判別式 D が平方数である2次形式 $ax^2+bxy+cy^2$ について

2021年1月
石動高校　片山　喜美

判別式 D が平方数である2次形式

$$f(x,y)=ax^2+bxy+cy^2,\quad a,b,c,\in\mathbb{Z},\quad D=b^2-4bc=m^2\ (m\in\mathbb{N})\quad gcd(a,b,c)=1$$

は、 $Sl(2,\mathbb{Z})$ による変換によって、

$$a'x^2+mxy\quad 0\leqq a'<m,\quad gcd(a',m)=1$$

の形の2次形式に同値となる。
　このとき、 a' はただ1通りに定まる。従って、判別式 $D=m^2\quad(m\in\mathbb{N})$ の2次形式の類数は $\varphi(m)$ である。

例　$f(x,\,y)=3x^2+10xy-8y^2$
判別式は $D=10^2-4\cdot3\cdot(-8)=196=14^2$ と平方数になる。このとき、 $f(x,\,y)=(3x-2y)(x+4y)$
　$x'=3x-2y$ とおく。 $gcd(3,-2)=1$ であるから $3\delta+2\gamma=1$ が整数解を持つ

$$\begin{pmatrix}3&-2\\\gamma&\delta\end{pmatrix}\in SL(2,\,\mathbb{Z})$$

そこで

$$\begin{pmatrix}x'\\y'\end{pmatrix}=\begin{pmatrix}3&-2\\\gamma&\delta\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}$$

とおく。逆に解くと

$$\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}\delta&2\\-\gamma&3\end{pmatrix}\begin{pmatrix}x'\\y'\end{pmatrix}=\begin{pmatrix}\delta x'+2y'\\-\gamma x'+3y'\end{pmatrix}$$

従って、

$$f(x,\,y)=x'\{(\delta x'+2y')+4(-\gamma x'+3y')\}=x'\{(\delta-4\gamma)x'+14y'\}=(\delta-4\gamma)x'^2+14x'y'$$

$3\delta+2\gamma=1$ を満たす一般解は $\gamma=-1+3k,\quad\delta=1-2k\quad(k\in\mathbb{Z})$
　従って、x'^2 の係数は

$$\delta-4\gamma=(1-2k)-4(-1+3k)=5-14k\equiv5\pmod{14}$$

$k=0$ として、 $5x'^2+14x'y'$ とできる。これは、条件を満たす 2 次形式になっている。

$x'=x+4y$ とおく場合はどうか。前と同様に行列を考える。

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 4 \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

逆に解くと

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \delta & -4 \\ -\gamma & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \delta x'-4y' \\ -\gamma x'+y' \end{pmatrix} \qquad (\delta-4\gamma=1)$$

従って、

$$f(x,\,y)=\{3(\delta x'-4y')-2(-\gamma x'+y')\}x'=(3\delta+2\gamma)x'^2-14x'y'$$

これは、条件を満たす 2 次形式になっていない。

一般の $f(x,\,y)=ax^2+bxy+cy^2,\quad D=b^2-4ac=m^2\quad (m\in\mathbb{Z})$ について、段階的に変形を考えていく。

(i) $f(x,\,y)=a\left(x+\dfrac{q}{p}y\right)\left(x+\dfrac{s}{r}y\right) \qquad (p,q,r,s\in\mathbb{Z},\quad gcd(p,q)=gcd(r,s)=1)$ への変形

$ax^2+bxy+cy^2=0\quad a\neq 0$ を x について解くと、$x=\dfrac{-b\pm\sqrt{b^2-4ac}}{2a}=\dfrac{-b\pm m}{2a}$

よって、

$$f(x,\,y)=a\left(x-\frac{-b+m}{2a}\right)\left(x-\frac{-b-m}{2a}\right)$$

$\dfrac{b-m}{2a}=\dfrac{q}{p},\quad \dfrac{b+m}{2a}=\dfrac{s}{r},\quad gcd(p,q)=gcd(r,s)=1$ と既約分数で表せば与えられた形の式になる。//

(ii) $f(x,\,y)=(px+qy)(rs+sy)\quad gcd(p,q)=gcd(r,s)=1$ となることについて
$f(x,\,y)=a\left(x+\dfrac{q}{p}y\right)\left(x+\dfrac{s}{r}y\right)=\dfrac{a}{pr}(px+qy)(rs+sy)$
ここで、$\dfrac{a}{pr}=\dfrac{l}{k}\quad k,l\in\mathbb{Z}\quad k>0\quad (gcd(k,l)=1)$ と既約分数で表す。

$$ax^2+bxy+cy^2=\frac{l}{k}(px+qy)(rx+sy)=\frac{l}{k}\{prx^2+(ps+qr)xy+qsy^2)\}$$

$$\begin{cases} ka &= lpr & \cdots\ ① \\ kb &= l(ps+qr) & \cdots\ ② \\ kc &= lqs & \cdots\ ③ \end{cases}$$

①で　$l|ka$　かつ　$gcd(k,l)=1$　より　$l|a$

同様に ②, ③ より、 $l|b,\quad l|c$ となる。すなわち、 l は a,b,c の公約数である。$gcd(a,b,c)=1$ より $l=1$ である。従って

$$\begin{cases} ka &= pr & \cdots & ①' \\ kb &= ps+qr & \cdots & ②' \\ kc &= qs & \cdots & ③' \end{cases}$$

$|k|>1$ であると仮定する。このとき、 k の素因数の 1 つを μ とする。

- ①$'$ より、 $\mu|pr$ 。従って、 $\mu|p$ もしくは、 $\mu|r$
- ②$'$ より $\mu|p$ のとき、$\mu|qr$ 。よって、 $\mu|q$ もしくは $\mu|r$。このうち $\mu|q$ の場合は $gcd(p,q)=1$ に反するから、 $\mu|r$ 。
- ③$'$ より、 $\mu|qs$ 。従って、 $\mu|q$ もしくは、 $\mu|s$ 。 $\mu\ q$ ならば $gcd(p,q)=1$ に反する。 $\mu\ s$ ならば $gcd(r,s)=1$ に反する。

以上により $|k|=1$。 p の正負を調整して、$k=1$ としてよい。

これらにより、 $f(x,\,y)=(px+qy)(rs+sy)\quad gcd(p,q)=gcd(r,s)=1$ となる。 //

(iii)　$\begin{pmatrix} p & q \\ \gamma & \delta \end{pmatrix} \in Sl(2,\mathbb{Z})$ による変換

$gcd(p,q)=1$ であるから、$p\delta-q\gamma=1$ をみたす $\gamma,\,\delta\in\mathbb{Z}$ が存在する。特殊解 $\gamma_0,\,\delta_0$ およ+び整数 k を用いて、一般解は $\gamma=\gamma_0+pk,\quad \delta=\delta_0+qk$ とできる。

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} p & q \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} px+qy \\ \gamma y+\delta y \end{pmatrix}$$

とおく。逆に解いて、

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \delta & -q \\ -\gamma & p \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \delta x'-qy' \\ -\gamma x'+py' \end{pmatrix}$$

$$\begin{aligned} f(x,\,y)=(px+qy)(rx+sy) &= x'\{r(\delta x'-qy')+s(-\gamma x'+py')\} \\ &= x'\{r(\delta x'-qy')+s(-\gamma x'+py')\} \\ &= x'\{(r\delta-s\gamma)x'+(-rq+ps)y'\}=(r\delta-s\gamma)x'^2+(-rq+ps)x'y' \end{aligned}$$

- $-rq+ps=-r\cdot\dfrac{b-m}{2a}p+p\cdot\dfrac{b+m}{2a}r=2pr\cdot\dfrac{m}{2a}=m$
- $r\delta-s\gamma=r(\delta_0+qk)-s(\gamma_0+pk)=(r\delta_0-s\gamma_0)+(rq-ps)k=(r\delta_0-s\gamma_0)-mk$
  $a'=(r\delta_0-s\gamma_0)-mk$ とおくと、 $0\leqq a'<m$ を満たすような整数 k がただ 1 つ存在する。
  以上により、$\begin{pmatrix} p & q \\ \gamma & \delta \end{pmatrix} \in Sl(2,\mathbb{Z})$ による変換で $a'x^2+mxy\quad D=a^2-4bc=m^2\quad (m\in\mathbb{N})\quad 0\leqq a'<m$ の 2 次形式に移すことができる。

(iv) $a'x^2+mxy$ と $a''x^2+mxy$ が同値ならば、 $a' \equiv a''\pmod m$ である。

$\because)\quad x=\alpha x'+\beta y' \quad y=\gamma x'+\delta y' \quad (\alpha\delta-\beta\gamma=1)$ として、

$$a'x^2+mxy=(\alpha x'+\beta y')\{a'(\alpha x'+\beta y')+m(\gamma x'+\delta y')\}$$

$$=(\alpha x'+\beta y')\{(a'\alpha+m\gamma)x'+(a'\beta+m\delta)y'\}$$

$$=\alpha(a'\alpha+m\gamma)x'^2+\{\alpha(a'\beta+m\delta)+\beta(a'\alpha+m\gamma)\}x'y'+\beta(a'\beta+m\delta)y'^2$$

係数を比較して

$$\begin{cases} a'' &= \alpha(a'\alpha+m\gamma) & \cdots ① \\ m &= \alpha(a'\beta+m\delta)+\beta(a'\alpha+m\gamma) & \cdots ② \\ 0 &= \beta(a'\beta+m\delta) & \cdots ③ \end{cases}$$

③ より、 $\beta=0$ もしくは、$a'\beta+m\delta=0$

- $\beta=0$ のとき
  $\Delta=\alpha\delta-\beta\gamma=\alpha\delta=1$ より $\alpha=\delta=\pm1$
  $\alpha=\delta=1$ のとき、② の右辺 $=1(0+m\cdot1)+0=m=$ 左辺
  ① より $a''=a''+m\gamma\equiv a'\pmod m$
  従って、主張は正しい。
- $a'\beta+m\delta=0$ のとき
  $gcd(a',m)=1$ であるから、 $\beta=mt,\quad \delta=-a't\quad (t\in\mathbb{Z})$ とできる。
  $\Delta=\alpha\delta-\beta\gamma=\alpha(-a't)-mt\gamma=-t(a'\alpha+m\gamma)=1$
  従って、 $t=1$ もしくは $t=-1$
  $t=1$ のとき、 $a'\alpha+m\gamma=-1,\beta=m$
  ② の右辺 $=0+m\cdot(-1)=-m\neq$ 左辺
  $t=-1$ のとき、 $a'\alpha+m\gamma=1,\beta=-m$
  ② の右辺 $=0-m\cdot1=-m\neq$ 左辺
  いずれにしても、 ② は成り立たない。よって、 $a'\beta+m\delta\neq0$

以上により、主張が正しいことが示された。//

具体的な式の変換

判別式が平方数である 2 次形式について、$a'x^2+mxy$ の形を「標準形」と呼ぶことにする。標準形に変形するには、 方程式 $ax\,2+bx+c=0$ の解のうち、大きいほうの解を $\dfrac{q}{p}\quad (gcd(p,q)=1、p>0)$ であるとき、 $px-qy=x'$ とおけばよい。

例 $f(x,\,y)=6x^2-13xy+6y^2$ について

$D=13^2-4\cdot6\cdot=169-144=25=5^2$ であるから $m=5$

$f(x,\,y)=(2x-3y)(3x-2y)$ であるから、 $x'=2x-3y$ とおく。

$$\begin{pmatrix} x \\ y \end{pmatrix}=\begin{pmatrix} \delta & 3 \\ -\gamma & 2 \end{pmatrix}\begin{pmatrix} x' \\ y' \end{pmatrix}=\begin{pmatrix} \delta x'+3y' \\ -\gamma x'+2y' \end{pmatrix} \qquad (2\delta+3\gamma=1)$$

従って、

$$f(x,\,y) = x'\{3(\delta x' + 3y') - 2(-\gamma x' + 2y')\} = (3\delta + 2\gamma)x'^2 + 5x'y'$$

$2\delta + 3\gamma = 1$ の一般解は $\gamma = 1 + 2k, \quad \delta = -1 - 3k \quad (k \in \mathbb{Z})$

$$f(x,\,y) = \{3(-1-3k) + 2(1+2k)\}x'^2 + 5x'y' = (-1-5k)x'^2 + 5x'y'$$

$k = -1$ として、標準形は $4x^2 + 5xy$