mod}3)$

$d(k)=-3f^2g^2$

$m(\alpha)=3g$

$M_k=\frac{8\sqrt{3}}{9\pi}fg$

定理1より次の補題を得る。

補題1

純3次体 $k=Q(\alpha),\alpha=\sqrt[3]{m},m=fg^2$ において

整数底を $[1,\ \alpha,\ \beta]$ とおくとき、

(i) $m\equiv\pm1(\mathrm{mod}9)$ でないとき、

$\alpha^2=g\beta$

$\beta^2=f\alpha$

$\alpha\beta=fg$

(ii) $m\equiv\pm1(\mathrm{mod}9)$ のとき、

$\alpha^2=-e_2g-e_1e_2g\alpha+3e_2g\beta$

$\beta^2=\frac{2e_1e_2fg-e_2g-1}{9}+\frac{f-e_1e_2g}{9}\alpha+\frac{e_2g+2}{3}\beta$

$\alpha\beta=\frac{e_2g(f-e_1)}{3}+\frac{1-e_2g}{3}\alpha+e_1e_2g\beta$

である。

2.2 整イデアルの底の求め方

定理2

純3次体の各イデアル類は

$$NA \leq M_k$$

を満たす整イデアル$A(\neq 0)$を含む。

この定理よりkの類数hを求めるには、ノルムがM_k以下のすべての整イデアルを求め類別すればよいことがわかる。

ノルムがM_k以下の整イデアルを求める方法は次のとおりである。

$p \leq M_k$を満たす有理素数pのkにおける素因子p_iのうち$Np_i \leq M_k$である素因子の集合をPとするとPは

$$P = \{p_i | p_i \in Speck,\ Np_i,\ \leq M_k\}$$

と表せる。Pより整イデアルA_iの集合Aを

$$A = \left\{A_i | A_i = \prod_{p_i \in P} p_j,\ NA_i \leq M_k\right\}$$

のように作ればAがノルムがM_k以下のすべての整イデアルすべての集合である。

次にAを類別する方法を示す。

kの整数底を$[1, \alpha, \beta]$としたとき。整イデアルA_iの底$[\alpha_1, \beta_1, \gamma_1]$として次の形のものを求めることができる。

$$\alpha_1 = a_1$$

$$\beta_1 = b_1 + b_2\alpha$$

$$\gamma_1 = c_1 + c_2\alpha + c_3\beta$$

求める手順は以下のとおりである。

まず素イデアル$p_i \in P$の底を求めるが有理素数pが仮因子であるか否か、即ち$(m(\alpha), p) = 1$であるか否かで方法は大別される。定理1と合わせると次の5つの場合に分けられる。

(i) $m \equiv \pm 1 \pmod 9$でないとき

(a) $(m(\alpha), p) = 1$のとき

(b) $(m(\alpha), p) \neq 1$のとき

(ii) $m \equiv \pm 1 \pmod 9$のとき

(c) $(m(\alpha), p) = 1$のとき

(d) $(m(\alpha), p) \neq 1$のとき

(e) $p = 3$のとき

I $(m(\alpha), p)=1$ であるとき、次の定理が知られている。

定理3

代数体 $k=Q(\alpha)$ において $f(X)\in Z[X]$ を α の Q に関する最小多項式とする。

$(m(\alpha), p)\neq 1$ であるとき、多項式 $f(X)$ の mod$p$ に関する既約多項式への分解が

$f(X)\equiv p_1(X)^{e_1}\cdots\cdots p_g(X)^{e_g}(\mathrm{mod}p)$

$p_1(X)\in Z[X]$ は単多項式

ならば p の k における素因子 p_i は

$p_i=(p, p_i(\alpha))$

となる。そして p_i の次数は多項式 $p_i(X)$ の次数に等しい。

純3次体 $k=Q(\alpha)$ における α の Q に関する最小多項式 X^3-m の mod$p$ に関する既約多項式への分解は

(1) X^3-m は mod$p$ で既約

(2) $X^3-m\equiv(X+a)(X^2+bX+c)(\mathrm{mod}p)$

(3) $X^3-m\equiv(X+a)(X+b)(X+c)(\mathrm{mod}p)$

のいずれかであり、定理3より。

(1) のとき

p は単項イデアルであり、イデアルの類別という点では考えなくてよいイデアルである。

(2) のとき

$(p)=p_1p_2$

$p_1=(p, \alpha+a)$, $p_2=(p, \alpha^2+b\alpha+c)$

$Np_1=p$, $Np_2=p^2$

(3) のとき

$(p)=p_1p_2p_3$

$p_1=(p, \alpha+a)$, $p_2=(p, \alpha+b)$, $p_3=(p, \alpha+c)$

$Np_1=Np_2=Np_3=p$

である。

(a) $m\equiv\pm1(\mathrm{mod}9)$ でなく $(m(\alpha), p)=1$ のとき

(イ) $p_i(\alpha)$ が1次因子のとき

$p_i(\alpha)=\alpha+a$ とすると、$p_i=(p, \alpha+a)$ であるから、p_i を k の整数底 $[1, \alpha, \beta]$ で表したときの生成元は定理1，補題1より

$p=p$

$p\alpha = p\alpha$

$p\beta = p\beta$

$a+\alpha = a+\alpha$

$a\alpha+\alpha^2 = a\alpha+g\beta$

$a\beta+\alpha\beta = fg+a\beta$

である。従って行列Mを

$$M=\begin{pmatrix} p & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & p \\ a & 1 & 0 \\ 0 & a & g \\ fg & 0 & a \end{pmatrix}$$

としてMに行に関する基本変形をほどこすとことによって、素イデアルpの底$[\alpha_1, \beta_1, \gamma_1]$として次の形のものを求めることができる。

$\alpha_1 = a_1$

$\beta_1 = b_1+b_2\alpha$

$\gamma_1 = c_1+c_2\alpha+c_3\beta$

（ロ）$p_i(\alpha)$が2次因子のとき

$p_i(\alpha) = \alpha^2+b\alpha+c$として（イ）と同様にすると

$$M=\begin{pmatrix} p & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & p \\ c & b & g \\ m & c & bg \\ bfg & fg & c \end{pmatrix}$$

を得る。

(c) $m \equiv \pm 1 \pmod 9$で$(m(\alpha), p) = 1$のとき

（イ）$p_i(\alpha)$が1次因子のとき

同様にして、

$$M=\begin{pmatrix} p & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & p \\ a & 1 & 0 \\ -e_2g & a-e_1e_2g & 3e_2g \\ \frac{1}{3}e_2g(f-e_1) & \frac{1}{3}(1-e_2g) & a+e_1e_2g \end{pmatrix}$$

を得る。

（ロ） $p_i(\alpha)$ が2次因子のとき

同様にして、

$$M=\begin{pmatrix} p & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & p \\ c-e_2g & b-e_1e_2g & 3e_2g \\ m-be_2g & c-be_1e_2g & 3be_2g \\ \frac{1}{3}\{be_2g(f-e_1)+e_1m-e_2g\} & \frac{1}{3}\{b(1-e_2g)+e_2fg-e_1e_2g\} & c+be_1e_2g+e_2g \end{pmatrix}$$

を得る。

II $(m(\alpha), p)\neq 1$ であるとき次の定理が知られている。

定理4

k を代数体とする。環準同型 φ

$\varphi: O_F\to \widetilde{F_P}$（$F_P=Z/pZ$ の代数閉包）

$\varphi|_Z=\varphi_0$（$\varphi_0: Z\to F_p$ は自然準同型）

の同値類を次のように定義する。

$\varphi_1\sim\varphi_2\Leftrightarrow$ 体 $\varphi_1(o_k)$ から体 $\varphi_2(o_k)$ への同型 ρ で $\rho o\varphi_1(\alpha)=\varphi_2(\alpha)(\forall\alpha\in o_k)$ となるものが存在する。

このとき、p の k における素因子と環準同型の同値類とは $p=Ker\varphi$ なる関係により1対1に対応する。

(b) $m\equiv\pm1(\mathrm{mod}9)$ でなく $(m(\alpha), p)\neq 1$ のとき

定理4より φ は $\varphi|_z=\varphi_0$, $\varphi(\alpha)$, $\varphi(\beta)\in\widetilde{F_P}$ により一意的に決まり補題1などより $\varphi(\alpha)=\varphi(\beta)=0$ であるから、$p=Ker\varphi=[p, \alpha, \beta]$ となる。

(d) $m \equiv \pm 1 (\mathrm{mod}9)$ で $(m(\alpha), p) \neq 1$ のとき

同様にして $3\varphi(\beta)-1 \equiv 0(\mathrm{mod}p)$ を得るから、

1次合同式 $3X \equiv 1(\mathrm{mod}p)$ の解を x_0 として $p = [p, \alpha, \beta - x_0]$

(e) $m \equiv \pm 1(\mathrm{mod}9)$ で $p = 3$ のとき

同様にして2次合同式

$$X^2+AX+B \equiv 0(\mathrm{mod}3)$$

$$A = -\frac{1}{3}(e_2g+2)$$

$$B = -\frac{1}{9}(2e_1e_2fg-2e_2g+e_1f-1)$$

を得るが、$A' \equiv A$, $B' \equiv B(\mathrm{mod}3)$, A', $B' = \pm 1$ として f, g, A', B' の関係は

$f \equiv \pm 1(\mathrm{mod}9) \Rightarrow A' = -1, B' = 0$

$f \equiv \pm 2(\mathrm{mod}9) \Rightarrow A' = 0, B' = -1$

$f \equiv \pm 4(\mathrm{mod}9) \Rightarrow A' = 1, B' = 0$

となるから3の k における分解を

$(3) = p_1p_2^2$ または $p_1^2p_2$

$Np_1 = Np_2 = 3$

として

$f \equiv \pm 1(\mathrm{mod}9) \Rightarrow p_1 = [3, \alpha - e_1, \beta]$, $p_2 = [3, \alpha - e_1, \beta - 1]$

$f \equiv \pm 2(\mathrm{mod}9) \Rightarrow p_1 = [3, \alpha - e_1, \beta + 1]$, $p_2 = [3, \alpha - e_1, \beta - 1]$

$f \equiv \pm 4(\mathrm{mod}9) \Rightarrow p_1 = [3, \alpha - e_1, \beta]$, $p_2 = [3, \alpha - e_1, \beta - 1]$

となる。

以上よりすべての素イデアル $p_i \in P$ について

$$\alpha_1 = a_1$$

$$\beta_1 = b_1 + b_2\alpha$$

$$\gamma_1 = c_1 + c_2\alpha + c_3\beta$$

の形の底 $[\alpha_1, \beta_1, \gamma_1]$ が求まる。

そして、2つのイデアルの底がそのように表されているとき、それらのイデアルの積についても、素イデアルを求めたのと同様に行列Mを作り、行に関する基本変形をほどこすことによって同じ形の底を求められるから、すべての整イデアル A_i の底について

$$\alpha_1 = a_1$$

$$\beta_1 = b_1 + b_2\alpha$$

$$\gamma_1 = c_1 + c_2\alpha + c_3\beta$$

の形の底 $[\alpha_1, \beta_1, \gamma_1]$ が求まる。

3．正規底と極小元

k の元 $\alpha(\in R)$ に対し、その共役を α', α'' とすると $\alpha''=\overline{\alpha'}$ (複素共役)である。

写像 $\varphi: \alpha(\in R)\alpha \quad \vec{\alpha}=(\alpha, \mathrm{Re}(\alpha'), \mathrm{Im}(\alpha'))(\in R^3)$

によって、R^3 に埋め込む。

このとき k の整イデアル A の元 α に対し

$$|\beta|<|\alpha|, \ |\beta'|<|\alpha'|$$

をみたす A の元が (0) 以外に存在しないとき、α を A の極小元といい、

$$\alpha \in M(A)$$

と表す。また k の元 α に対し、円柱 U_α, C_α を

$$U_\alpha=\left\{(x, y, z)\,|\,|x|<|\alpha|, \ y^2+z^2<|\alpha'|^2\right\}$$

$$C_\alpha=\left\{(x, y, z)\,|\,x>\alpha, \ y^2+z^2<|\alpha'|^2\right\}$$

と定義すると円柱 U_α の内部に k の整イデアル A の元全体の像が作る3次元 Lattice $L_3(\alpha)$ の元は原点以外存在しない。

前記の方法で k の整イデアル A の底を求めたとき底の交換によって

$$A=[\alpha_0, \beta_0, \gamma_0], \ \alpha_0 \in M(\alpha)$$

の形の底を求めることが次の目標である。

補題2

写像 φ による整イデアル A の元 $\delta=p+q\alpha+r\beta$ の像は

(i) $m \equiv \pm 1 \pmod 9$ でないとき

$$\left(p+q\alpha+r\beta, \ p-\frac{1}{2}q\alpha-\frac{1}{2}r\beta, \ \frac{\sqrt{3}}{2}(q\alpha-r\beta)\right)$$

(ii) $m \equiv \pm 1 \pmod 9$ のとき

$$(p+q\alpha+r\beta, \ y, \ z)$$

$$y=p-\frac{1}{2}q\alpha+\frac{1}{3}r-\frac{1}{6}re_1\alpha-\frac{1}{6}re_2\frac{\alpha^2}{g}$$

$$z=\frac{\sqrt{3}}{2}\left(q\alpha+\frac{1}{3}re_1\alpha-\frac{1}{3}re_2\frac{\alpha^2}{g}\right)$$

である。

kの整イデアルAAの底$[\alpha_1, \beta_1, \gamma_1]$を

写像$\lambda:(x, y, z)(\in R^3)\alpha\ (x-y, z)(\in R^2)$

により2次元Lattice L_2 に射影する。このときL_2の生成元$\vec{b}=(b_x, b_z)$, $\vec{c}=(c_x, c_z)$が与えられたとき、底の変換によって次の性質をもつように変形することができる。

(i) $0<b_x, |b_z|<\frac{1}{2}$

(ii) $0<d_x<b_x, |d_x|<\frac{1}{2}$となる$L_2$の元$\vec{d}=(d_x, d_z)$は存在しない。

(iii) $0<c_x<b_x$

(iv) $0<d_x<b_x, |d_z|<|c_z|$となるL_2の元$\vec{d}=(d_x, d_z)$は存在しない。

これらの条件をみたす底を正規底と呼ぶことにする。

変形の手順は以下のとおりである。

まずL_2の生成元$\vec{b}=\vec{b_1}$, $\vec{c}=\vec{c_1}$が与えられたとき、

$$b_z c_z>0, |b_z|>\frac{1}{2}, |c_z|>\frac{1}{2}\ (*)$$

満たしていないならば

$$k_i=\left[-\frac{c_{ix}}{b_{ix}}\right]$$

に対し、

$$\vec{b_{i+1}}=\vec{c_i}+k_i\vec{b_i}$$
$$\vec{c_{i+1}}=\vec{b_i}$$

という操作を繰り返し(*)を満たすように変形できる。

補題3

写像$\lambda o\varphi$による整イデアルAの元$\delta=p+q\alpha+r\beta$の像は

(i) $m\equiv\pm1(\mathrm{mod}9)$でないとき

$$\left(\frac{3}{2}(q\alpha+r\beta), \frac{\sqrt{3}}{2}(q\alpha-r\beta)\right)$$

(ii) $m\equiv\pm1(\mathrm{mod}9)$のとき

$$\left(\frac{1}{2}(3q\alpha+re_1\alpha+re_2\frac{\alpha^2}{g}), \frac{\sqrt{3}}{2}(q\alpha+\frac{1}{3}re_1\alpha-\frac{1}{3}re_2\frac{\alpha^2}{g})\right)$$

である。

kの整イデアルAの極小元α_0を次のようにして1つ求める。

$r>0$, $r\in Q$に対し

集合 $U_\alpha(A)=\{\alpha_i|\overrightarrow{\alpha_i}\in L_3(A)\cap U_r,\ \alpha>0\}$

とするとき、

$$\alpha_0=\min_i\{\alpha_i|\alpha_i\in U_r(A)\}$$

はAの極小元である。従って 極小元をもとめるには$U_r(A)$の元から探すことができるがrを小さくすると円柱U_rの体積が小さくなり集合$U_r(A)$の元の数が減り探しやすくなるが小さすぎると$U_r(A)=\emptyset$となってしまう。適当なrを定めるためにミンコフスキーの定理を純3次体に応用して次の系を得る。

系

純3次体の整イデアルAの底を$[\alpha_1,\ \beta_1,\ \gamma_1]$,

$\alpha_i\in R$としα_i', α_i''をその共役とする。また3つの1次形式を

$$f_1=a\alpha_1+b\alpha_2+c\alpha_3(=x)$$

$$f_2=a\alpha_1'+b\alpha_2'+c\alpha_3'(=y+zi)$$

$$f_3=a\alpha_1''+b\alpha_2''+c\alpha_3''(=y-zi)$$

$$\Delta=|d(\alpha_1,\ \beta_1,\ \gamma_1)|^{\frac{1}{2}}=NA|d(k)|^{\frac{1}{2}}$$

とする。

このとき正の実数rを$r^3=\Delta$と定めると、

$$|f_i|<r(n=1,\ 2,\ 3)$$

は0と異なる有理整数解をもつ。

この系と$L_3(A)$が原点対称であることにより、円柱U_rにおいてrを$r^3=NA|d(F)|^{\frac{1}{2}}$を満たすように定めると、円柱$U_r$に$L_3(A)$の0と異なる元が少なくとも1つ存在する。

集合$U_r(A)$の元を$\vec{r}=(r,\ r,\ 0)$に平行に$x-z$平面に射影すると領域Sを

$$x^2+y^2\leq r^2(x\leq 0)$$

$$-r\leq z\leq r(0<x\leq r)$$

$$(x-r)^2+z^2\leq r^2(r<x)$$

としてSに含まれる。したがってL_3の極小元で射影するとSに含まれるものが必ず存在する。従ってSに含まれるL_2の元をすべて求め$U_r(A)$の最小元として極小元を求めることができる。

L_2の正規底$\vec{b}$, $\vec{c}$として

$$\vec{d}=m\vec{b}+n\vec{c}(m,\ n\in Z)$$

と表したとき、

$$\vec{d} \in S$$

となる必要条件を考える。

$\vec{b}, \vec{c}$ に平行でSに接する4直線 $l_i (i = 1, 2, 3, 4)$ でかこまれた領域をTとすると

$$m\vec{b} \notin T \text{ または } n\vec{c} \notin T \Rightarrow \vec{d} \notin S$$

であるから

$$m_1 \leq m \leq m_2 \Leftrightarrow m\vec{b} \in T$$

$$n_1 \leq n \leq n_2 \Leftrightarrow n\vec{c} \in T$$

$$m_1 = \left[\frac{|\vec{c}|re}{b_x c_z - b_z c_x}\right] + 1$$

$$m_2 = \left[\frac{c_z - |\vec{c}|e}{b_x c_z - b_z c_x} r\right]$$

$$n_1 = \left[\frac{|\vec{b}|re}{b_x c_z - b_z c_x}\right] + 1$$

$$n_2 = \left[\frac{-b_z - |\vec{b}|e}{b_x c_z - b_z c_x} r\right]$$

について $\vec{d} \in S$ かどうか判定する。このようにして求めた L_2 の元 $\vec{d} = (d_x, d_z)$ に対し、$L_3(\alpha)$ の元 $\vec{\delta} = (\delta_x, \delta_y, \delta_z)$ で

$$\lambda(\vec{\delta}) = \vec{d} \quad (**)$$

を満たす格子点の集合は $\vec{\alpha_1} = (a_1, a_1, 0)$ と平行な直線上に並ぶから(＊＊)を満たす $\vec{\delta}$ を1つでも求められれば

$$\vec{\delta_i} = \vec{\delta} + k_i \vec{\alpha_1} (k_i \in Z)$$

によって直線上を移動させ探せる。

$$\vec{d} = \lambda(m(p\vec{\beta_1} + q\vec{\gamma_1}) + n(r\vec{\beta_1} + s\vec{\gamma_1}))$$

であるから正規底を求める連分数展開において変換した底 $\vec{b'}, \vec{c'}$ を $\vec{b}, \vec{c}$ で表したときの係数をその都度計算しておき、p, q, r, s をもとめれば（＊＊）を満たす $\vec{\delta} \in L_3(A)$ として、

$$\vec{\delta} = (mp + nr)\vec{\beta_1} + (mq + ns)\vec{\gamma_1}$$

を定めることができる。

k の整イデアルAの極小元 α_0 が求まったとき、

$$A = [\alpha_0, \beta_0, \gamma_0], \alpha_0 \in M(A)$$

の形の底を求める。

$\alpha_0 = l\alpha_1+m\beta_1+n\gamma_1,\ l,\ m,\ n \in Z$

としたとき、

$$\begin{pmatrix}\alpha_0\\ \beta_0\\ \gamma_0\end{pmatrix} = \begin{pmatrix}l & m & n\\ p & q & r\\ s & t & u\end{pmatrix}\begin{pmatrix}\alpha_1\\ \beta_1\\ \gamma_1\end{pmatrix}$$

として $p,\ q,\ r,\ s,\ t,\ u$ を次のように求める。

（i）$l \neq 0$ または $m \neq 0$ のとき

$r = 0$ としても求められることを示す。

$l' = l/d,\ m' = m/d,\ d = (l,\ m)$ として $p,\ q$ を

$l'q-m'p = 1$

の解として求める。

また $v = \begin{vmatrix}p & q\\ r & s\end{vmatrix}$ として $u,\ v$ を

$nv+ud = 1$

の解として求める。このとき

$s = l'v,\ t = m'v$

とすると、$pt-qs = v$ である。

（ii）$l = m = 0$ のとき

$n = \pm 1$ であるから

$p = 0,\ q = 1,\ r = 0,\ s = 1,\ t = 0,\ u = 0$

とすればよい。

4．基本単数とイデアル類群

極小元 α_0 を含むイデアル A の底

$A = [\alpha_0,\ \beta_0,\ \gamma_0]\alpha_0 \in M(A)$

が求まったとする。このとき極小元を含む A の底の列を

$A(i) = \{(\alpha_i,\ \beta_i,\ \gamma_i) \mid [\alpha_i,\ \beta_i\gamma_i],\ \alpha_i$ は $\overrightarrow{\alpha_i} \in C_{\alpha_{i-1}} \cap L_3(A)$ を満たす最小の元$\}$

によって作る。このとき、α_i を 1 に移す写像 ϕ_{α_i} を

$\phi_{\alpha_i} : x(\in A)\alpha\ \dfrac{x}{\alpha_i}(\in k)$

とすると、$L_3(A)$ は $\vec{1}$, $\phi_{\alpha_i}(\vec{\beta_i})$, $\phi_{\alpha_i}(\vec{\gamma_i})$ を生成元の1組とする3次元 Lattice $L_3'(A)$ になる。このとき $x, y \in k$ として

$$\vec{x} \in C_y \Leftrightarrow \phi_{\alpha_i}(\vec{x}) \in C_{y'},\ \vec{y'} = \varphi_{\alpha_i}(\vec{y})$$

が成り立つ。極小元を求めたときと同様にすべての元を $\vec{1} = (1, 1, 0)$ に平行に $x-z$ 平面上に射影する。正規化された底を $\vec{b}$, $\vec{c}$ とすると、

$$\lambda o \phi_{\alpha_i}(\vec{\alpha}_{i+1}) \in B = \left\{\vec{b},\ \vec{c},\ \vec{b}-\vec{c},\ \vec{b}+\vec{c},\ 2\vec{b}+\vec{c}\right\}$$

となるから、$\vec{\alpha}_{i+1}$ を求めるには

$$\vec{\delta} = (\delta_x, \delta_y, \delta_z) \in L_3'(A) \cap C_1$$

として

$$\lambda(\vec{\delta}) \in B$$

となる元のうち δ_x が最小となるものを求めればよい。

$$A(i+1) = (\alpha_{i+1}, \beta_{i+1}, \gamma_{i+1})$$

を次のように求める。

β', γ' を $\lambda o \phi_{\alpha_i}(\vec{\beta'}) = \vec{b}$, $\lambda o \phi_{\alpha_{i+21}}(\vec{\gamma'}) = \vec{c}$ を満たす A の元として

(i) $\vec{b'} = \vec{b}$ のとき

$$(\alpha_{i+1}, \beta_{i+1}, \gamma_{i+1}) = (\alpha_{i+1}, \gamma', \alpha_i)$$

(ii) $\vec{b'} \in \left\{\vec{c},\ \vec{b}-\vec{c},\ \vec{b}+\vec{c},\ 2\vec{b}+\vec{c}\right\}$ のとき

$$(\alpha_{i+1}, \beta_{i+1}, \gamma_{i+1}) = (\alpha_{i+1}, \beta', \alpha_i)$$

このようにして極小元を含む A の底の列を決めていくと作り方から A(0) を決めれば一意的に決まっていく。

このとき、円柱 C_{α_i} は内部に原点以外に格子点を含まない原点対称の凸形であるから、ミンコフスキーの定理より C_{α_i} の体積はある一定の値以下である。従って単項イデアルは有限個しか異なるものがない。従って

$$(\alpha_0) = (\alpha_n),\ (\alpha_0) \neq (\alpha_i)(i = 1, 2, \ldots, n-1)$$

を満たす n が存在する。

このとき、$\dfrac{\alpha_n}{\alpha_0}$ は k の単数であり k の基本単数を ε_0 として

$$\frac{\alpha_n}{\alpha_0} = \varepsilon_0^l$$

とおくと、$(\varepsilon_0\alpha_0)=(\alpha_0)$ より $l=1$ である。即ち、

$$\varepsilon_0=\frac{\alpha_n}{\alpha_0}$$

である。従って任意の $i(\geq 0)$ に対し

$$\alpha_{n+i}=\varepsilon_0\alpha_i$$

であるから、単数の差を無視すれば

$$\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$$

は M(A) の元のすべてである。そして 整イデアル A の極小元の比の集合

$$\left\{\frac{\alpha_1}{\alpha_0}, \frac{\alpha_2}{\alpha_1}, \ldots, \frac{\alpha_n}{\alpha_{n-1}}\right\}$$

は A の属するイデアル類の不変量である。

5．おわりに

以上より、類数を求めるには各イデアルについてこの不変量を求め同じ類に属するかどうかを調べて数えればいいことがわかる。また、イデアル類群の構造を決定するには、各イデアル類よりなるべくノルムの小さい整イデアルを代表元として選び、イデアルの積について同様の比の列を作り初項がどのイデアル類に入るかを調べればよいことがわかる。尚、実際のプログラムリストは省略する。

<参考文献>

[1] 細谷 順二「純3次体の基本単数とイデアル類群の計算法」1991年度上智大学修士論文集 1992。

[2] 和田 秀男「整数論への計算機の応用」上智大学数学講究録No.7 1980。

[3] 和田 秀男「コンピュータと素因子分解」遊星社，1987。

[4] 藤崎 源二郎「代数的整数論入門 上・下」裳華房，1975。

[5] 新井 正夫「3次体の整数底を求める一方法」Ⅰ・Ⅱ学習院女子部論叢第2号（1977），第3号（1978）。

[6] J. Hosoya, H. Wada, "Tables of Ideal Class Group of Purely Cubic Fields", Proceeding of the Japan Academy, Vol.68 SerA, No5, 1992.

[7] H.Wada, "A table of fundamental units of purely cubic fields", Proceeding of the Japan Academy, Vol.46, SerA, 1970.

[8] K. Nakamula, "A table for pure cubic fields", Advanced Studies in Pure Mathematics 13, Investigation in Number Theory, 1988.