資　料

2 次数体のイデアル群の計算法*

片　山　　茂**

Abstract

This is a study of the method for computing a basis and invariant-series of the ideal group of quadratic number fields.

Some numerical examples to test the validity of our method are given.

1. まえがき

2次体のイデアル類群については，和田[1]による虚2次体 $Q(\sqrt{-m})$，$0<m<24000$ の“trivial”でない非巡回のものの不変系の表，Lakein[2]による実2次体 $Q(\sqrt{p})$，$p\equiv 1 \pmod 4$，$p\leqq 2776817$ の素数，の非巡回のものの不変系の報告などがあるが，その計算の方法は示されていない***，情報処理の立場からは，その方法に興味があると思われる．本稿で，不変系だけでなく，1組の底も求める，筆者の方法を紹介し，その実験の結果を報告する．

2. 類数と類代表イデアル

Z を有理整数環とする．2次体 $Q(\sqrt{m})$ の整数環は $[1,\omega]$，ここに $m\not\equiv 1 \pmod 4$ のとき $\omega=\sqrt{m}$，$m\equiv 1 \pmod 4$ のとき $\omega=(1+\sqrt{m})/2$ とする．また $Q(\sqrt{m})$ の（整）イデアルは $[a, b+c\omega]$ $(a>0, b, c\in Z)$ の形にかけ，さらに

$$[a, b+c\omega]=c[a_0, b_0+\omega]$$

となる．$[a, r+\omega]$ の形のイデアルを原始イデアルという．$(r\in Z)$

補題 S[3]　$(a, r+\omega)^{****}=[a, r+\omega]^{****}\Leftrightarrow a\mid N(r+\omega)$

イデアル A，B が，$A=\lambda B$ $(0\neq\lambda\in Q(\sqrt{m}))$ となるとき対等であるといい，$A\sim B$ で表わす，この関係は同値律をみたし，イデアルを類に分ける．この類の数が類数である．

定理 O[3]　原始イデアル $A=[a, r+\omega]$，$B=[b, s+\omega]$ で $\xi=(r+\omega)/a$，$\eta=(s+\omega)/b$ とおくとき，

$$A\sim B\Leftrightarrow \xi=\frac{l\eta+m}{p\eta+q},\quad \begin{vmatrix} l & m \\ p & q \end{vmatrix}=\pm 1$$

$$(l,\ m,\ p,\ q\in Z)$$

定理 I[3]　任意の複素数は基本区域

$$(G)\quad -\frac{1}{2}\leqq x<\frac{1}{2},\ |z|\geqq 1\ \left(|z|=1 \text{ ならば } -\frac{1}{2}\leqq x\leqq 0\right)$$

に属するある複素数 $z=x+yi$ $(x,\ y$ 実数$)$ と対等であり，G に属する2数は対等*****でない．

定理 R[3]　与実2次体 $Q(\sqrt{m})$ に属する2次無理数は $Q(\sqrt{m})$ に属する簡約された2次無理数と対等である．

ここに2次無理数 ω が簡約されているとは，ω とそれと共役な ω' とに関して，

$$\omega>1,\ 0>\omega'>-1$$

であるときのことである．従ってこの**定理 R** の主張することは，2次無理数 ω を連分数展開すると，ある終項 ω_n に至って，

$\omega=(l\omega_n+m)/(p\omega_n+q)$，$lq-mp=\pm 1$ において

$$\omega_n>1,\ 0>\omega_n'>-1\quad (l, m, p, q\in Z)$$

の成り立つことである．また ω_n が簡約されていればその番号以上のすべての終項は簡約されていることも容易に分る．

---

* A Method for Computing the Ideal Class Group of Quadratic Number Fields by Shigeru KATAYAMA (Laboratory of Mathematics, Faculty of Education, Tottori University).

** 鳥取大学教育学部数学教室

*** 本稿実験中に和田氏から和田[1]の計算方法の連絡を受けたが本稿はそれと別の方法であるので紹介する．

**** $(\alpha_1, \alpha_2)=\{\xi\alpha_1+\eta\alpha_2 \mid \xi, \eta\in Q(\sqrt{m})$ の整数$\}$
$[\alpha_1, \alpha_2]=\{x\alpha_1+y\alpha_2 \mid x, y\in Z\}$

***** 2つの数 z_1，z_2 において，

$$z_2=\frac{lz_1+m}{pz_1+q},\quad \begin{vmatrix} l & m \\ p & q \end{vmatrix}=\pm 1\quad (l, m, p, q\in Z)$$

のとき z_1，z_2 は対等という．

定理 R′[3] 与実2次体 $Q(\sqrt{m})$ に属する簡約された2次無理数の数は有限である.

定理 R″[3] 簡約された2次無理数は純循環連分数に展開される.

以上から

虚2次体の場合 定理 O, I から, 与虚2次体 $Q(\sqrt{m})$ のイデアル $[a, r+\omega]$ はその2次無理数 (複素数) $(r+\omega)/a$ が G に属するものが代表イデアルで, その個数が類数である, これは2次無理数 $(r+\omega)/a$ の G に属する条件を, ある組合せの個数の問題として解ける[4].

実2次体の場合 定理 O, R から, 与実2次体 $Q(\sqrt{m})$ のイデアル $[a, r+\omega]$ からの2次無理数 $(r+\omega)/a$ はある $Q(\sqrt{m})$ の簡約された2次無理数と対等であるから, $Q(\sqrt{m})$ に属するすべての簡約された2次無理数を求め——**定理 R′** から可能——その中で対等でないものの個数が類数で, それに対応するイデアルが代表イデアルである[5].

3. 代表イデアルの位数

代表イデアルの位数をしらべるには, 代表イデアルは原始イデアルで表わしてあるから, 先ずその積と対等な原始イデアルを求め, 次にそれを簡約する方法がわかればよい.

3.1 代表イデアルの積

次の定理が成り立つ.

定理 $A=[a, r+\omega]$, $B=[b, s+\omega]$ を代表イデアルとする.

(1) $\omega=\sqrt{m}$ のとき,

$d_1=ax+by+(r+s)z$, $((a, b, (r+s))^*=d_1,\ x, y, z\in Z)$, $e_1=asx+bry+(rs+m)z$

とおく,

(2) $\omega=(1+\sqrt{m})/2$ のとき,

$$d_1=ax+by+(r+s+1)z$$
$$((a, b, (r+s+1))=d_1,\ x, y, z\in Z)$$
$$e_1=asx+bry+(rs+(m-1)/4)z$$

とおくとき, いずれの場合も

$$AB\sim[ab/d_1^2, (e/d_1)+\omega]$$

証明 $AB=[ab, a(s+\omega), b(r+\omega), rs+(r+s)\omega+\omega^2]$

$\omega=\sqrt{m}$ のとき, $rs+(r+s)\omega+\omega^2=rs+m+(r+s)\omega$

$$(a, b, r+s)=d_1\Rightarrow\exists x,\ y,\ z\in Z,\quad d_1=ax+by+(r+s)z$$

となる.

$$e=asx+bry+(rs+m)z$$
$$=s(ax+by+(r+s)z)-bsy+bry-s^2z+mz$$
$$=sd_1+by(r-s)+z(m-s^2)$$
$$=d_1\left(s+\frac{b}{d_1}(r-s)y+\frac{m-s^2}{d_1}z\right)\quad ☆$$

$d_1|b$, $b|(m-S^2)$(補題 S)$\Rightarrow d_1|(m-s^2)\Rightarrow d_1|e$

従って

$$AB=\left[ab, a\left(s-\frac{e}{d_1}\right), b\left(r-\frac{e}{d_1}\right), rs+m-(r+s)\frac{e}{d_1}, e+d_1\omega\right]$$

と変形されて,

☆から $\dfrac{b}{d_1}\left|s-\dfrac{e}{d_1}\right.$,

同様に $\dfrac{a}{d_1}\left|r-\dfrac{e}{d_1}\right.$,

また,

$$rs+m-(r+s)(e/d_1)$$
$$=[(rs+m)(ax+by+(r+s)z)-(r+s)(asx+bry+(rs+m)z)]/d_1$$
$$=[ax(m-s^2)+by(m-r^2)]/d_1$$

従って $(ab/d_1)|(rs+m-(r+s)(e/d_1))$

故に

$$AB=[ab/d_1,\ e+d_1\omega]=d_1[ab/d_1^2,\ e/d_1+\omega]$$
$$\sim[ab/d_1^2,\ (e/d_1)+\omega]$$

$\omega=(1+\sqrt{m})/2$ の場合も同様して成り立つことがわかる.

3.2 原始イデアルの簡約

3.1 によって得られた, 積と対等な原始イデアル $[ab/d_1^2, (e/d_1)+\omega]$ がさらに, どの代表イデアルと対等であるかをみる, 以下記号をあらため $[a, r+\omega]$ で考察する.

虚2次体の場合 定理 I によって $[a, r+\omega]$ に対する $(r+\omega)/a$ が G のどの数と対等かをみればよい. それには, 高木[3]の「モ変形」S, T に相当する次の変換を繰返すことによって対等数に到達する.

S 変換 $\omega=\sqrt{-m}(m>0)$ のとき,

$$\frac{r+\omega}{a}=\frac{r}{a}+\frac{\omega}{a},\ \frac{r}{a}\ を\ -\frac{1}{2}\leqq\frac{r}{a}<\frac{1}{2},$$

$\omega=(1+\sqrt{-m})/2$ $(m>0)$ のとき,

$$\frac{r+\omega}{a}=\frac{2r+1}{2a}+\frac{\sqrt{-m}}{2a},\ \frac{2r+1}{2a}\ を\ -\frac{1}{2}\leqq\frac{2r+1}{2a}$$

---

* 最大公約数

$<\frac{1}{2}$,

にそれぞれ変換する——それには mod a で余りを出し，あと適当に $\pm a$ によって処理する．

T 変換　$T\left(\frac{r+\omega}{a}\right)=\frac{-a}{r+\omega}$

$\omega=\sqrt{-m}$ $(m>0)$ のとき，

$\left(\frac{r+\omega}{a}\right)\left(\frac{r+\bar{\omega}}{a}\right)=\frac{r^2+m}{a^2}$, $\alpha=\frac{r^2+m}{a}$ とおくと，

$$T\left(\frac{r+\omega}{a}\right)=\frac{-a}{r+\omega}=\frac{-r+\omega}{\alpha}.$$

対応するイデアルは $[\alpha, -r+\omega]$.

$\omega=(1+\sqrt{-m})/2$ $(m>0)$ のとき，

$$\left(\frac{r+\omega}{a}\right)\left(\frac{r+\bar{\omega}}{a}\right)=\frac{(2r+1)^2+m}{4a}\cdot\frac{1}{a},$$

$\alpha=((2r+1)^2+m)/4a$ とおくと，

$$T\left(\frac{r+\omega}{a}\right)=\frac{-a}{r+\omega}=\frac{-(2r+1)+\sqrt{-m}}{2\alpha}=\frac{-r-1+\omega}{\alpha}.$$

対応するイデアルは $[\alpha, -r-1+\omega]$ このプログラムはサブルーチン MATRIX と COMPAR である．

実2次体の場合　定理 R によって，2次無理数 $(r+\omega)/a$ を連分数展開すると，いつか終項に簡約された2次無理数が表われるから，**定理 R″** から，その循環節を一巡する間に必ず代表イデアルの表示に対応する簡約された2次無理数が表われるはずである．このプログラムはサブルーチン KETT 2．

以上のように虚，実ともに始めの原始イデアルが，どの代表イデアルと対等かがわかり，積が確定する．特に単項イデアル $[1, \omega]$ と対等であるとき，その巾指数がその代表イデアルの位数である．

4. 直積因子の決定

イデアル類群は代表イデアルを元として，有限アーベル群である．これを G で表わし，位数を h とする．

定義[6]　アーベル群 G の部分群を $A_1, A_2, \cdots, A_n, e$ を単位元として

1) $G=A_1A_2\cdots A_n$;

2) $(A_1A_2\cdots A_{i-1})\cap A_i=\{e\}$ $(i=2, 3, \cdots, n)$

であるとき，G は $A_1, A_2, \cdots, A_n$ の直積であるという．$A_1, A_2, \cdots, A_n$ を直接因子という．直接因子の決定には次の定理に拠る．

定理 D[6]　G の元の中で位数最大のものの一つを a とすると，a によって生成される巡回群 $\langle a\rangle$ は G の直積因子の一つである．

なお各元の位数，各元の巾の値（**3.**）を援用する．以下 G は非巡回群とする．

第1因子　位数の最大の元の一つ a_1 を選ぶと，**定理 D** によって $\langle a_1\rangle$ は直積因子である．a_1 の位数を l_1 とする．

第2因子　$(l_1, h/l_1)=d_1$ とおく，G の元 $a_2(\neq a_1)$ を次の3条件をみたすように選ぶ．

（1）　a_2 の位数 l_2 は d_1 または d_1 の約数，

（2）　$\langle a_1\rangle\cap\langle a_2\rangle=\{e\}$,

（3）　条件（1），（2）をみたし，l_2 の最大のもの．このとき $\langle a_1\rangle\langle a_2\rangle$ は定義から直積である．

これには d_1 とその約数の大きいものから（2）の条件をチェックすればよい．（2）については，もし

$$\langle a_1\rangle\cap\langle a_2\rangle\neq\{e\}\ \text{即}$$

$$\text{☆}\quad a_1^x=a_2^y\neq e\ (x, y\in\boldsymbol{Z})$$

であると仮定すると

$$(a_1^x)^{l_1}=(a_2^y)^{l_1}=e$$

従って $l_1|l_2x$ 即 $(l_1/l_2)|x$ となって，☆ が起るのは

$$x=(l_1/l_2)k,\ k=1, 2, \cdots, l_2-1$$

のときであるから，これらについての a_1^x がすべて $\langle a_2\rangle$ に属さないとき（2）に適するものである．

このチェックは **3.** で元の巾がどの元になるかがわかっているから簡単にできる．ここで $l_1l_2=h$ であれば終．

第3因子　$(l_2, h/l_1l_2)=d_2$ とおく，G の元 $a_3(\neq a_1, a_2)$ を次の3条件をみたすように選ぶ．

（1）　a_3 の位数 l_3 は d_2 または d_2 の約数，

（2）　$\langle a_1\rangle\langle a_2\rangle\cap\langle a_3\rangle=\{e\}$,

（3）　条件（1），（2）をみたし，l_3 の最大のもの．

このとき $\langle a_1\rangle\langle a_2\rangle\langle a_3\rangle$ は前段と定義により直積である．

前と同様に d_2 とその約数の大きいものから（2）の条件をチェックすればよい，もし

$$\langle a_1\rangle\langle a_2\rangle\cap\langle a_3\rangle\neq\{e\}\ \text{即}$$

$$\text{☆☆}\quad a_1^xa_2^y=a_3^z\neq e,\ x,\ y,\ z\in\boldsymbol{Z}$$

であると仮定すると，

$$(a_1^x)^{l_2}(a_2^y)^{l_2}=(a_3^z)^{l_2}=e$$

従って $l_1|l_3x$ かつ $l_2|l_3y$ 即 $(l_1/l_3)|x$ かつ $(l_2/l_3)|y$ となって，☆☆ が起るのは

$$x=(l_1/l_3)k,\ k=1, 2, \cdots, l_3$$
$$y=(l_2/l_3)k',\ k'=1, 2, \cdots, l_3$$

（ただし $x=y=l_3$ は除く）のときであるから，積 $a_1^xa_2^y$ がすべて $\langle a_3\rangle$ に属さないとき，a_3 は条件(2)

に適するものである.

このとき, $l_1l_2l_3=h$ ならば終.

第4因子 $(l_3, h/l_1l_2l_3)=d_3$ とおく, G の元 a_4 $(\neq a_1, a_2, a_3)$ を次の3条件をみたすように選ぶ.

(1) a_4 の位数 l_4 は d_3 または d_3 の約数,

(2) $\langle a_1\rangle\langle a_2\rangle\langle a_3\rangle\cap\langle a_4\rangle=\{e\}$,

(3) 条件(1),(2)をみたし, l_4 の最大のもの.

このとき $\langle a_1\rangle\langle a_2\rangle\langle a_3\rangle$ はこれまでのことと定義により直積となる.

d_3 とその約数の大きいものから(2)の条件をチェックすればよい. いま,

☆☆☆ $a_1^xa_2^ya_3^z=a_4^u\neq e$ $(x, y, z, u\in\boldsymbol{Z})$

と仮定すると, 前述と同様に

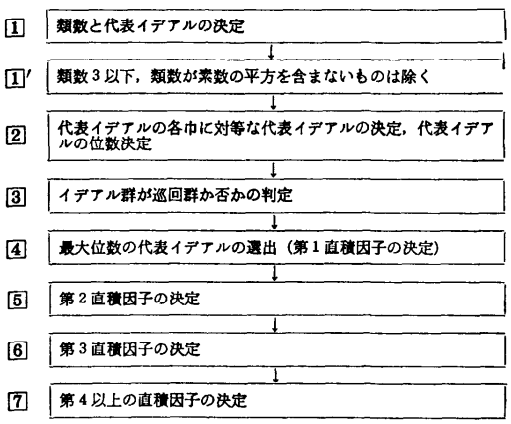
$$x=(l_1/l_4)k,\ k=1, 2, \cdots, l_4;$$
$$y=(l_2/l_4)k',\ k'=1, 2, \cdots, l_4;$$
$$z=(l_3/l_4)k'',\ k''=1, 2, \cdots, l_4$$

となる, ただし $x=y=z=l_4$ の場合は除く, 従って $a_1^xa_2^ya_3^z$ がすべて $\langle a_4\rangle$ に属さないとき, a_4 は条件(2)に適するものである, ここで $l_1l_2l_3l_4=h$ であれば終り. 以下同様に続けて直積因子の底 a_1, a_2, $\cdots$, a_n; 不変系 l_1, l_2, $\cdots$, l_n $(l_1l_2\cdots l_n=h)$ が決まる.

5. プログラム

Table 1 のサブルーチンの内, SEKI, MATRIX, KETT2を示す.

メインプログラムの流れは次のようになる.



虚2次体の場合のメインプログラムを示すが, 実2次体の場合には, 1の段階では実2次体の場合の類数と代表イデアルを求めるプログラム[5]を用い,

M1=(−M−1)/4→M1=(M−1)/4;

M1=−M→M1=M

Table 1 Sub-programs for computing ideal class group.

処理内容	PROGRAM NAME 実, 虚 共通	
素数の発生	PRSB SIEVEZ	
X の素因数分解	FACTOR (X)	
整数の平方因数の有無の判定	SQFREE NOFREE	
整数の整列	WELLOR	
整数 A_1, A_2, A_3 の最大公約数 D と $A_1X+A_2Y+A_3Z=D$ の整数解 X, Y, Z を求める	GCM (A_1, A_2, A_3)	
原始イデアルの積を原始イデアルに変換	SEKI	
	実2次体	虚2次体
因数の選出	SELECT	MAIN に含まれる
簡約された2次無理数の連分数展開	KETT	
2次無理数の簡約 (実2次体では連分数展開, 虚2次体ではS変換, T変換)	KETT2	MATRIX
代表イデアルとの比較	(KETT2 に含まれる)	COMPAR

とする.

1'——7 の段階では,

CALL MATRIX
CALL COMPAR } →CALL KETT2

とする他は全く同一 (文番号は別) である.

(→は変更)

CLN: 類数,

U(N), V(N), N=1, CLN: 代表イデアル,

OS(N, TT)=NZ: N 番目の代表イデアルの TT 乗(巾) は NZ 番目の代表イデアル,

OR(N)=TT: N 番目の代表イデアルの位数は TT

D1: 最大公約数,

MAX, GG, G1G1, G1G1G1: 不変系

K, KK: D1の約数の番号,

CLN2: 3 での巡回群の判定用.

6. 計 算 例

計算例を **Fig. 1**(次頁参照) に示す.

(注1) 不変系だけを目的とするときは, 次のような場合を考慮してプログラムを作成する;

2次体の判別式を割る素数の数を t とする, t と類数 h とから不変系が決まる場合 (和田[1]の 'trivial' の場合) ——計算例では $\boldsymbol{Q}(\sqrt{-390})$, $\boldsymbol{Q}(\sqrt{82})$.

また $Q(\sqrt{32009})$ のように類数 $h(=9)$ と代表イデアルの最大位数（この場合3）とから不変系が決まる場合など．

（注2） $Q(\sqrt{115601})$ の計算でサブルーチン KETT2の 413 行 B1>45000 のことがある．さらに大きくなる2次体では可変多倍長の計算をする．

```
NUMBER=        82  CLASS NUMBER=    4
   CYCLIC GROUP,BASIS  (    6,    4+W)

NUMBER=     32009  CLASS NUMBER=    9
   INVARIANT  (    3,    3)
   BASIS      (   86,    9+W)(   85,   13+W)

NUMBER=    115601  CLASS NUMBER=   45
   CYCLIC GROUP,BASIS  (  163,   34+W)

NUMBER=      -390  CLASS NUMBER=       16
   INVARIANT  (    4,    2,    2)
   BASIS      (   17,   -1+W)   (   13,    0+W)   (    5,    0+W)

NUMBER=    -23142  CLASS NUMBER=       64
   INVARIANT  (    4,    4,    2,    2)
   BASIS      (   71,   -2+W)   (   41,   -8+W)   (   29,    0+W)   (   19,    0+W)
```

Fig. 1 Computer results for $Q(\sqrt{m})$ (Number=m).

MAIN PROGRAM, SUBROUTINES

```
      C   COMPUTATION OF IDEAL CLASS GROUP
      C   OF IMAGINARY QUADRATIC NUMBER FIELD
      C   MAIN PROGRAM
01          IMPLICIT INTEGER(A-V)
02          INTEGER P(100),E(100),F(100),G(100),
           1B(1252),U(300),V(300),
           2X1,X2,Y1,Y2,Z2,XG,
           3DR(300),DS(210,105),
           4INSU(100)
03          COMMON/AB/B/BB/M/EB/LLL/GB/CLN
           1/CB/AZ,RZ/CCB/BZ,SZ/JB/M1
           2/DB/X1,X2,Y1,Y2,Z2,D1,D2
           3/KB/KIGUZ/FB/U,V,NZ
           4/LB/P,E,F/MB/JZ/NB/G/CB/INSU
04          CALL PRSB
05    10    READ(5,97) M
06    97    FORMAT(I5)
07          IF(M.EQ.0) STOP
08          IF(MOD(M,4).EQ.3) GO TO 400
09          MD=4*M
10          KIGUZ=2
11          M1=-M
12          IC2=0
13          GO TO 401
14    400   MD=M
15          KIGUZ=1
16          M1=(-M-1)/4
17          IC2=1
18    401   MD3S=SQRT(FLOAT(MD)/3.0)
19          N=0
20    402   ID=(MD+IC2*IC2)/4
21          IDZ=ID
22          IF(N.NE.0) GO TO 404
23          N=N+1
24          U(N)=1
25          V(N)=0
26          IF(IC.EQ.1) GO TO 700
27    404   CALL FACTOR(IDZ)
      C   SELECTION OF FACTORS
28          IDS=SQRT(FLOAT(ID))
29          AA=1
30          L=1
31    11    P(L)=0
32    22    G(L)=AA
33          L=L+1
34          IF(L.LE.JZ) GO TO 11
35          L=JZ
36    12    P(L)=P(L)+1
37          IF(P(L).LE.E(L)) GO TO 14
38    13    L=L-1
39          IF(L.EQ.0) GO TO 50
40          AA=G(L)
41          GO TO 12
42    14    AA=AA*P(L)
43          IF(AA.GT.IDS) GO TO 13
44          IF(AA.LT.IC2) GO TO 22
45          CC=ID/AA
46          IF(AA.EQ.IC2.OR.AA.EQ.CC.OR.
           1IC2.EQ.0) GO TO 500
47          IF(KIGUZ.EQ.1) GO TO 1000
48          N=N+1
49          U(N)=AA
50          V(N)=(-IC2)/2
51          N=N+1
52          U(N)=AA
53          V(N)=IC2/2
54          GO TO 22
55    1000  N=N+1
56          U(N)=AA
57          V(N)=(-IC2-1)/2
58          N=N+1
59          U(N)=AA
60          V(N)=(IC2-1)/2
61          GO TO 22
62    500   IF(KIGUZ.EQ.1) GO TO 1001
63          N=N+1
64          U(N)=AA
65          V(N)=(-IC2)/2
66          GO TO 22
67    1001  N=N+1
68          U(N)=AA
69          V(N)=(-IC2-1)/2
70          GO TO 22
71    50    IC2=IC2+2
72          IF(IC2.LE.MD3S) GO TO 402
73    700   IM=-M
74          CLN=N
75          WRITE(6,201) IM,CLN
76    201   FORMAT(1H0,7X,7HNUMBER=,I10,
           12X,13HCLASS NUMBER=,I10)
77          CLN2=CLN/2+1
78          IF(CLN.LE.3) GO TO 10
79          CALL NOFREE
80          IF(LLL.EQ.1) GO TO 10
81          N=1
82          DR(1)=1
83          DS(1,1)=1
84    9000  N=N+1
85          TT=1
86          AZ=U(N)
87          RZ=V(N)
88          BZ=AZ
89          SZ=RZ
90    70    CALL SEKI
91          TT=TT+1
92          IF(BZ-1) 80,90,80
93    80    CALL MATRIX
94          IF(BZ.EQ.1) GO TO 90
95          CALL COMPAR
96          DS(N,TT)=NZ
97          IF(TT.NE.CLN2) GO TO 70
98          WRITE(6,205) U(N),V(N)
99    205   FORMAT(1H ,10X,13HCYCLIC GROUP,,
           15HBASIS,2X,1H(,I5,1H,,I5,3H+W))
100         GO TO 10
101   90    DR(N)=TT
102         DS(N,1)=N
103         DS(N,TT)=1
104         IF(N.GE.CLN) GO TO 100
105         GO TO 9000
106   100   CNT=0
107         MAX=0
```

```
      N=2
      K=1
  310 IF(OR(N).LE.MAX) GO TO 320
      CNT=N
      MAX=OR(N)
  320 N=N+1
      IF(N.LE.CLN) GO TO 310
      MAXX=MAX
      QMAX=CLN/MAX
      CALL GCM(MAXXX,QMAX,0)
 8000 IF(K.EQ.1) GO TO 410
      GG=INSU(K)
      GO TO 411
  410 GG=D1
  411 MG=MAX/GG
      II=1
      GG1=GG-1
  360 II=II+1
      IF(II.GT.CLN) GO TO 561
      IF(OR(II).NE.GG) GO TO 360
      IF(II.EQ.CNT) GO TO 360
      DO 600 HG=1,GG1
      DO 601 HHG=1,GG1
      MGHG=MG*HG
      IF(OS(CNT,MGHG).EQ.OS(II,HHG)) GO TO 360
  601 CONTINUE
  600 CONTINUE
      GO TO 370
  561 IF(K.NE.1) GO TO 8001
      GGG=GG
      CALL FACTOR(GGG)
      CALL WELLOR
 8001 K=K+1
      GO TO 8000
  370 IK=II
      IF(GG*MAX.NE.CLN) GO TO 360
      WRITE(6,207) MAX,GG
  207 FORMAT(1H ,10X,12HINVARIANT  (,I5,1H,,I5,1H))
      WRITE(6,208) U(CNT),V(CNT),U(IK),V(IK)
  208 FORMAT(1H ,10X,5HBASIS,5X,1H(,I5,1H,,I5,
     13H*W),1H(,I5,1H,,I5,3H*W))
      GO TO 10
  380 GGMAX=CLN/(GG*MAX)
      GGL=GG
      KK=1
      CALL GCM(GGL,GGMAX,0)
 8010 IF(KK.EQ.1) GO TO 510
      G1G1=INSU(KK)
      GO TO 511
  510 G1G1=D1
  511 MG=MAX/G1G1
      MMG=GG/G1G1
      GGG1=G1G1-1
      II=1
  361 II=II+1
      IF(II.GT.CLN) GO TO 562
      IF(II.EQ.CNT) GO TO 361
      IF(II.EQ.IK) GO TO 361
      IF(OR(II).NE.G1G1) GO TO 361
      DO 362 HG=1,G1G1
      DO 363 HG1=1,G1G1
      IF(HG.EQ.G1G1.AND.HG1.EQ.G1G1) GO TO 390
      MGHG=MG*HG
      MMGHG=MMG*HG1
      NX=OS(CNT,MGHG)
      NY=OS(IK,MMGHG)
      AZ=U(NX)
      RZ=V(NX)
      BZ=U(NY)
      SZ=V(NY)
      CALL SEKI
      CALL MATRIX
      CALL COMPAR
      DO 364 HHG=1,GGG1
      IF(OS(II,HHG).EQ.NZ) GO TO 361
  364 CONTINUE
  363 CONTINUE
  362 CONTINUE
      GO TO 390
  562 IF(KK.NE.1) GO TO 8011
      G1G1L=G1G1
      CALL FACTOR(G1G1L)
      CALL WELLOR
 8011 KK=KK+1
      GO TO 8010
  390 IIK=II
      MAX1=MAX*GG*G1G1
      IF(MAX1.NE.CLN) GO TO 381
      WRITE(6,209) MAX,GG,G1G1
  209 FORMAT(1H ,10X,12HINVARIANT  (,I5,1H,,I5,1H,,I5,1H))
      WRITE(6,210) U(CNT),V(CNT),U(IK),V(IK),U(IIK),V(IIK)
  210 FORMAT(1H ,10X,5HBASIS,5X,1H(,I5,1H,,I5,3H*W),
     13X,1H(,I5,1H,,I5,3H*W),
     23X,1H(,I5,1H,,I5,3H*W))
      GO TO 10
  381 GGGMAX=CLN/MAX1
      G1G1L=G1G1
      KKK=1
      CALL GCM(G1G1L,GGGMAX,0)
 8020 IF(KKK.EQ.1) GO TO 610
      G1G1G1=INSU(KKK)
      GO TO 611
  610 G1G1G1=D1
  611 MG=MAX/G1G1G1
      MMG=GG/G1G1G1
      MMMG=G1G1/G1G1G1
      GGGG1=G1G1G1-1
      II=1
  366 II=II+1
      IF(II.GT.CLN) GO TO 563
      IF(OR(II).NE.G1G1G1) GO TO 366
      IF(II.EQ.CNT) GO TO 366
      IF(II.EQ.IK) GO TO 366
      IF(II.EQ.IIK) GO TO 366
      DO 462 HG=1,G1G1G1
      DO 463 HG1=1,G1G1G1
      DO 464 HG2=1,G1G1G1
      IF(HG.EQ.G1G1G1.AND.HG1.EQ.G1G1G1
     1.AND.HG2.EQ.G1G1G1) GO TO 490
      MGHG=MG*HG
      MMGHG1=MMG*HG1
      MMGHG2=MMMG*HG2
      NX=OS(CNT,MGHG)
      NY=OS(IK,MMGHG1)
      NW=OS(IIK,MMGHG2)
      AZ=U(NX)
      RZ=V(NX)
      BZ=U(NY)
      SZ=V(NY)
      CALL SEKI
      CALL MATRIX
      CALL COMPAR
      NZ1=NZ
      AZ=U(NZ1)
      RZ=V(NZ1)
      BZ=U(NW)
      SZ=V(NW)
      CALL SEKI
      CALL MATRIX
      CALL COMPAR
      NZ2=NZ
      DO 465 HHG=1,GGGG1
      IF(NZ2.EQ.OS(II,HHG)) GO TO 366
  465  CONTINUE
  464 CONTINUE
  463 CONTINUE
  462  CONTINUE
      GO TO 490
  563 IF(KKK.NE.1) GO TO 8022
      G1G1GL=G1G1G1
      CALL FACTOR(G1G1GL)
      CALL WELLOR
 8022 KKK=KKK+1
      GO TO 8020
  490 IIIK=II
      MAX2=MAX*GG*G1G1*G1G1G1
      IF(MAX2.NE.CLN) GO TO 382
      WRITE(6,212) MAX,GG,G1G1,G1G1G1
  212  FORMAT(1H ,10X,12HINVARIANT  (,I5,1H,,I5,
     11H,,I5,1H,,I5,1H))
      WRITE(6,211) U(CNT),V(CNT),U(IK),V(IK),
     1U(IIK),V(IIK),U(IIIK),V(IIIK)
  211  FORMAT(1H ,10X,5HBASIS,5X,1H(,I5,1H,,I5,3H*W),
     13X,1H(,I5,1H,,I5,3H*W),
     23X,1H(,I5,1H,,I5,3H*W),
     32X,1H(,I5,1H,,I5,3H*W))
      GO TO 10
  382  WRITE(6,999)
  999  FORMAT(1H ,20HDATA ERROR NO KEISAN)
      GO TO 10
      END
```

```
      SUBROUTINE SEKI
      IMPLICIT INTEGER(A-V)
      INTEGER X1,X2,Y1,Y2,Z2
      COMMON/BB/M/CB/A,R/CCB/B,S/JB/M1
     1/DB/X1,X2,Y1,Y2,Z2,D1,D2
     2/KB/KIGUZ
      IF(A.EQ.1) RETURN
      IF(B.NE.1) GO TO 9
      B=A
      S=R
      RETURN
    9 IF(R) 1,2,2
    1 R=R+A
    2 IF(S) 3,4,4
    3 S=S+B
    4 IF(KIGUZ.EQ.1) GO TO 10
      RS=R+S
      GO TO 20
   10 RS=R+S+1
   20 AL=A
      BL=B
      RSL=RS
      CALL GCM(AL,BL,RSL)
      E=A*S*X2+B*R*Y2+(R*S+M1)*Z2
      AB=A*B
      IF(D2.EQ.1) GO TO 1000
      B=AB/(D2*D2)
      RR=E/D2
      S=MOD(RR,B)
      RETURN
 1000 B=AB
      S=MOD(E,B)
      RETURN
      END

      SUBROUTINE MATRIX
      IMPLICIT INTEGER (A-V)
      COMMON/CCB/A,R/KB/KIGUZ/BB/M
      IF(KIGUZ.EQ.1) GO TO 900
      IF(R.EQ.0) GO TO 50
      R=MOD(R,A)
   10 IF(R) 11,50,12
   11 R=R+A
   12 IF(FLOAT(R)/FLOAT(A).LT.0.5) GO TO 50
      R=R-A
   50 AR=(R*R+M)/A
      IF(FLOAT(AR)/FLOAT(A)-1.0) 88,66,99
   66 IF(R) 99,99,77
   77 A=AR
      R=-R
      GO TO 99
   88 A=AR
      R=-R
      R=MOD(R,A)
      WR=FLOAT(R)/FLOAT(A)
      IF(WR.GE.-0.5.AND.WR.LT.0.5) GO TO 50
      GO TO 10
   99 RETURN
  900 IF(R.EQ.0) GO TO 150
      R=MOD(R,A)
  100 IF(R) 110,150,120
  110 R=R+A
  120 RZ=2*R+1
      AZ=2*A
      MODR=MOD(RZ,AZ)
      IF(MODR.LT.A) GO TO 150
      R=R-A
  150 RR=2*R+1
      AR=(RR*RR+M)/(4*A)
      IF(FLOAT(AR)/FLOAT(A)-1.0) 188,166,99
  166 IF(RR) 99,99,177
  177 A=AR
      R=-R-1
      GO TO 99
  188 A=AR
      R=-R-1
      R=MOD(R,A)
      RZ=2*R+1
      AZ=2*A
      WRA=FLOAT(RZ)/FLOAT(AZ)
      IF(WRA.GE.-0.5.AND.WRA.LT.0.5) GO TO 150
      GO TO 100
      END
      SUBROUTINE COMPAR
      IMPLICIT INTEGER (A-V)
      INTEGER U(300),V(300)
      COMMON/FB/U,V,NZ/CCB/BZ,SZ/GB/CLN
      DO 10 I=1,CLN
      IF(U(I)-BZ) 10,11,10
   11 IF(V(I)-SZ) 10,12,10
   10 CONTINUE
   12 NZ=1
      RETURN
      END

      SUBROUTINE KETT2
      IMPLICIT INTEGER(A-V)
      INTEGER U(300),V(300),U2(300),V2(300)
      COMMON/FB/U,V,U2,V2,CLN/PB/MS
     1/BB/M,MODM
     2/CCB/A,B/FFB/NZ
      IF(B) 3,4,4
    3 B=B+A
    4 A2=A
      B2=B
    1       DO 10 N=1,CLN
      IF(U(N)-A2) 10,11,10
   11 IF(V(N)-B2) 10,12,10
   10       CONTINUE
      IF(MODM.NE.1) GO TO 2
      A1=2*A2
      B1=2*B2+1
      GO TO 5
    2 A1=A2
      B1=B2
    5 KZ=(B1*MS)/A1
      IF(B1.LE.45000) GO TO 40
      C=B1-45000
      CC=C*C
      CCC=90000*C
      CCCC=45000*45000
      Q1=M/A1
      Q2=CC/A1
      Q3=CCC/A1
      Q4=CCCC/A1
      R1=M-A1*Q1
      R2=CC-A1*Q2
      R3=CCC-A1*Q3
      R4=CCCC-A1*Q4
      Q5=(R1-(R2+R3+R4))/A1
      NR=Q1-(Q2+Q3+Q4)+Q5
      GO TO 41
   40 NR=(M-B1*B1)/A1
   41 B2=A1*KZ-B1
      A2=NR+2*B1*KZ-A1*KZ*KZ
  700 IF(MODM.NE.1) GO TO 30
      A2=A2/2
      B2=(B2-1)/2
   30 IF(A2.GE.0) GO TO 31
      A2=-A2
   31 B3=MOD(B2,A2)
      B2=B3
      IF(B2.GE.0) GO TO 1
      B2=B2+A2
      GO TO 1
   12 NZ=N
      A=A2
      B=B2
      GO TO 800
      GO TO 700
  800 RETURN
      END
```

参考文献

1) H. Wada: A Table of Ideal Class groups of Imaginary Quadratic Fields, Proc. Japan Acad. 46, pp. 401～403 (1970).
2) B. Lakein: Computation of the Ideal Class Group of Certain Complex Quatic Fields. II, Math. Comp. V. 29, pp. 139～144 (1975).
3) 高木：初等整数論講義，共立出版 (1971).
4) 片山：虚2次数体の類数の計算，情報処理, Vol. 18, No. 6, pp. 612～613 (1977).
5) 片山：実2次数体の類数の計算の一工夫，情報処理 Vol. 19. No. 5, pp. 475～477 (1978).
6) Waerden: Moderne Algebra, I, II, Springer (1950, 1940).

(昭和52年8月31日受付)