整数係数 2 元 2 次形式の主種定理のガウスによる構成的証明の応用

前田博信

要約

ガウスは主種に属する 2 元 2 次形式が与えられたとき，判別式が 1 の不定符号の 3 元 2 次形式を作り，これを標準形 x^2-2yz に変換することにより，2 倍化するとちょうど最初の 2 元 2 次形式になるような 2 元 2 次形式を計算する方法を与えた（1801 年）．この方法は整数係数でなくても係数域がある条件をみたせばそのまま適用できることを示す．

文献

[DA] C. F. Gauss, Disquisitiones Arithmeticae, Fleischer, Leipzig, 1801.
（和訳, 高瀬正仁,『ガウス整数論』, 朝倉書店, 1995.）
[K] 久保田富雄,『数論論説』, 牧野書店, 1999.
[S] J.-P. Serre, Cours d'arithmétique, Presses Univ. de France, 1970.
(和訳, 彌永健一,『数論講義』, 岩波書店, 1979.)

定義と記号

1. 2 次の斉次式 $ax^2+2bxy+cy^2$ を (a,b,c) と表す．
2. すべてが 0 ではない整数 l,m,n の正の最大公約数を $\gcd(l,m,n)$ と表す．
3. $d=b^2-ac$ を (a,b,c) の判別式という．
4. $X=pxx'+p'xy'+p''yx'+p'''yy'$, $Y=qxx'+q'xy'+q''yx'+q'''yy'$ という置換により
$$AX^2+2BXY+CY^2=(ax^2+2bxy+cy^2)(a'x'^2+2b'x'y'+c'y'^2),$$
$$\gcd(A,2B,C)=\gcd(a,2b,c)\gcd(a',2b',c')$$
が成り立つとき，(A,B,C) は (a,b,c) と (a',b',c') の合成 (composition) であるという．結合ともいう．
5. (a,b,c) と (a,b,c) の合成を (a,b,c) の 2 倍化（duplication）という．重複ともいう．
6. 3 元 2 次形式 $ax^2+a'x'^2+a''x''^2+2bx'x''+2b'xx''+2b''xx'$ の判別式は $ab^2+a'b'^2+a''b''^2-aa'a''-2bb'b''$，すなわち，係数行列の行列式の -1 倍とする．

§1. 2次形式の合成の計算方法と例

[DA] 第235条の最後の注意事項から出発する.

$p,p',p'',p''',q,q',q'',q''',n,n'$ $(nn'\neq 0)$ が与えられたとき，次の9式

$$an'=pq'-qp'$$
$$2bn'=(pq'''-qp''')-(p'q''-q'p'')$$
$$cn'=p''q'''-q''p'''$$
$$a'n=pq''-qp''$$
$$2b'n=(pq'''-qp''')+(p'q''-q'p'')$$
$$c'n=p'q'''-q'p'''$$
$$Ann'=q'q''-qq'''$$
$$2Bnn'=pq'''+qp'''-p'q''-q'p''$$
$$Cnn'=p'p''-pp'''$$

により a,b,c,a',b',c',A,B,C を定めると，

$X=pxx'+p'xy'+p''yx'+p'''yy'$，$Y=qxx'+q'xy'+q''yx'+q'''yy'$

という置換により，

$$AX^2+2BXY+CY^2=(ax^2+2bxy+cy^2)(a'x'^2+2b'x'y'+c'y'^2),$$
$$b^2-ac=n^2(B^2-AC),\quad b'^2-a'c'=n'^2(B^2-AC)$$

が成立する.

上記の9つの式のうち最初の6つをベクトルと行列を用いて書き換えると，2つの4次ベクトルの交代積 $\begin{bmatrix}p\\p'\\p''\\p'''\end{bmatrix}\wedge\begin{bmatrix}q\\q'\\q''\\q'''\end{bmatrix}$ が次の交代行列

$$W=\begin{bmatrix}0 & n'a & na' & n'b+nb'\\ -n'a & 0 & -n'b+nb' & nc'\\ -na' & n'b-nb' & 0 & n'c\\ -n'b-nb' & -nc' & -n'c & 0\end{bmatrix}$$

に等しいことを表し，残りは，4元2次形式 $2yz-2xu$ による表現

$$\begin{bmatrix}p & p' & p'' & p'''\\ q & q' & q'' & q'''\end{bmatrix}\begin{bmatrix}0 & 0 & 0 & -1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ -1 & 0 & 0 & 0\end{bmatrix}\begin{bmatrix}p & q\\ p' & q'\\ p'' & q''\\ p''' & q'''\end{bmatrix}$$

$$=2nn'\begin{bmatrix}C & -B\\ -B & A\end{bmatrix}=2nn'\begin{bmatrix}A & B\\ B & C\end{bmatrix}^{ad}$$

を表す（L^{ad} は L の余因子行列（adjugate, Adjunkte）を表す）.

なお，$\det W = \left\{n^2(b'^2 - a'c') - n'^2(b^2 - ac)\right\}^2$ であり，この右辺は交代行列 W の Pfaff 式の平方である（J. F. Pfaff は Gauss が Helmstedt 大学に学位論文を提出（1799 年）したときの主査であった）．

続く [DA] 第 236 条には $n'^2(b^2 - ac) = n^2(b'^2 - a'c')$ をみたす (a, b, c), (a', b', c'), n, n' $(nn' \neq 0)$ が与えられたとき，[DA] 第 235 条の最後の注意事項を成り立たせるような $p, p', p'', p''', q, q', q'', q'''$ を一組求める方法が書かれている．

例. $(a, b, c) = (2, 7, 11)$, $(a', b', c') = (3, 9, 2)$, $n' = 5$, $n = 3$ とすると $n'^2 \times (b^2 - ac) = 5^2 \times 27 = n^2 \times (b'^2 - a'c') = 3^2 \times 75 = 675$ である．交代積が下の W になるような整数成分の 2 つの 4 次ベクトルを求めてみる．

$$W = \begin{bmatrix} 0 & 10 & 9 & 62 \\ -10 & 0 & -8 & 6 \\ -9 & 8 & 0 & 55 \\ -62 & -6 & -55 & 0 \end{bmatrix}$$

W の成分の最大公約数が 1 であるからユークリッドの互除法を用いて，$WZW = W$ をみたす 4 次交代行列 Z を求める．

例えば，$Z = \begin{bmatrix} 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$.

次に，適当な 4 次ベクトル $\boldsymbol{Q}'$ で $W\boldsymbol{Q}' = \boldsymbol{q}' \neq \boldsymbol{0}$ となるものをとり，$\boldsymbol{q}'$ の成分から最大公約数 μ をくくりだして $\boldsymbol{q}' = \mu\boldsymbol{q}$ とする．例えば，

$$W \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 10 \\ 0 \\ 8 \\ -6 \end{bmatrix} \text{ より，} \mu = 2, \ \boldsymbol{q} = \begin{bmatrix} 5 \\ 0 \\ 4 \\ -3 \end{bmatrix}.$$

（$Z\boldsymbol{q} = \boldsymbol{Q}$ とおくと $W\boldsymbol{Q} = \boldsymbol{q}$ となるから $\mu = 1$ に帰着される.）$\boldsymbol{q}$ の成分の最大公約数が 1 であるから，ユークリッドの互除法を用いて $\boldsymbol{q}$ との内積が 1 となる $\boldsymbol{P}$ を求め，$\boldsymbol{p} = W\boldsymbol{P}$ とおく．例えば，

$$\boldsymbol{P} = \begin{bmatrix} 1 \\ 0 \\ -1 \\ 0 \end{bmatrix} \text{ とおくと } \boldsymbol{p} = \begin{bmatrix} -9 \\ -2 \\ -9 \\ -7 \end{bmatrix} \text{ となる.}$$

この $\boldsymbol{p}$ と $\boldsymbol{q}$ の交代積が W に等しく，$C = -3$, $B = 0$, $A = 1$ となるから，

$$X = -9xx' - 2xy' - 9yx' - 7yy', \ Y = 5xx' + 4yx' - 3yy'$$

という置換により

$$X^2-3Y^2=(2x^2+14xy+11y^2)(3x'^2+18x'y'+2y'^2)$$

が成り立つ.

注意. $\boldsymbol{p},\boldsymbol{q}$ の選び方は一意的ではないから, (A,B,C) も一意的ではない.

例えば, 上の $\boldsymbol{P}$ を $\begin{bmatrix}0\\0\\1\\1\end{bmatrix}$ とすると $\boldsymbol{p}$ は $\begin{bmatrix}71\\-2\\55\\-55\end{bmatrix}$ となり, $A=1$, $B=-16$, $C=253$ となるから

$$X=71xx'-2xy'+55yx'-55yy',\quad Y=5xx'+4yx'-3yy'$$

という置換により

$$X^2-32XY+253Y^2=(2x^2+14xy+11y^2)(3x'^2+18x'y'+2y'^2)$$

が成り立つ. [DA] 第 234 条には, $\boldsymbol{r}$ と $\boldsymbol{s}$ の交代積が W の k 倍となるとき

$$\boldsymbol{r}=\delta\boldsymbol{p}-\beta\boldsymbol{q},\quad \boldsymbol{s}=-\gamma\boldsymbol{p}+\alpha\boldsymbol{q},\quad \alpha\delta-\beta\gamma=k$$

をみたす整数 $\alpha,\beta,\gamma,\delta$ を計算する方法が書いてある.

§2. 2 倍化の計算と, そのときの置換の性質

前節の計算で $a=a'$, $b=b'$, $c=c'$, $n=n'=1$ の場合を考察する.

このとき W の第 2 行と第 3 行が等しくなるから, $p''=p'$, $q''=q'$ とおくと, p,p',p''',q,q',q''' は次の式をみたしている.

$$a=pq'-qp'$$
$$2b=pq'''-qp'''$$
$$c=p'q'''-q'p'''$$
$$A=q'^2-qq'''$$
$$2B=pq'''+qp'''-2p'q'$$
$$C=p'^2-pp'''$$

ここで $\gcd(A,2B,C)=1$ を仮定すると, 「p, p', p''', q, q', q''' がすべて奇数である」ことはない. そこで, $p=2\bar{p}$, $q=2\bar{q}$ とおいてみると, $(A,-B,C)$ の 3 元 2 次形式 y^2-2xz による表現

$$\begin{bmatrix}\bar{q}&q'&q''\\ \bar{p}&p'&p'''\end{bmatrix}\begin{bmatrix}0&0&-1\\0&1&0\\-1&0&0\end{bmatrix}\begin{bmatrix}\bar{q}&\bar{p}\\ q'&p'\\ q'''&p'''\end{bmatrix}=\begin{bmatrix}A&-B\\-B&C\end{bmatrix}$$

が得られる.

ここで，改めて，

$$q'=\alpha,\ \bar{q}=\alpha',\ q'''=\alpha'',\ p'=\beta,\ \bar{p}=\beta',\ p'''=\beta''$$

とおいてみると，$\gcd(A,2B,C)=1$ のとき，2倍化して (A,B,C) になるような (a,b,c) を（一つ）求めるには，$(A,-B,C)$ の3元2次形式 x^2-2yz による表現

$$\begin{bmatrix}\alpha & \alpha' & \alpha''\\ \beta & \beta' & \beta''\end{bmatrix}\begin{bmatrix}1 & 0 & 0\\ 0 & 0 & -1\\ 0 & -1 & 0\end{bmatrix}\begin{bmatrix}\alpha & \beta\\ \alpha' & \beta'\\ \alpha'' & \beta''\end{bmatrix}=\begin{bmatrix}A & -B\\ -B & C\end{bmatrix}$$

を（一つ）求めて，$\gcd(a,2b,c)=1$ を示せばよいことがわかった．このとき本来の $p,p',p'',p''',q,q',q'',q'''$ はこの順で $2\beta',\beta,\beta,\beta'',2\alpha',\alpha,\alpha,\alpha''$ となるから，$s=\alpha'\beta''-\alpha''\beta'$，$t=-(\alpha\beta''-\alpha''\beta)$，$r=\alpha\beta'-\alpha'\beta$ とおくと，$(a,b,c)=(2r,-s,t)$ となり，$\gcd(2r,-2s,t)=1$ であれば $(2r,-s,t)$ の2倍化が (A,B,C) となることが分かる．また，この計算では α' と α'' を，β' と β'' を同時に入れ換えてもよい．このときは $p,p',p'',p''',q,q',q'',q'''$ が $\beta',\beta,\beta,2\beta'',\alpha',\alpha,\alpha,2\alpha''$ となり，$(a,b,c)=(r,-s,2t)$ となるから，$\gcd(2r,-2s,t)$ と $\gcd(r,-2s,2t)$ の少なくとも一方が1であることを示せばよいことも分かる．

§3. 主種定理の計算による証明

最初に，主種に属する2元2次形式 (A,B,C)，$\gcd(A,2B,C)=1$ が与えられたとき，判別式が1の3元2次形式を作る（[K]，206頁参照）．

$B^2-AC=D$ とおくと，

$$A\xi^2+2B\xi\eta+C\eta^2=1-A'D\ (\equiv 1 \bmod D)$$

をみたす整数 ξ,η,A' が選べるから

$$S=\begin{bmatrix}A & -B & \eta\\ -B & C & \xi\\ \eta & \xi & A'\end{bmatrix}$$

とおくと $\det S=-1$ となり，S を係数行列とする判別式が1の整数係数3元2次形式

$$\varphi(t,u,v)=At^2+Cu^2+A'v^2+2\xi uv+2\eta vt-2Btu$$

が定まる．$A\neq 0$，$D\neq 0$ とすると，

$$AD\varphi(t,u,v)=Av^2-\{Du-(A\xi+B\eta)v\}^2+D(At+\eta v-Bu)^2$$

であることから，φ は，「$D>0$ のとき」，または，「$D<0$ かつ $A>0$ のとき」は不定符号となる．Gauss は，判別式が 1 で不定符号の 3 元 2 次形式が x^2-2yz に還元できる，すなわち

$$S=\begin{bmatrix}\alpha & \alpha' & \alpha''\\ \beta & \beta' & \beta''\\ \gamma & \gamma' & \gamma''\end{bmatrix}\begin{bmatrix}1 & 0 & 0\\ 0 & 0 & -1\\ 0 & -1 & 0\end{bmatrix}\begin{bmatrix}\alpha & \beta & \gamma\\ \alpha' & \beta' & \gamma'\\ \alpha'' & \beta'' & \gamma''\end{bmatrix},\ \det\begin{bmatrix}\alpha & \alpha' & \alpha''\\ \beta & \beta' & \beta''\\ \gamma & \gamma' & \gamma''\end{bmatrix}=1$$

をみたす $\alpha,\alpha',\alpha'',\beta,\beta',\beta'',\gamma,\gamma',\gamma''$ が計算できることを示して，2 倍化すると (A,B,C)（ただし，$\gcd(A,2B,C)=1$）に一致する 2 元 2 次形式を計算した（[DA] 第 286 条）．

その結果として，「判別式が 1 で不定符号の 3 元 2 次形式 φ は 0 を表現する」ことが示された．もし，最初から「φ は 0 を表現する」ことが分かれば，上の $\alpha,\alpha',\alpha'',\beta,\beta',\beta'',\gamma,\gamma',\gamma''$ を 3 元 2 次形式の還元を使わなくても初等的に求めることができることを示そう．

$\varphi(u,u',u'')=0$ とする．すなわち，$\boldsymbol{u}=\begin{bmatrix}u\\ u'\\ u''\end{bmatrix}$ が，$\boldsymbol{u}^TS\boldsymbol{u}=0$ をみたすとする（$\boldsymbol{u}^T$ は $\boldsymbol{u}$ の転置を表す）．$\boldsymbol{u}$ の成分から公約数をくくりだして $\gcd(u,u',u'')=1$ としてよい．ユークリッドの互除法により $uv+u'v'+u''v''=1$ をみたす v,v',v'' を求めて $\boldsymbol{v}=\begin{bmatrix}v\\ v'\\ v''\end{bmatrix}$ とおき，$\boldsymbol{v}'=S^{-1}\boldsymbol{v}$ とおく．S^{-1} の成分も整数であるから $\boldsymbol{v}'$ も整数成分のベクトルであり，$\boldsymbol{u}^TS\boldsymbol{v}'=\boldsymbol{u}^T\boldsymbol{v}=1$ をみたす．$\boldsymbol{v}'^TS\boldsymbol{v}'=\mu$ とする．μ の偶奇で 2 つの場合に分ける．

(I) $\mu=2\mu'$ の場合．

$\boldsymbol{v}''=-\boldsymbol{v}'+\mu'\boldsymbol{u}$ とおくと $\boldsymbol{v}''^TS\boldsymbol{v}''=0$，$\boldsymbol{v}''^TS\boldsymbol{u}=-1$ となる．次に，$S\boldsymbol{u}$ と $S\boldsymbol{v}''$ のベクトル積 $S\boldsymbol{u}\times S\boldsymbol{v}''$ を $\boldsymbol{t}$ とする．ベクトル積の性質からただちに，$\boldsymbol{t}^TS\boldsymbol{u}=0$，$\boldsymbol{t}^TS\boldsymbol{v}''=0$ が分かる．ここで，列ベクトル $\boldsymbol{x}$，$\boldsymbol{y}$ の標準内積 $\boldsymbol{x}^T\boldsymbol{y}$ を $\boldsymbol{x}\cdot\boldsymbol{y}$ と書くと，3 次列ベクトル $\boldsymbol{x}$，$\boldsymbol{y}$，$\boldsymbol{a}$，$\boldsymbol{b}$ と 3 次正方行列 A について

$$\det\begin{bmatrix}\boldsymbol{x}\cdot\boldsymbol{a} & \boldsymbol{y}\cdot\boldsymbol{a}\\ \boldsymbol{x}\cdot\boldsymbol{b} & \boldsymbol{y}\cdot\boldsymbol{b}\end{bmatrix}=(\boldsymbol{x}\cdot\boldsymbol{a})(\boldsymbol{y}\cdot\boldsymbol{b})-(\boldsymbol{x}\cdot\boldsymbol{b})(\boldsymbol{y}\cdot\boldsymbol{a})=(\boldsymbol{x}\times\boldsymbol{y})\cdot(\boldsymbol{a}\times\boldsymbol{b})$$

$$(A\boldsymbol{x}\times A\boldsymbol{y})=(A^{ad})^T(\boldsymbol{x}\times\boldsymbol{y})$$

が成り立つ．したがって，

$$
\begin{aligned}
\boldsymbol{t}^T S\boldsymbol{t} &= (S\boldsymbol{u} \times S\boldsymbol{v}'')^T S(S\boldsymbol{u} \times S\boldsymbol{v}'') \\
&= (\boldsymbol{u} \times \boldsymbol{v}'')^T S^{ad} S(S\boldsymbol{u} \times S\boldsymbol{v}'') \\
&= -(\boldsymbol{u} \times \boldsymbol{v}'') \cdot (S\boldsymbol{u} \times S\boldsymbol{v}'') \\
&= -(\boldsymbol{u} \cdot S\boldsymbol{u})(\boldsymbol{v}'' \cdot S\boldsymbol{v}'') + (\boldsymbol{u} \cdot S\boldsymbol{v}'')(\boldsymbol{v}'' \cdot S\boldsymbol{u}) \\
&= -(\boldsymbol{u}^T S\boldsymbol{u})(\boldsymbol{v}''^T S\boldsymbol{v}'') + (\boldsymbol{u}^T S\boldsymbol{v}'')(\boldsymbol{v}''^T S\boldsymbol{u}) = 1
\end{aligned}
$$

である．そこで，列ベクトル $\boldsymbol{t}$，$\boldsymbol{u}$，$\boldsymbol{v}''$ を並べてできる 3 次正方行列を L とすれば，

$$
L^T S L = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{bmatrix}, \quad \text{特に } (\det L)^2 = 1
$$

となることが分かる．必要なら $\boldsymbol{u}$ と $\boldsymbol{v}''$ を入れ換えて $\det L = 1$ としてよい．

(II) $\mu = 2\mu'' + 1$ の場合．

$\boldsymbol{u}' = \boldsymbol{v}' - \mu''\boldsymbol{u}$，$\boldsymbol{v}''' = \boldsymbol{v}' - (\mu'' + 1)\boldsymbol{u}$ とおくと $\boldsymbol{u}'^T S\boldsymbol{u}' = 1$，$\boldsymbol{v}'''^T S\boldsymbol{v}''' = -1$，$\boldsymbol{u}'^T S\boldsymbol{v}''' = 0$ となる．$\boldsymbol{t}' = S\boldsymbol{u}' \times S\boldsymbol{v}'''$ とおくと，$\boldsymbol{t}'^T S\boldsymbol{u}' = 0$，$\boldsymbol{t}'^T S\boldsymbol{v}''' = 0$ となり，前の場合のときと同様の計算で $\boldsymbol{t}'^T S\boldsymbol{t}' = 1$ となることが分かるから，$\boldsymbol{t}'$，$\boldsymbol{u}'$，$\boldsymbol{v}'''$ を並べてできる 3 次正方行列を L' とし，

$$
L = L' \begin{bmatrix} 1 & -1 & 0 \\ 1 & 0 & -1 \\ 1 & -1 & -1 \end{bmatrix}
$$

とおくと

$$
L^T S L = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{bmatrix}, \quad \text{特に } (\det L)^2 = 1
$$

となる．必要なら 2 列目と 3 列目を入れ換えて $\det L = 1$ としてよい．

そこで，

$$
L^{-1} = \begin{bmatrix} \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \\ \alpha'' & \beta'' & \gamma'' \end{bmatrix}
$$

（$\alpha, \alpha', \alpha'', \beta, \beta', \beta'', \gamma, \gamma', \gamma''$は整数）とすると，求める式

$$
S = (L^{-1})^T \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{bmatrix} L^{-1}
$$

$$= \begin{bmatrix} \alpha & \alpha' & \alpha'' \\ \beta & \beta' & \beta'' \\ \gamma & \gamma' & \gamma'' \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \\ \alpha'' & \beta'' & \gamma'' \end{bmatrix}$$

かつ

$$\det \begin{bmatrix} \alpha & \alpha' & \alpha'' \\ \beta & \beta' & \beta'' \\ \gamma & \gamma' & \gamma'' \end{bmatrix} = 1$$

が得られた.

例. $F(X,Y) = 5X^2 + 4XY + 31Y^2$ とする. $(A,B,C) = (5,2,31)$ であり, 判別式 $D = 2^2 - 5 \times 31 = -151$ $(\equiv 1 \bmod 4)$ である.

$$F(X,Y) \equiv 11^2(5X + 2Y)^2 \mod D$$

であるから F は主種に属する. $F(11,0) = 5 \times 11^2 = 1 - 4 \times (-151)$ であるから上記の S と φ は

$$S = \begin{bmatrix} 5 & -2 & 0 \\ -2 & 31 & 11 \\ 0 & 11 & 4 \end{bmatrix}, \quad \varphi(t,u,v) = 5t^2 + 31u^2 + 4v^2 + 22uv - 4tv$$

となる. 簡単な計算で $\varphi(-3,-7,20) = 0$ が分かるから,

$$L = \begin{bmatrix} -3 & -2 & -3 \\ -6 & -4 & -7 \\ 17 & 11 & 20 \end{bmatrix} \text{ とおくと } L^T S L = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{bmatrix}$$

となることが分かり,

$$L^{-1} = \begin{bmatrix} -3 & 7 & 2 \\ 1 & -9 & -3 \\ 2 & -1 & 0 \end{bmatrix}$$

であるから

$$\varphi(t,u,v) = (-3t + 7u + 2v)^2 - 2(t - 9u - 3v)(2t - u).$$

となり,

$$X = -18xx' + 7xy' + 7yx' - yy', \quad Y = 2xx' - 3xy' - 3yx' + 2yy'.$$

という置換により $(40,-17,11)$ の 2 倍化が $(5,2,31)$ になる :

$$5X^2 + 4XY + 31Y^2 = (40x^2 - 34xy + 11y^2)(40x'^2 - 34x'y' + 11y'^2)$$

ことが分かる.

したがって, 上の方法による主種定理の証明の核心部分は「φ が 0 を表現する」ことを示すことであり, 残りの部分は初等的である. Gauss は 3

元2次形式の還元を用いたが，今日ではより一般に「整数係数の n 元2次形式は判別式が ± 1 で不定符号ならば0を表す」ことを Minkowski-Hasse の定理を用いて証明できる（[S]，Chap. V, Théorème 3）.

§4. 応用

前節の方法は，係数域を変えても，上で構成した φ が0を表すことが示されるか，あるいは仮定するならば，そのまま通用する.

例えば，単項イデアル整域 R で，2が単元か素元で，2が素元の場合はその剰余体が完全体であって，ゼロでない元は代表として単元の平方が選べるとき，R 係数の (A,B,C) が $\gcd(A,2B,C)=1$ であり，判別式と素な平方元を表現する，と仮定するならば，2倍化して (A,B,C) となる (a,b,c) で $\gcd(a,2b,c)=1$ をみたすものが具体的に計算できる．R の例としては，(1) 有理整数環 $\mathbf{Z}$，(2) p 進整数環 $\mathbf{Z}_p$，(3) 実2次体 $\mathbf{Q}(\sqrt{5})$ の整数環 $\mathbf{Z}[(1+\sqrt{5})/2]$，(4) 円の3等分体の整数環 $\mathbf{Z}[(-1+\sqrt{-3})/2]$，などがある

例. $F(X,Y)=3X^2-16XY-7Y^2$ とする．すなわち，$(A,B,C)=(3,-8,-7)$ とする．F の判別式は $85=5\times 17$ であり，

$$F(X,Y)\equiv 57(3X-8Y)^2 \mod 85$$

である．57は5を法としても17を法としても平方剰余でないから，F は整数係数の2次形式としては主種に属さない．ところが，$\mathbf{Z}[(-1+\sqrt{-3})/2]$ 上では $F(14\sqrt{-3},-42\sqrt{-3})=7056=84^2$ は判別式と素な平方元であり，

$$X=-10xx'+(-5+2\sqrt{-3})xy'+(-5+2\sqrt{-3})yx'+(-2+2\sqrt{-3})yy',$$
$$Y=34xx'+(17-4\sqrt{-3})xy'+(17-4\sqrt{-3})yx'+(7-4\sqrt{-3})yy'$$

という置換により2倍化

$$\begin{aligned}&3X^2-16XY-7Y^2\\&=\left((-28\sqrt{-3})x^2+2(-1-14\sqrt{-3})xy+(-1-8\sqrt{-3})y^2\right)\\&\times\left((-28\sqrt{-3})x'^2+2(-1-14\sqrt{-3})x'y'+(-1-8\sqrt{-3})y'^2\right)\end{aligned}$$

が得られる．以下，前節で用いた記号をそのまま使う.

$\xi=14\sqrt{-3}$，$\eta=-42\sqrt{-3}$ であり，$A'=-83$ であるから

$$S=\begin{bmatrix}3 & 8 & -42\sqrt{-3}\\ 8 & -7 & 14\sqrt{-3}\\ -42\sqrt{-3} & 14\sqrt{-3} & -83\end{bmatrix},\det S=-1$$

となり，

$$S^{-1} = -S^{ad} = \begin{bmatrix} -1169 & -2428 & 182\sqrt{-3} \\ -2428 & -5043 & 378\sqrt{-3} \\ 182\sqrt{-3} & 378\sqrt{-3} & 85 \end{bmatrix}$$

となることが分かる.

$$\varphi(-182\sqrt{-3}, -378\sqrt{-3}, -84) = (-14\sqrt{-3})^2\varphi(13, 27, -2\sqrt{-3}) = 0$$

であるから, $\boldsymbol{u} = \begin{bmatrix} 13 \\ 27 \\ -2\sqrt{-3} \end{bmatrix}$ とおく. $\boldsymbol{v}$ の選び方は一意的ではないが, $\boldsymbol{v} = \begin{bmatrix} -2 \\ 1 \\ 0 \end{bmatrix}$ とおける. このとき $\boldsymbol{v}' = \begin{bmatrix} -90 \\ -187 \\ 14\sqrt{-3} \end{bmatrix}$ となり, $\mu = \boldsymbol{v}'^T S \boldsymbol{v}' = -7$ となる. $-7 = 2 \times (-4) + 1$ より, $\mu'' = -4$ とおくと $\boldsymbol{u}' = \begin{bmatrix} -38 \\ -79 \\ 6\sqrt{-3} \end{bmatrix}$, $\boldsymbol{v}''' = \begin{bmatrix} -51 \\ -106 \\ 8\sqrt{-3} \end{bmatrix}$ となり,

$$L = \begin{bmatrix} -89 + 2\sqrt{-3} & 51 - 2\sqrt{-3} & 89 \\ -185 + 4\sqrt{-3} & 106 - 4\sqrt{-3} & 185 \\ 1 + 14\sqrt{-3} & -1 - 8\sqrt{-3} & -14\sqrt{-3} \end{bmatrix}$$

$$L^{-1} = \begin{bmatrix} 17 - 4\sqrt{-3} & -5 + 2\sqrt{-3} & 1 - 14\sqrt{-3} \\ 17 & -5 & -14\sqrt{-3} \\ 7 - 4\sqrt{-3} & -2 + 2\sqrt{-3} & 1 - 6\sqrt{-3} \end{bmatrix}$$

となる. これから $\alpha = 17 - 4\sqrt{-3}$, $\beta = -5 + 2\sqrt{-3}$, $\alpha' = 17$, $\beta' = -5$, $\alpha'' = 7 - 4\sqrt{-3}$, $\beta'' = -2 + 2\sqrt{-3}$, $s = 1 + 14\sqrt{-3}$, $t = -1 - 8\sqrt{-3}$, $r = -14\sqrt{-3}$ であることが読み取れる.

§5. 補足

[DA] 第 236 条の合成の計算も係数域が標数が 2 でない単項イデアル整域であればそのまま通用する.

例. $(a, b, c) = (2, 1, 3)$, $(a', b', c') = (1, -1, -4)$, $n = 1$, $n' = \sqrt{-1}$ とすると $n'^2 \times (b^2 - ac) = (-1) \times (-5) = n^2 \times (b'^2 - a'c') = 1 \times 5 = 5$.

$$X = -2\sqrt{-1}xy' - yx' + (1 - \sqrt{-1})yy',$$

$$Y = xx' - (1 + \sqrt{-1})xy' - 3\sqrt{-1}yy'$$

という置換により

$$3X^2 - 2XY + 2Y^2 = (2x^2 + 2xy + 3y^2)(x'^2 - 2x'y' - 4y'^2).$$ 終わり.

（２０１９年１月１５日提出, まえだ　ひろのぶ, maeda@cc.tuat.ac.jp）