平成13年度　学位論文

整係数２元２次形式について

兵庫教育大学大学院　学校教育研究科
教科・領域教育専攻　自然系コース
Ｍ００１８８Ｃ　脇　田　伸　男

目 次

0章　序

本論文では Gauss による 2 元 2 次形式の簡約理論について述べる. 整数 a, b, c を係数とする x, y についての同次 2 次式

$$f(x,y) = ax^2 + bxy + cy^2 = \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

を整 (数) 係数 2 元 2 次形式といい, $D = b^2 - 4ac$ を f の判別式という. 以下 2 次形式といえば, 特に断らない限り整係数 2 元 2 次形式を指す.

整係数 1 次方程式 $ax + by = c$ の整数解を見つける問題は古代バビロニアの時代から研究され, ギリシヤ時代にその解法が完成したといわれる. 一般に整係数方程式の整数解を求める問題に現れる方程式は Diophantus 方程式とか不定方程式などと呼ばれる. 1 次不定方程式 $ax + by = c$ が解をもつ条件は a と b の最大公約数 d が c を割り切ることであり, そのとき 1 組の整数解 $x = \alpha$, $y = \beta$ と (整数) パラメータ t を用いて一般解が $x = \alpha + (\frac{b}{d})t$, $y = \beta - (\frac{a}{d})t$ と表される.

2 次不定方程式 $x^2 + y^2 = z^2$ の自然数解はピタゴラス数として知られており, 古代バビロニアの遺跡から発見された粘土板には巨大なピタゴラス数が記録されている. また Fermat(1601〜1665) はその書簡に $4k+1$ 型 (4 で割って 1 余る整数) の素数 p は 2 つの平方数の和として表されること, 言い換えれば 2 次不定方程式 $x^2 + y^2 = p$ が解をもつこと, また $3k+1$ 型の素数 p に対して 2 次不定方程式 $x^2 + 3y^2 = p$ が解をもつこと, などを記している. しかし $ax^2 + bxy + cy^2$ がどのような整数を表し得るかといった 2 次不定方程式の一般的理論は 19 世紀になって初めてその土台が築かれることになる.

Gauss(1777〜1855) はその著 “Disquisitiones Arithmeticae” で Legendre の平方剰余の相互法則の証明を与えると共に 2 元 2 次形式の理論を作り上げる. Gauss は個々の 2 次形式がどのような数を表すかといった問題を越えて, 2 次形式全体を研究の対象とした. 2 次形式の間に対等という同値関係を導入し, この同値関係で判別式が不変であること, 任意の 2 次形式がある簡約 2 次形式に対等であることを示し, これより同じ判別式をもつ 2 次形式が有限個 (類数) の同値類に分割されることを示した. これが Gauss の簡約理論と

呼ばれるものである. Gauss の簡約理論により 2 次形式がどのような整数を表し得るかといった問題が見通しよく解決できるようになったのである.

以下, 論文の構成について述べる.

1 章では 2 次形式を考察するにあたり必要となる初等整数論および群の基本事項などについて説明するが一部を除き定理の証明を省略し, 参考文献をあげるにとどめた.

2 章では連分数の基本事項について述べる. この章の内容は 5 章で正の判別式をもつ 2 次形式を考察する際に必要となる.

§2.1 では, 有理数の連分数分展開について, §2.2 では無理数の連分数展開について述べる. 無理数の連分数展開が無限連分数となること, 任意の無限連分数が無理数に収束することなどを示す. 連分数展開をする際に現れるいくつかの数列とその間の関係式が重要である.

3 章では (整係数) 2 次形式の間に対等と呼ばれる同値関係を導入し, 対等な 2 次形式が同じ判別式をもつことを示す. これより同じ判別式をもつ 2 次形式がいくつかの同値類に分割され, これらの同値類の個数としてその判別式の類数が定義される.

§3.1 では 2 次形式, 判別式, 特殊 1 次変換, 2 次形式の間の対等および正に対等, などの基本的概念を導入する.

§3.2 では特殊 1 次変換によりモデュラ変換が定まること, モデュラ変換が整係数既約 2 次式の根である 2 次代数的数の上の変換を引き起こすことなどを示す. これより 2 次代数的数の間にも対等, および正に対等という同値関係が定義される.

§3.3 では 2 次形式に対応する 2 次式の根を第 1 根, 第 2 根に区別し, 同じ判別式をもつ 2 つの 2 次形式が正に対等であることと, 対応する 2 次式の第 1 根が正に対等であることとが同値であることを示す.

4 章では負の判別式 D に対する類数が有限であることを示す. 負の判別式をもつ 2 次形式は正と負の 2 種類に分けることができ, 対等関係を考察する際, 正の 2 次形式のみを考察すればよい. 従って 4 章では正の 2 次形式のみを扱う.

§4.1 では簡約 2 次形式を定義し, 与えられた判別式をもつ簡約 2 次形式が有限個であることを示す.

§4.2 では正の 2 次形式が, 簡約 2 次形式であることと, 対応する 2 次式の第 1 根が基本領域と呼ばれる領域内にあることとが同値であることを示す. さらに任意に与えられた正の 2 次形式に対して, それと正に対等な簡約 2 次形式が唯 1 つ存在することを示し, 類数

が有限であることを導く. これより虚部が正の 2 次代数的数に正に対等な点が基本領域内に唯一つ存在することがわかる.

最後の §4.3 ではいくつかの負の判別式の値に対して簡約 2 次形式と類数を求める計算例を述べる.

5 章では正の判別式 D に対する類数が有限であることを示す.

証明の流れは 4 章と同様である. 簡約 2 次形式を定義し, 判別式 D の簡約 2 次形式が有限個であること, 任意の 2 次形式がある簡約 2 次形式に対等であることを示す. しかし証明の様相は 4 章とは異なり, 2 章で準備した連分数が重要な役割を演じる. また 2 次形式に対等な簡約 2 次形式も一意に定まるとは限らない.

§5.1 では簡約 2 次形式, 簡約 2 次無理数を定義し, 与えられた判別式 D をもつ簡約 2 次形式が有限個であることを示す.

§5.2 では 2 次無理数, 簡約 2 次無理数がそれぞれ循環連分数, 純循環連分数で表されること, 任意の 2 次無理数がある簡約 2 次無理数に正に対等であることを示す. これより正の判別式をもつ 2 次形式の類数が有限であることが導かれる. 次に最小周期が m の簡約 2 次無理数 ξ の中間連分数を

$$\xi = [k_0, k_1, \ldots, k_{n-1}, \xi_n] \quad (n = 1, 2, \ldots, m-1)$$

としたとき ξ と対等な簡約 2 次無理数が $\xi_0 = \xi$, ξ_1, ξ_2,...,ξ_{m-1} のみであることを証明する. これは狭義の類数を計算する方法の根拠となる. 最後にいくつかの正の判別式の値に対して簡約 2 次形式と類数を求める計算例を述べる.

6 章では 2 次形式による整数の表示問題について述べる. 2 次形式 $f(x, y) = ax^2 + bxy + cy^2$ と整数 n に対して $f(x, y) = n$ を満たす整数 x, y が存在するとき n は f によって表示されるという. この章では「与えられた 2 次形式が自然数 n を表示するか」, 「与えられた判別式をもつ 2 次形式の中に自然数 n を表示するものが存在するか」等の問題について考察する.

1章　準備

この章では2次形式を考察するにあたり必要となる初等整数論および群の基本事項などについて説明するが, 一部を除き定理の証明を省略した. それらの定理の証明については参考文献 [1, 4, 2, 6] などを参考にされたい.

なお, 本論文では集合や写像, 同値関係などについての基本的事項, 例えば参考文献 [1, 1章2節], [4, 1章] にあるようなものは既知とする.

論文を通して次の記号を用いる. ただし i は $i^2 = -1$ を満たす数である.

$$
\begin{array}{lcl}
\mathbb{N} & = & \{1, 2, 3, 4, ...\} \quad \text{自然数全体} \\
\mathbb{Z} & = & \{0, \pm 1, \pm 2, \pm 3, ...\} \quad \text{整数全体} \\
\mathbb{Q} & = & \left\{ \frac{b}{a} \,\middle|\, a, b \in \mathbb{Z},\ a \neq 0 \right\} \quad \text{有理数全体} \\
\mathbb{R} & = & \text{実数全体} \\
\mathbb{C} & = & \{a + ib \mid a, b \in \mathbb{R}\} \quad \text{複素数全体} \\
\lfloor x \rfloor & & \text{ガウス記号. 実数 } x \text{ を越えない最大の整数を表す.}
\end{array}
$$

1.1　初等整数論の基本事項

以下この章において a, b, c,... は特に断らない限り整数を表すものとする.

定理 1.1 (除法の定理) 整数 a と自然数 b が与えられたとき

$$a = bq + r, \quad 0 \leq r < b$$

を満たす整数 q, r が一意に存在する.

q を a を b で割った商, r を a を b で割った余りという.

整数 a, b, c が $a = bc$ をみたすとき a は b の倍数である, b は a の約数である, b は a を割る, などといい $b \mid a$ と表す.

以下 $a \mid b$ とあれば a, b が整数であることは仮定されているものとする.

$a \mid b$ かつ $a \mid c$ のとき a を b, c の公約数, $a \mid c$ かつ $b \mid c$ のとき c を a, b の公倍数という.

$(a, b) \neq (0, 0)$ のとき, すなわち a, b のいずれか一方が 0 でないとき a, b の公約数の中に最大のものが存在する. それを a, b の最大公約数といい $(a,\ b)$ と表す. ただし $(0, 0) = 0$ と定める.

$(a, b) = 1$ のとき a と b は互いに素であるという.

1.2 平方剰余

定義 1.2 n は自然数とする. 整数 a, b が $n \mid a - b$ を満たすとき $a \equiv b \pmod{n}$ と表し, n を法 (modulus) として a は b に合同であるという.

定義 1.3 (Legendre の記号) p を奇素数, a を p と互いに素な整数とする. 合同方程式 $x^2 \equiv a \pmod{p}$ が解をもつとき a は法 p で平方剰余であるといい $\left(\dfrac{a}{p}\right) = 1$ と表す. 解をもたないときは法 p で平方非剰余であるといい $\left(\dfrac{a}{p}\right) = -1$ と表す.

$p \mid a$ のときは $\left(\dfrac{a}{p}\right) = 0$ と定める.

$\left(\dfrac{*}{p}\right)$ を Legendre の記号, または平方剰余記号という.

$\left(\dfrac{ab}{p}\right) = \left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right)$ が成り立つ.

定理 1.4 (Euler の規準) a が奇素数 p の倍数でないとき次がなり立つ.

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

定理 1.5 (第１補充法則)

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod{4} \\ -1, & p \equiv 3 \pmod{4} \end{cases}$$

定理 1.6 (第２補充法則)

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv 1,7 \pmod 8 \\ -1, & p \equiv 3,5 \pmod 8 \end{cases}$$

定理 1.7 (平方剰余の相互法則) p, q が相異なる奇素数のとき次がなり立つ.

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

1.3 群論の基本事項

定義 1.8 集合 G に 2 項演算が定義され次の条件を満たすとき G を群という.

(i) 結合法則が成り立つ. すなわち任意の $a, b, c \in G$ に対して $(ab)c = a(bc)$ が成り立つ.

(ii) ある元 $e \in G$ が存在して任意の $a \in G$ に対して $ae = ea = a$ が成り立つ.

(iii) 任意の $a \in G$ に対して $aa^{-1} = a^{-1}a = e$ を満たす a^{-1} が存在する.

上の条件 (ii) を満たす e は一意に定まる. e を G の単位元という. また a に対して条件 (iii) を満たす a^{-1} は一意に定まる. a^{-1} を a の逆元という.

定義 1.9 群 G の部分集合 $H \neq \emptyset$ が次の条件を満たすとき G の部分群であるといい, $H \leq G$ と表す.

(i) 任意の $a, b \in H$ に対して $ab \in H$ である.

(ii) $a \in H$ ならば $a^{-1} \in H$ である.

部分群 H は G の演算に関してそれ自身群となる.

定理 1.10 有理数を成分とする n 次正則行列全体 $GL(n, \mathbb{Q})$ は行列の積を演算とする群である.

定理 1.11 集合 X から X への全単射全体は写像の合成を積として群をなす. これを X 上の対称群, 又は変換群といい S_X などと表す.

X 上の対称群の元を X 上の変換または置換という.

定義 1.12 群 G から群 G' への写像 f が条件：

任意の $a, b \in G$ に対して $f(ab) = f(a)f(b)$

を満たすとき準同型 (写像) であるという. 特に f が全単射であるとき f を同型 (写像) という. またこのとき G と G' は同型であるといい $G \simeq G'$ と表す.

定義 1.13 G の部分群 N が G の任意の元 g にたいして $N = g^{-1}Ng$ を満たすとき G の正規部分群であるといい $N \trianglelefteq G$ と表す.

群 G と $H \leq G$ に対して

$$aH = \{ah \,|\, h \in H\}$$

とおき H の G における a を含む (左) 剰余類という. H の G における剰余類全体を G/H と表す.

定理 1.14 $N \trianglelefteq G$ のとき $G/N \ni aN, bN$ に対してその積を $(aN)(bN) = abN$ と定義することにより G/N が群となる. これを G の N による剰余群という.

$f : G \mapsto G'$ が群 G から群 G' への準同型であるとき

$$Im(f) = \{f(g) \mid g \in G\}, \qquad Ker(f) = \{x \in G \mid f(x) = 1\}$$

とおき $Ker(f)$ を f の核, $Im(f)$ を f の像という.

定理 1.15 (準同型定理) $f : G \mapsto G'$ が準同型ならば $Ker(f) \trianglelefteq G$, $Im(f) \leq G'$ であり $Im(f) \simeq G/Ker(f)$ が成り立つ.

特殊１次変換のなす群

整数を成分とする２次行列のなす集合を次のように定める.

$$SL(\mathbb{Z})^{\pm} = \left\{ \left[\begin{array}{cc} r & s \\ t & u \end{array} \right] \;\middle|\; r,s,t,u \in \mathbb{Z}, ru-st = \pm 1 \right\}$$

$$SL(\mathbb{Z})^{+} = \left\{ \left[\begin{array}{cc} r & s \\ t & u \end{array} \right] \;\middle|\; r,s,t,u \in \mathbb{Z}, ru-st = 1 \right\},$$

$$SL(\mathbb{Z})^{-} = SL(\mathbb{Z})^{\pm} - SL(\mathbb{Z})^{+}$$

$SL(\mathbb{Z})^{\pm}$の元を特殊１次変換, $SL(\mathbb{Z})^{+}$の元を正の特殊１次変換, $SL(\mathbb{Z})^{-}$ の元を負の特殊１次変換という.

定理 1.16 $SL(\mathbb{Z})^{+}$および $SL(\mathbb{Z})^{\pm}$は行列の乗法に関して群をなす.

Proof　$SL(\mathbb{Z})^{+}$についても同様であるから $SL(\mathbb{Z})^{\pm}$についてのみ示す.

定理1.10より有理数係数２次正則行列全体 $GL(2,\mathbb{Q})$ は行列の乗法に関して群をなす. $SL(\mathbb{Z})^{\pm}$は $GL(2,\mathbb{Q})$ の部分集合であるから部分群の定義1.9の条件を満たすことを示せばよい.

$A, B \in SL(\mathbb{Z})^{\pm}$ に対して $|AB| = |A||B| = \pm 1$ であるから $AB \in SL(\mathbb{Z})^{\pm}$ である.

また $SL(\mathbb{Z})^{\pm} \ni A = \left[\begin{array}{cc} r & s \\ t & u \end{array} \right]$ に対して $A^{-1} = \left[\begin{array}{cc} u & -s \\ -t & r \end{array} \right] \in SL(\mathbb{Z})^{\pm}$ である.

以上から $SL(\mathbb{Z})^{\pm}$は $GL(2,\mathbb{Q})$ の部分群であり, それ自身群である. ∎

モデュラ変換

$SL(\mathbb{Z})^{\pm}$ の元 $T = \left[\begin{array}{cc} r & s \\ t & u \end{array} \right]$ と $t\xi + u \neq 0$ を満たす $\xi \in \mathbb{C}$ に対して

$$T(\xi) = \frac{r\xi + s}{t\xi + u}$$

により１つの複素数が定まる. この対応を $\xi \mapsto T(\xi)$ をモデュラ変換という.

さて $SL(\mathbb{Z})^{\pm}$ の元

$$T = \begin{bmatrix} r & s \\ t & u \end{bmatrix}, \quad T' = \begin{bmatrix} r' & s' \\ t' & u' \end{bmatrix}$$

に対して $T'(\xi), T(T'(\xi))$ が定まるとき

$$T(T'(\xi)) = \frac{rT'(\xi)+s}{tT'(\xi)+u} = \frac{r\dfrac{r'\xi+s'}{t'\xi+u'}+s}{t\dfrac{r'\xi+s'}{t'\xi+u'}+u} = \frac{(rr'+st')\xi+(rs'+su')}{(tr'+ut')\xi+(ts'+uu')}$$

となるので $T(T'(\xi)) = TT'(\xi)$ が成り立つ.

定理 1.17 $SL(\mathbb{Z})^{\pm} \ni T, T'$ に対して $T'(\xi), T(T'(\xi))$ が定まるとき $T(T'(\xi)) = TT'(\xi)$ が成り立つ.

2章　連分数

この章では5章で必要となる連分数の基本事項について述べる.

§2.1では, 有理数の連分数展開について, §2.2では無理数の連分数展開について述べる. 無理数の連分数展開が無限連分数となること, 任意の無限連分数が無理数に収束することなどを示す. 連分数展開をする際に現れるいくつかの数列とその間の関係式が5章で利用される.

2.1　有理数の連分数展開

有理数 ω_0 に対して以下の手順で有理数の (有限) 列 $\{\omega_0, \omega_1, ...\}$ と整数の (有限) 列 $\{k_0, k_1, ...\}$ が定まる.

- $k_0 = \lfloor \omega_0 \rfloor$ とおく.
- $\omega_0 \neq k_0$ のときは $\omega_1 = \dfrac{1}{\omega_0 - k_0}$ とおくと ω_1 も有理数で $0 < \omega_0 - k_0 < 1$ であるから $\omega_1 > 1$ である.
- 有理数 $\omega_1 > 1$ に対して自然数 $k_1 = \lfloor \omega_1 \rfloor$ が定まる. $\omega_1 \neq k_1$ のときは $\omega_2 = \dfrac{1}{\omega_1 - k_1}$ とおくと ω_2 も有理数で $\omega_2 > 1$ である.
- 以下同様にして有理数 $\omega_j > 1$ が定まれば自然数 $k_j = \lfloor \omega_j \rfloor$ が定まる. ここで $1 \leq j \leq n$ のとき $k_j \in \mathbb{N}$ であることを注意しておく.
- $\omega_j \neq k_j$ のときは $\omega_j = \dfrac{d}{c}\ (c > 0)$ と既約分数表示すれば $k_j = q, \omega_{j+1} = \dfrac{c}{r}$ となる. ただし q, r はそれぞれ d を c で割った商と余りである. これより ω_{j+1} を既約分数表示したときの分母は c より小さくなる. 従ってこの操作を続けると, ある n において $\omega_n = k_n$ となり, 有理数の (有限) 列 $\{\omega_0, \omega_1, ..., \omega_n\}$ と整数の (有限) 列 $\{k_0, k_1, ..., k_n\}$ が定まる.

数列 $\{\omega_0, \omega_1, ..., \omega_n\}$ と $\{k_0, k_1, ..., k_n\}$ に対して

$$[k_0, \omega_1], \quad [k_0, k_1, \omega_2], \quad [k_0, k_1, k_2, \omega_3], \quad ..... \quad , [k_0, ..., k_{n-1}, \omega_n]$$

を順次, 次のように定める. $\omega_n = k_n$ に注意されたい.

$$[k_0, \omega_1] = k_0 + \frac{1}{\omega_1}$$

$$[k_0, k_1, \omega_2] = k_0 + \cfrac{1}{k_1 + \cfrac{1}{\omega_2}}$$

$$[k_0, k_1, k_2, \omega_3] = k_0 + \cfrac{1}{k_1 + \cfrac{1}{k_2 + \cfrac{1}{\omega_3}}}$$

$$\vdots \qquad\qquad \vdots$$

$$[k_0, k_1, ..., k_{n-1}, k_n] = k_0 + \cfrac{1}{k_1 + \cfrac{1}{\ddots \quad \ddots \quad + \cfrac{1}{k_{n-1} + \cfrac{1}{k_n}}}}$$

明らかに等式

$$\omega_0 = [k_0, \omega_1] = [k_0, k_1, \omega_2] = \cdots = [k_0, ..., k_{n-1}, k_n]$$

が成り立つ. 最後の式 $[k_0, ..., k_{n-1}, k_n]$ を長さ $n+1$ の有限連分数, $\omega_0 = [k_0, ..., k_{n-1}, k_n]$ を有理数 ω_0 の連分数展開という. 一般に整数 k_0 と自然数 $k_1, .., k_n$ が任意に与えられたとき上のような $[k_0, k_1, ..., k_{n-1}, k_n]$ を連分数と呼ぶ. 以上より次の定理は明かである.

定理 2.1 任意の有理数は有限連分数展開される.

整数 h_0 と自然数 $h_1, ..., h_n$ が任意に与えられたとき, 連分数 $[h_0, ..., h_{n-1}, h_n]$ は 1 つの有理数 α を表す. ここで $h_n > 1$ ならば $\alpha = [h_0, h_1, ..., h_n]$ は有理数 α の連分数展開となる. $h_n = 1$ の場合は $\alpha = [h_0, h_1, ..., h_{n-1} + 1]$ が有理数 α の連分数展開となる. これを補題として述べておく.

補題 2.2 任意に与えられた整数 h_0 と自然数 $h_1,..,h_n$ に対して $\alpha=[h_0,...,h_n]$ とおくと $\alpha=[h_0,...,h_n]$ または $\alpha=[h_0,...,h_{n-1}+1]$ が有理数 α の連分数展開である.

有理数 ω の長さ $n+1$ の連分数展開 $\omega=[k_0,k_1,...,k_{n-1},k_n]$ において $k_n=1$ であるとき最後の部分は

$$\cdots+\cfrac{1}{k_{n-1}+\cfrac{1}{k_n}}=\cdots+\cfrac{1}{k_{n-1}+1}$$

となるから $\omega=[k_0,k_1,...,k_{n-1}+1]$ と長さ n の連分数に展開できる. また $k_n>1$ であるときは

$$\cdots+\cfrac{1}{k_n}=\cdots+\cfrac{1}{k_n-1+\cfrac{1}{1}}$$

となるから $\omega=[k_0,k_1,...,k_n-1,1]$ と長さ $n+2$ の連分数に展開できる. これより次の定理を得る.

定理 2.3 有理数は偶数, 奇数両方の長さの有限連分数として表すことができる.

例えば $\dfrac{61}{13}$ は

$$\frac{61}{13}=4+\frac{1}{\frac{13}{9}}=4+\cfrac{1}{1+\cfrac{1}{\frac{9}{4}}}=4+\cfrac{1}{1+\cfrac{1}{2+\frac{1}{4}}}=[4,1,2,4]$$

と長さ 4 の連分数に展開されるが, $\dfrac{61}{13}=[4,1,2,3,1]$ と長さ 5 の連分数にも展開できる.

さて有理数 $\omega=\omega_0$ から定まる数列 $\{k_0,k_1,...,k_n\}$ に対して

$$T_j=\begin{bmatrix}k_j & 1\\ 1 & 0\end{bmatrix}\qquad(j=0,1,2,..,n)$$

は負の特殊1次変換である．$\omega_j\ (0 \leq j \leq n)$ は 0 でないので p.8 で述べたことから次が成り立つ．

$$\begin{aligned}
\omega_0 = k_0 + \frac{1}{\omega_1} \quad &\text{より} \quad \omega_0 = \frac{k_0\omega_1 + 1}{\omega_1} = T_0(\omega_1), \\
\omega_1 = k_1 + \frac{1}{\omega_2} \quad &\text{より} \quad \omega_1 = \frac{k_1\omega_2 + 1}{\omega_2} = T_1(\omega_2), \\
\vdots \qquad\qquad &\qquad\qquad \vdots \\
\omega_{n-1} = k_{n-1} + \frac{1}{\omega_n} \quad &\text{より} \quad \omega_{n-1} = \frac{k_{n-1}\omega_n + 1}{\omega_n} = T_{n-1}(\omega_n)
\end{aligned}$$

このとき定理 1.17 より

$$\omega = T_0T_1\cdots T_{j-2}T_{j-1}(\omega_j), \quad j = 1, 2, ..., n$$

が成り立つ．ここで

$$T_0T_1\cdots T_{j-2}T_{j-1} = \begin{bmatrix} p_j & p'_j \\ q_j & q'_j \end{bmatrix}$$

とおくと

$$\begin{bmatrix} p_j & p'_j \\ q_j & q'_j \end{bmatrix} = \begin{bmatrix} p_{j-1} & p'_{j-1} \\ q_{j-1} & q'_{j-1} \end{bmatrix} \begin{bmatrix} k_{j-1} & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} k_{j-1}p_{j-1} + p'_{j-1} & p_{j-1} \\ k_{j-1}q_{j-1} + q'_{j-1} & q_{j-1} \end{bmatrix}$$

となる．従って

$$T_0T_1\cdots T_{j-2}T_{j-1} = \begin{bmatrix} p_j & p_{j-1} \\ q_j & q_{j-1} \end{bmatrix}, \quad \begin{cases} p_j = k_{j-1}p_{j-1} + p_{j-2} \\ q_j = k_{j-1}q_{j-1} + q_{j-2} \end{cases} \tag{2.1}$$

および

$$\omega = [k_0, k_1, \ldots, k_{j-1}, \omega_j] = T_0T_1\cdots T_{j-2}T_{j-1}(\omega_j) = \frac{p_j\omega_j + p_{j-1}}{q_j\omega_j + q_{j-1}} \tag{2.2}$$

が成り立つ．特に $j = n$ のときは $\omega_n = k_n$ であるから

$$\omega = [k_0, k_1, \ldots, k_{n-1}, k_n] = T_0T_1\cdots T_{n-2}T_{n-1}(k_n) = \frac{p_nk_n + p_{n-1}}{q_nk_n + q_{n-1}} \tag{2.3}$$

が成り立つ．ここで等式

$$[k_0, \ldots, x] = \frac{p_nx + p_{n-1}}{q_nx + q_{n-1}}$$

は x について恒等式となるので $x = 1$, すなわち $k_n = 1$ であっても 式 (2.3) が成り立つ. 従って定理 2.3 のように連分数の最終項を変更しても上式 (2.3) は成立する. また

$$\begin{vmatrix} p_j & p_{j-1} \\ q_j & q_{j-1} \end{vmatrix} = |T_0 T_1 \cdots T_{j-2} T_{j-1}| = (-1)^j \tag{2.4}$$

であることにも注意されたい.

2.2 無理数の連分数展開

無理数 ω_0 に対して, 無理数の無限列 $\{\omega_0, \omega_1, ..\}$ と整数の無限列 $\{k_0, k_1, ...\}$ が以下の手順で定まる.

- $k_0 = \lfloor \omega_0 \rfloor$ とおく. ω_0 が無理数であるから $\omega_0 \neq k_0$ である.
- $0 < \omega_0 - k_0 < 1$ であるから $\omega_1 = \dfrac{1}{\omega_0 - k_0}$ とおけば ω_1 は無理数で $\omega_1 > 1$ である.
- $k_1 = \lfloor \omega_1 \rfloor$ とおけば $k_1 \in \mathbb{N}$ である.
- $0 < \omega_1 - k_1 < 1$ であるから $\omega_2 = \dfrac{1}{\omega_1 - k_1}$ とおけば ω_2 も無理数で $\omega_2 > 1$ である.
- 以下, 無理数 $\omega_n > 1$ と自然数 $k_n = \lfloor \omega_n \rfloor$ が定まったとき, 同様にして無理数 $\omega_{n+1} = \dfrac{1}{\omega_n - k_n} > 1$ と自然数 $k_{n+1} = \lfloor \omega_{n+1} \rfloor$ が定まる.

有理数の場合と異なり, この操作は無限に続くので無理数の無限列 $\{\omega_0, \omega_1, ...\}$ と整数の無限列 $\{k_0, k_1, ...\}$ が定まる. ここで $j \geq 1$ のとき $k_j \in \mathbb{N}$ であることを注意しておく.

数列 $\{\omega_0, \omega_1, ...\}$ と $\{k_0, k_1, ...\}$ の定め方から次が成り立つ.

$$\omega_0 = [k_0, \omega_1] = k_0 + \frac{1}{\omega_1}$$

$$= [k_0, k_1, \omega_2] = k_0 + \cfrac{1}{k_1 + \cfrac{1}{\omega_2}}$$

$$= [k_0, k_1, k_2, \omega_3] = k_0 + \cfrac{1}{k_1 + \cfrac{1}{k_2 + \cfrac{1}{\omega_3}}}$$

$$\vdots \qquad\qquad \vdots$$

$$= [k_0, k_1, ..., k_{n-1}, \omega_n] = k_0 + \cfrac{1}{k_1 + \cfrac{1}{\ddots \quad \ddots \quad \ddots \quad + \cfrac{1}{k_{n-1} + \cfrac{1}{\omega_n}}}}$$

$[k_0, k_1, ..., k_{n-1}, \omega_n]$ を無理数 ω_0 の中間連分数ということにする.

以下において任意に与えられた整数の無限列 $\{h_j\}_{j\geq 0}$, $h_j \in \mathbb{N}$ $(j \geq 1)$, に対して極限

$$\lim_{n\to\infty} [h_0, h_1, ..., h_n] = [h_0, h_1, h_2, ...]$$

が 1 つの無理数を定めることと, 無理数 ω_0 が整数列 $\{k_j\}$ により

$$\omega_0 = \lim_{n\to\infty} [k_0, k_1, ..., k_n] = [k_0, k_1, k_2, ...]$$

と無限連分数展開されることを示す.

次の補題は上で示したことから容易に導かれる (証明略).

補題 2.4 任意に与えられた整数 h_0 と自然数 $h_1, h_2, .., h_{n-1},$ および実数 $\beta > 1$ に対して

$$\alpha = [h_0, h_1, ..., h_{n-1}, \beta]$$

とおくと $[h_0, h_1, ..., h_{n-1}, \beta]$ は α の中間連分数である.

さて無理数 $\omega = \omega_0$ から定まる無限列 $\{\omega_j\}$ と $\{k_j\}$ に対して

$$T_n = \begin{bmatrix} k_n & 1 \\ 1 & 0 \end{bmatrix} \qquad (n = 0, 1, 2, ...)$$

とおけば T_n は次のモデュラ変換 (cf. p.8) を引き起こす.

$$\begin{aligned}
\omega_0 = k_0 + \frac{1}{\omega_1} \quad &\text{より} \quad \omega_0 = \frac{k_0\omega_1 + 1}{\omega_1} = T_0(\omega_1) \\
\omega_1 = k_1 + \frac{1}{\omega_2} \quad &\text{より} \quad \omega_1 = \frac{k_1\omega_2 + 1}{\omega_2} = T_1(\omega_2) \\
&\vdots \qquad\qquad\qquad\quad \vdots \\
\omega_n = k_n + \frac{1}{\omega_{n+1}} \quad &\text{より} \quad \omega_n = \frac{k_n\omega_{n+1} + 1}{\omega_{n+1}} = T_n(\omega_{n+1}) \\
&\vdots \qquad\qquad\qquad\quad \vdots
\end{aligned}$$

これより

$$\omega = T_0T_1 \cdots T_{n-2}T_{n-1}(\omega_n)$$

となる. ここで

$$T_0T_1 \cdots T_{n-2}T_{n-1} = \begin{bmatrix} p_n & p'_n \\ q_n & q'_n \end{bmatrix}$$

とおくと, 有理数の場合と同様にして

$$T_0T_1 \cdots T_{n-2}T_{n-1} = \begin{bmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{bmatrix}, \quad \begin{cases} p_j = k_{j-1}p_{j-1} + p_{j-2} \\ q_j = k_{j-1}q_{j-1} + q_{j-2} \end{cases} \tag{2.5}$$

および

$$\omega = [k_0, k_1, \ldots, k_{n-1}, \omega_n] = T_0T_1 \cdots T_{n-2}T_{n-1}(\omega_n) = \frac{p_n\omega_n + p_{n-1}}{q_n\omega_n + q_{n-1}} \tag{2.6}$$

が得られる. また

$$\begin{vmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{vmatrix} = |T_0T_1 \cdots T_{n-2}T_{n-1}| = (-1)^n \tag{2.7}$$

が成り立つ. ここで整数列 $\{q_j\}$ は

$$q_0 = 0, \quad q_1 = 1, \quad q_0 < q_1 \leq q_2 < q_3 < \cdots\cdots, \quad \lim_{n\to\infty} q_n = \infty \tag{2.8}$$

を満たすことを注意しておく. さらに 式 (2.6) より

$$\begin{aligned}\left|\omega - \frac{p_n}{q_n}\right| &= \left|\frac{p_n\omega_n + p_{n-1}}{q_n\omega_n + q_{n-1}} - \frac{p_n}{q_n}\right| = \left|\frac{-(p_nq_{n-1} - p_{n-1}q_n)}{q_n(q_n\omega_n + q_{n-1})}\right| \\ &= \left|\frac{(-1)^{n-1}}{q_n(q_n\omega_n + q_{n-1})}\right| = \frac{1}{q_n(q_n\omega_n + q_{n-1})} \\ &< \frac{1}{q_n(q_nk_n + q_{n-1})} = \frac{1}{q_nq_{n+1}}\end{aligned}$$

となるので次の補題を得る.

補題 2.5 無理数 ω の連分数展開に現れる整数列 $\{k_j\}$ から式 (2.5) で定まる整数列 $\{p_j, q_j\}$ について次が成り立つ.

$$\left|\omega - \frac{p_n}{q_n}\right| < \frac{1}{q_nq_{n+1}} < \frac{1}{q_n^2}$$

補題 2.6 無理数 ω の連分数展開に現れる整数列 $\{k_j\}$ と $\{p_j, q_j\}$ について次が成り立つ.

$$\frac{p_n}{q_n} = [k_0, k_1, \dots, k_{n-1}] \qquad (n = 1, 2, \dots)$$

Proof　$\alpha = [k_0, k_1, \dots, k_{n-1}]$ とおく. 補題 2.2 よりこれは有理数 α の連分数展開であるか, 定理 2.3 のように連分数の最終項を変更したものである. 従って式 (2.3) と式 (2.1) より

$$[k_0, k_1, \dots, k_{n-1}] = \frac{p_{n-1}k_{n-1} + p_{n-2}}{q_{n-1}k_{n-1} + q_{n-2}} = \frac{p_n}{q_n}$$

を得る. ∎

定理 2.7 無理数 ω の連分数展開に現れる整数列 $\{k_j\}$ について次が成り立つ.

$$\lim_{n\to\infty}[k_0, k_1, \dots, k_n] = \omega$$

Proof　補題 2.6 と補題 2.5 より

$$|\omega - [k_0, k_1, \dots, k_n]| = \left|\omega - \frac{p_{n+1}}{q_{n+1}}\right| < \frac{1}{{q_{n+1}}^2}$$

となる. 式 (2.8) より $\lim_{n\to\infty} q_n = \infty$ であるから $\lim_{n\to\infty}[k_0, k_1, \dots, k_n] = \omega$ を得る. ∎

$[k_0, k_1, \ldots, k_n, ...]$ を無限連分数, $\omega = [k_0, k_1, \ldots, k_n, ...]$ を ω の無限連分数展開という.

定理 2.8 $n \geq 1$ のとき $k_n \geq 1$ となる整数列 $\{k_n\}$ に対して極限

$$\eta = \lim_{n\to\infty} [k_0, k_1, \ldots, k_n]$$

が存在し, 無限連分数展開 $\eta = [k_0, k_1, \ldots, k_n, \ldots]$ が成り立つ. 特に η は無理数である.

Proof　整数列 $\{k_n\}$ に対して

$$T_n = \begin{bmatrix} k_n & 1 \\ 1 & 0 \end{bmatrix}, \quad T_0T_1\cdots T_{n-2}T_{n-1} = \begin{bmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{bmatrix}$$

とおけば整数列 $\{p_n\}$, $\{q_n\}$ が定まる. ここで補題 2.6 より

$$\frac{p_n}{q_n} = [k_0, k_1, \ldots, k_{n-1}]$$

が成り立つ. 一方, 式 (2.7) より

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{p_nq_{n-1} - p_{n-1}q_n}{q_nq_{n-1}} = \frac{(-1)^n}{q_nq_{n-1}}$$

となる. これより

$$\frac{p_{n+1}}{q_{n+1}} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^n}{q_n}\left(\frac{1}{q_{n-1}} - \frac{1}{q_{n+1}}\right)$$

が導かれるが (2.8) より

$$\frac{1}{q_{n-1}} - \frac{1}{q_{n+1}} > 0$$

であるから,

$$\frac{p_{2k+1}}{q_{2k+1}} - \frac{p_{2k-1}}{q_{2k-1}} = \frac{(-1)^{2k}}{q_{2k}}\left(\frac{1}{q_{2k-1}} - \frac{1}{q_{2k+1}}\right) > 0$$

となる. 従って

$$\frac{p_1}{q_1} < \frac{p_3}{q_3} < \cdots < \frac{p_{2k-1}}{q_{2k-1}} < \frac{p_{2k+1}}{q_{2k+1}} < \cdots$$

を得る. 同様にして

$$\frac{p_{2k+2}}{q_{2k+2}} - \frac{p_{2k}}{q_{2k}} = \frac{(-1)^{2k+1}}{q_{2k+1}}\left(\frac{1}{q_{2k}} - \frac{1}{q_{2k+2}}\right) < 0$$

より

$$\frac{p_2}{q_2} > \frac{p_4}{q_4} > \cdots > \frac{p_{2k+2}}{q_{2k+2}} > \frac{p_{2k}}{q_{2k}} > \cdots$$

を得る. 以上から

$$\frac{p_1}{q_1} < \frac{p_3}{q_3} < \cdots < \frac{p_{2k-1}}{q_{2k-1}} < \cdots\cdots\cdots < \frac{p_{2k}}{q_{2k}} \cdots < \frac{p_4}{q_4} < \frac{p_2}{q_2}$$

が成立する. ここで数列 $\left\{\dfrac{p_{2k+1}}{q_{2k+1}}\right\}$ は単調増加かつ上に有界であり, 数列 $\left\{\dfrac{p_{2k}}{q_{2k}}\right\}$ は単調減少かつ下に有界であるから極限

$$\lim_{k\to\infty}\frac{p_{2k+1}}{q_{2k+1}} = \omega_1, \qquad \lim_{k\to\infty}\frac{p_{2k}}{q_{2k}} = \omega_2$$

が存在する. 一方

$$\lim_{n\to\infty}\left(\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}\right) = \lim_{n\to\infty}\frac{1}{q_n q_{n-1}} = 0$$

であるから $\omega_1 = \omega_2$ である. よって

$$\lim_{n\to\infty}[k_0, k_1, \ldots, k_n] = \lim_{n\to\infty}\frac{p_{n+1}}{q_{n+1}} = \eta$$

となる実数 η の存在することが示された.

上のことから

$$\lim_{n\to\infty}[k_1, \ldots, k_n] = \eta_1$$

が定まる. このとき

$$\eta = k_0 + \frac{1}{\eta_1}$$

であり, $\eta_1 > k_1 \geq 1$ であるから $\lfloor\eta\rfloor = k_0$ である. 同様にして

$$\lfloor\eta_1\rfloor = k_1, \quad \eta_2 = \frac{1}{\eta_1 - k_1} \quad \text{とおけば} \quad \lfloor\eta_2\rfloor = k_2, ..., \lfloor\eta_n\rfloor = k_n, ...$$

が成り立つから $\{k_n\}$ は η の連分数展開に現れる整数列である. ゆえに無限連分数展開 $\eta = [k_0, k_1, \ldots, k_n, \ldots]$ が成り立つ. これより η が無理数であることもわかる. ∎

3 章　整係数２元２次形式

この章では (整係数) ２次形式の間に対等と呼ばれる同値関係を導入し, 対等な２次形式が同じ判別式をもつことを示す. これより同じ判別式をもつ２次形式がいくつかの同値類に分割され, これらの同値類の個数としてその判別式の類数が定義される.

§3.1 では２次形式, 判別式, 特殊１次変換, ２次形式の間の対等および正に対等などの基本概念を導入する.

§3.2 では特殊１次変換によりモデュラ変換が定まること, モデュラ変換が整係数既約２次式の根である２次代数的数の上の変換を引き起こすことなどを示す. これより２次代数的数の間にも対等, および正に対等という同値関係が定義される.

§3.3 では２次形式に対応する２次式の根を第１根, 第２根に区別し, 同じ判別式をもつ２つの２次形式が正に対等であることと, 対応する２次式の第１根が正に対等であることとが同値であることを示す.

3.1　２次形式と２次形式の対等

整数 a, b, c を係数とする x, y についての同次２次式

$$f(x,y) = ax^2 + bxy + cy^2 = \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

を整係数２元２次形式という. また

$$\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$$

を f の行列といい

$$D = b^2 - 4ac = -4 \begin{vmatrix} a & b/2 \\ b/2 & c \end{vmatrix}$$

を f の判別式という. 以下, 単に２次形式といえば, 特に断らない限り, 整係数２元２次形式を指すものとする. また a, b, c が互いに素であるとき f を原始的２元２次形式という.

２次形式 f の判別式が平方数ならば f は１次式の積に分解され, f に関する問題が１次式の問題に帰着される. 従って, 特に断らない限り２次形式の判別式は非平方数であるとする.

さて２つの２次形式

$$f(x,y) = ax^2 + bxy + cy^2 = \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

と

$$f'(x',y') = a'x'^2 + b'x'y' + c'y'^2 = \begin{bmatrix} x' & y' \end{bmatrix} \begin{bmatrix} a' & b'/2 \\ b'/2 & c' \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix}$$

に対して

$$\begin{bmatrix} a' & b'/2 \\ b'/2 & c' \end{bmatrix} = \begin{bmatrix} r & t \\ s & u \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} r & s \\ t & u \end{bmatrix}$$

を満たす $T = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \in SL(\mathbb{Z})^{\pm}$ が存在するとき $f(x,y)$ と $f'(x',y')$ は対等であるといい $f(x,y) \sim f'(x',y')$ と表す. 特に $T \in SL(\mathbb{Z})^{+}$ のとき正に対等であるといい, $T \in SL(\mathbb{Z})^{-}$ のときは負に対等であるという.

$f(x,y) \sim f'(x',y')$ であるとき $f'(x',y')$ は $f(x,y)$ に次の変数の変換を行って得られる.

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} \tag{3.1}$$

このとき

$$\begin{cases} a' = ar^2 + brt + ct^2 \\ b' = 2ars + b(ru + st) + 2ctu \\ c' = as^2 + bsu + cu^2 \end{cases} \tag{3.2}$$

が成り立つことを注意しておく.

以下簡単のため, ２次形式 f, f', f'',... に対して, その行列をそれぞれ

$$\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}, \quad \begin{bmatrix} a' & b'/2 \\ b'/2 & c' \end{bmatrix}, \quad \begin{bmatrix} a'' & b''/2 \\ b''/2 & c'' \end{bmatrix}, \cdots$$

とおくことにする.

定理 3.1 ２次形式における対等および正に対等の関係は同値関係である.

Proof　正に対等の関係についても同様であるから, 対等関係が同値関係であることのみを示す.

単位行列 $E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ により

$$\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

となるので $f \sim f$ である. また $f \sim f'$ とすると

$$\begin{bmatrix} a' & b'/2 \\ b'/2 & c' \end{bmatrix} = T^t \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} T \qquad (T^t \text{ は } T \text{ の転置行列})$$

を満たす $T \in SL(\mathbb{Z})^{\pm}$ が存在する. このとき

$$\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} = (T^{-1})^t \begin{bmatrix} a' & b'/2 \\ b'/2 & c' \end{bmatrix} T^{-1}$$

が成り立つので $f' \sim f$ である.

最後に $f \sim f'$ かつ $f' \sim f''$ とすると

$$\begin{bmatrix} a' & b'/2 \\ b'/2 & c' \end{bmatrix} = T_1^t \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} T_1, \quad \begin{bmatrix} a'' & b''/2 \\ b''/2 & c'' \end{bmatrix} = T_2^t \begin{bmatrix} a' & b'/2 \\ b'/2 & c' \end{bmatrix} T_2$$

を満たす $T_1, T_2 \in SL(\mathbb{Z})^{\pm}$ が存在する. このとき

$$\begin{bmatrix} a'' & b''/2 \\ b''/2 & c'' \end{bmatrix} = (T_1 T_2)^t \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} T_1 T_2$$

が成り立つので $f \sim f''$ である. ∎

定理 3.2 $f \sim f'$ のとき整数 n について次は同値である.

(i) $f(x,y) = n$ が整数解をもつ.

(ii) $f'(x,y) = n$ が整数解をもつ.

Proof 仮定より

$$\begin{bmatrix} a' & b'/2 \\ b'/2 & c' \end{bmatrix} = \begin{bmatrix} r & t \\ s & u \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} r & s \\ t & u \end{bmatrix}$$

を満たす $\begin{bmatrix} r & s \\ t & u \end{bmatrix} \in SL(\mathbb{Z})^{\pm}$ が存在する. このとき

$$\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} = \begin{bmatrix} u & -t \\ -s & r \end{bmatrix} \begin{bmatrix} a' & b'/2 \\ b'/2 & c' \end{bmatrix} \begin{bmatrix} u & -s \\ -t & r \end{bmatrix}$$

が成り立つ.

$f(x,y) = n$ が整数解 (α, β) をもつとすれば

$$\begin{aligned} n &= \begin{bmatrix} \alpha & \beta \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \\ &= \begin{bmatrix} \alpha & \beta \end{bmatrix} \begin{bmatrix} u & -t \\ -s & r \end{bmatrix} \begin{bmatrix} a' & b'/2 \\ b'/2 & c' \end{bmatrix} \begin{bmatrix} u & -s \\ -t & r \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \end{aligned}$$

である. 従って

$$\begin{bmatrix} \alpha' \\ \beta' \end{bmatrix} = \begin{bmatrix} u & -s \\ -t & r \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

とおけば $f'(\alpha', \beta') = n$ となるので $f'(x,y) = n$ は解をもつ

逆に $f'(x,y) = n$ が解をもつと仮定しても同様である. ∎

定理 3.3 f が原始的で $f \sim f'$ ならば f' も原始的である.

Proof　仮定より a,b,c は互いに素で

$$\begin{bmatrix} a' & b'/2 \\ b'/2 & c' \end{bmatrix} = \begin{bmatrix} r & t \\ s & u \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} r & s \\ t & u \end{bmatrix}$$

を満たす $\begin{bmatrix} r & s \\ t & u \end{bmatrix} \in SL(\mathbb{Z})^{\pm}$ が存在する. このとき

$$\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} = \begin{bmatrix} u & -t \\ -s & r \end{bmatrix} \begin{bmatrix} a' & b'/2 \\ b'/2 & c' \end{bmatrix} \begin{bmatrix} u & -s \\ -t & r \end{bmatrix}$$

を得るが, これより

$$\begin{cases} a = a'u^2 - b'ut + c't^2 \\ b = -2a'su + b'(ru + st) - 2c'rt \\ c = a's^2 - b'rs + c'r^2 \end{cases}$$

となる. ここで a',b',c' の公約数は a,b,c の公約数でもあるから a',b',c' も互いに素である. 従って f' も原始的である. ∎

定理 3.4 対等な2次形式 f, f' の判別式をそれぞれ D, D' とすると $D = D'$ が成り立つ.

Proof

$$\begin{aligned} D' &= -4\begin{vmatrix} a' & b'/2 \\ b'/2 & c' \end{vmatrix} = -4\begin{vmatrix} r & t \\ s & u \end{vmatrix}\begin{vmatrix} a & b/2 \\ b/2 & c \end{vmatrix}\begin{vmatrix} r & s \\ t & u \end{vmatrix} \\ &= -4\begin{vmatrix} r & s \\ t & u \end{vmatrix}^2\begin{vmatrix} a & b/2 \\ b/2 & c \end{vmatrix} \\ &= -4\begin{vmatrix} a & b/2 \\ b/2 & c \end{vmatrix} = D \end{aligned}$$

∎

定理3.4より対等な2次形式は同じ判別式をもつ. 従って判別式 D をもつ2次形式全体が対等な関係で類別される. このときの各類を判別式 D をもつ2次形式の類と呼ぶ. またそれらの類の個数を判別式 D をもつ2次形式の類数といい $h(D)$ と表す. 同様に判別式 D をもつ2次形式全体を正の対等関係で類別したときの各類を狭義の類, 狭義の類の

個数を狭義の類数といい $h^+(D)$ と表す. 判別式 D をもつ2次形式の類はいくつかの狭義の類の和であるから $h^+(D) \geq h(D)$ が成り立つ.

3.2 2次代数的数

$a(\neq 0), b, c$ を整数とする. 2次式 $f(x) = ax^2+bx+c$ が $\mathbb{Q}$ 上既約であるとき $f(\xi) = 0$ を満たす複素数 ξ を2次代数的数という. 特に ξ が実数のとき2次無理数という. また a, b, c が互いに素であるとき $f(x) = ax^2 + bx + c$ は原始的であるということにする.

以下 $x^2 + 1 = 0$ の根を1つ固定し i とおく. $i^2 = -1$ であるから $i = \sqrt{-1}$ と書くこともある.

既約2次式 $f(x) = ax^2 + bx + c$ の判別式 D は平方数でない. 今その根を

$D > 0$ のとき

$$\xi = \frac{-b + \sqrt{D}}{2a}, \qquad \xi' = \frac{-b - \sqrt{D}}{2a}$$

$D < 0$ のとき

$$\xi = \frac{-b + i\sqrt{-D}}{2a}, \qquad \xi' = \frac{-b - i\sqrt{-D}}{2a}$$

とおき, ξ を第1根, ξ' を第2根と呼ぶことにする. また ξ と ξ' は互いに他の共役であるという.

2次代数的数 ξ に対して ξ を根とする整係数2次式 $ax^2 + bx + c$ のなかで原始的であるものが符号を除いて一意に定まる. このとき判別式 $D = b^2 - 4ac$ は一意に定まる. これを ξ の判別式という.

$a\xi^2 + b\xi + c = 0$ を満たす2次代数的数 ξ に対して $t\xi + u = 0$ となる整数は $t = u = 0$ のみである. 従って p.8 で述べたように $T = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \in SL(\mathbb{Z})^{\pm}$ により

$$\eta = T(\xi) = \frac{r\xi + s}{t\xi + u} \tag{3.3}$$

で1つの複素数 η が定まる.

補題 ξ が2次代数的数で $T \in SL(\mathbb{Z})^{\pm}$ のとき式 (3.3) で定まる η も2次代数的数である. また ξ と η の判別式は一致する.

Proof　$a\xi^2+b\xi+c=0$ とすると

$$\begin{bmatrix} \xi & 1 \end{bmatrix}\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}\begin{bmatrix} \xi \\ 1 \end{bmatrix} = a\xi^2+b\xi+c=0$$

である. 従って

$$\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} = \begin{bmatrix} r & t \\ s & u \end{bmatrix}\begin{bmatrix} a' & b'/2 \\ b'/2 & c' \end{bmatrix}\begin{bmatrix} r & s \\ t & u \end{bmatrix}$$

と a',b',c' を定めれば, $t\xi+u\neq 0$ であることから

$$\begin{aligned} a'\eta^2+b'\eta+c' &= \begin{bmatrix} \eta & 1 \end{bmatrix}\begin{bmatrix} a' & b'/2 \\ b'/2 & c' \end{bmatrix}\begin{bmatrix} \eta \\ 1 \end{bmatrix} \\ &= \left(\frac{1}{t\xi+u}\right)^2\begin{bmatrix} \xi & 1 \end{bmatrix}\begin{bmatrix} r & t \\ s & u \end{bmatrix}\begin{bmatrix} a' & b'/2 \\ b'/2 & c' \end{bmatrix}\begin{bmatrix} r & s \\ t & u \end{bmatrix}\begin{bmatrix} \xi \\ 1 \end{bmatrix} \\ &= \left(\frac{1}{t\xi+u}\right)^2\begin{bmatrix} \xi & 1 \end{bmatrix}\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}\begin{bmatrix} \xi \\ 1 \end{bmatrix} \\ &= \left(\frac{1}{t\xi+u}\right)^2\left(a\xi^2+b\xi+c\right)=0 \end{aligned}$$

より $a'\eta^2+b'\eta+c'=0$ が成り立つ. また

$$-4\begin{vmatrix} a & b/2 \\ b/2 & c \end{vmatrix} = -4\begin{vmatrix} a' & b'/2 \\ b'/2 & c' \end{vmatrix}$$

が成り立つので ξ と η の判別式は一致する. 従って $a'x^2+b'x+c'$ は$\mathbb{Q}$上既約である. ゆえに η も2次代数的数である. ∎

p.25で述べたように2次代数的数 ξ とモデュラ変換 T に対して式 (3.3) で1つの複素数 $T(\xi)$ が定まる. 従って定理 1.17 より次の補題が成り立つ.

補題 3.5 $T,T'\in SL(\mathbb{Z})^{\pm}$ のとき $T(T'(\xi))=TT'(\xi)$ である.

定理 3.6 $T\in SL(\mathbb{Z})^{\pm}$ に対して式 (3.3) で定まる写像は2次代数的数全体のなす集合からそれ自身への全単射 (変換) である.

Proof　任意の2次代数的数 η に対して $\xi=T^{-1}(\eta)$ とおけば補題 3.5 より

$$T(\xi)=TT^{-1}(\eta)=\eta$$

となるから T は全射を引き起こす. また $T(\xi) = T(\xi')$ とすれば $\xi = T^{-1}(T(\xi)) = T^{-1}(T(\xi')) = \xi'$ となるから T は単射を引き起こす. ∎

補題 $T \in SL(\mathbb{Z})^{\pm}$ に対して式 (3.3) で定まる写像がすべての2次代数的数を不変にすれば $T = \pm E$ である. ただし $E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ である.

Proof $T = \begin{bmatrix} r & s \\ t & u \end{bmatrix}$ とおく. $T(i) = i$ より $r = u, t = -s$ を得る. また $T(2i) = 2i$ より $s = -4t$ を得るから $s = t = 0$ である. $|T| = r^2 = \pm 1$ から $r = u = \pm 1$ を得る. よって $T = \pm E$ である. ∎

T によって引き起こされる変換は $|T| = 1$ のとき正のモデュラ変換, $|T| = -1$ のとき負のモデュラ変換と呼ばれる.

補題3.5により $T \in SL(\mathbb{Z})^{\pm}$ にモデュラ変換 (3.3) を対応させる写像は$SL(\mathbb{Z})^{\pm}$から2次代数的数のなす集合上の変換群への準同型となり, その核は上の補題から $\pm E$ である. 定理1.15よりモデュラ変換全体は $SL(\mathbb{Z})^{\pm}/\{\pm E\}$ と同一視できる. これを $M^{\pm}$ と表す. 同様に正のモデュラ変換全体は $SL(\mathbb{Z})^{+}/\{\pm E\}$ と同一視でき, これを M^{+} と表す.

ξ を η に移すモデュラ変換があるとき ξ と η は対等であるといい $\xi \sim \eta$ と表す. 特に正のモデュラ変換で移りあうとき正に対等であるといい, 負のモデュラ変換で移りあうとき負に対等であるという.

定理 3.7 2次代数的数の対等および正に対等の関係は同値関係である.

Proof 正に対等の関係についても同様であるから, 対等の関係が同値関係であることのみを示す.

任意の2次代数的数 ξ に対して $E(\xi) = \xi$ より $\xi \sim \xi$ である.

$\xi \sim \eta$ とすると $\eta = T(\xi)$ となる $T \in SL(\mathbb{Z})^{\pm}$ が存在する. このとき $\xi = T^{-1}(\eta)$ となるので $\eta \sim \xi$ である.

$\xi \sim \eta, \eta \sim \zeta$ とすると $\eta = T(\xi),\ \zeta = T'(\eta)$ となる $T, T' \in SL(\mathbb{Z})^{\pm}$ が存在する. このとき $\zeta = T'T(\xi)$ となるので $\xi \sim \zeta$ である. ∎

3.3 2次形式と2次代数的数

2次形式 $f(x,y)=ax^2+bxy+cy^2$ が与えられたとする. f の判別式は平方数でないとしているから $a\neq 0$ であり, 2次式 ax^2+bx+c は $\mathbb{Q}$ 上既約である. 従って f に対して ax^2+bx+c の第1根 ξ が定まる. この節では同じ判別式をもつ2次形式の対等関係と対応する2次式の第1根の対等関係について考察する. なお ξ は2次式 $-ax^2-bx-c$ の第2根であることを注意しておく.

この節では2次形式

$$f_1(x,y)=a_1x^2+b_1xy+c_1y^2,\quad f_2(x,y)=a_2x^2+b_2xy+c_2y^2$$

は同じ判別式をもつものとし, 対応する2次式の第1根をそれぞれ ξ_1, ξ_2 とする.

補題 3.8 $f_1(x,y)$ と $f_2(x,y)$ が正に対等ならば ξ_1 と ξ_2 も正に対等である.

Proof 仮定より

$$\begin{bmatrix} a_2 & b_2/2 \\ b_2/2 & c_2 \end{bmatrix}=\begin{bmatrix} r & t \\ s & u \end{bmatrix}\begin{bmatrix} a_1 & b_1/2 \\ b_1/2 & c_1 \end{bmatrix}\begin{bmatrix} r & s \\ t & u \end{bmatrix}$$

を満たす $\begin{bmatrix} r & s \\ t & u \end{bmatrix}\in SL(\mathbb{Z})^+$ が存在する. このとき

$$\begin{cases} a_1=a_2u^2-b_2ut+c_2t^2 \\ b_1=-2a_2us+b_2(ru+st)-2c_2rt \\ c_1=a_2s^2-b_2rs+c_2r^2 \end{cases}$$

が成り立つ. 従って $D>0$ のときは

$$\frac{r\xi_2+s}{t\xi_2+u}=\frac{r\dfrac{-b_2+\sqrt{D}}{2a_2}+s}{t\dfrac{-b_2+\sqrt{D}}{2a_2}+u}=\frac{(2a_2s-b_2r)+r\sqrt{D}}{(2a_2u-b_2t)+t\sqrt{D}}$$

となる. ここで分母を有理化すると

$$\begin{aligned}
&= \frac{(4a_2^2su - 2a_2b_2st - 2a_2b_2ru + 4a_2c_2rt) + 2a_2(ru - st)\sqrt{D}}{4a_2^2u^2 - 4a_2b_2ut + 4a_2c_2t^2} \\
&= \frac{-2a_2b_1 + 2a_2\sqrt{D}}{4a_2a_1} \\
&= \frac{-b_1 + \sqrt{D}}{2a_1} = \xi_1
\end{aligned}$$

となる. 従って $\xi_1 = \dfrac{r\xi_2 + s}{t\xi_2 + u}$ より ξ_1 と ξ_2 は正に対等である. $D < 0$ の場合も同様に証明できる. ∎

上の補題の条件のもとで ξ_2' が f_2 に対応する 2 次式の第 2 根であるとき $\dfrac{r\xi_2' + s}{t\xi_2' + u}$ は f_1 に対応する 2 次式の第 2 根であることを注意しておく.

補題 3.9 ξ_1 と ξ_2 が正に対等ならば $f_1(x, y)$ と $f_2(x, y)$ も正に対等である.

Proof ξ_1 と ξ_2 が正に対等であることから

$$\xi_1 = \frac{r\xi_2 + s}{t\xi_2 + u}$$

を満たす $\begin{bmatrix} r & s \\ t & u \end{bmatrix} \in SL(\mathbb{Z})^+$ が存在する. 上式を $a_1\xi_1^2 + b_1\xi_1 + c_1 = 0$ に代入すると

$$a_1\left(\frac{r\xi_2 + s}{t\xi_2 + u}\right)^2 + b_1\left(\frac{r\xi_2 + s}{t\xi_2 + u}\right) + c_1 = 0$$

となる. $(t\xi_2 + u)^2$ 倍すると

$$(a_1r^2 + b_1rt + c_1t^2)\xi_2^2 + (2a_1rs + b_1(ru + st) + 2c_1tu)\xi_2 + (a_1s^2 + b_1su + c_1u^2) = 0$$

を得る. この 2 次式の判別式は $b_1^2 - 4a_1c_1 = b_2^2 - 4a_2c_2$ である. 一方 ξ_2 を根とする 2 つの整係数 2 次式の判別式が一致すれば, 一方が他方の ± 1 倍である. 従って

$$\begin{cases}
a_1r^2 + b_1rt + c_1t^2 = \pm a_2 \\
2a_1rs + b_1(ru + st) + 2c_1tu = \pm b_2 \\
a_1s^2 + b_1su + c_1u^2 = \pm c_2
\end{cases}$$

が成り立つ (複合同順). これより

$$\begin{bmatrix} r & t \\ s & u \end{bmatrix} \begin{bmatrix} a_1 & b_1/2 \\ b_1/2 & c_1 \end{bmatrix} \begin{bmatrix} r & s \\ t & u \end{bmatrix} = \pm \begin{bmatrix} a_2 & b_2/2 \\ b_2/2 & c_2 \end{bmatrix}$$

となる. f_1 と f_2 が正に対等でないと仮定すると

$$\begin{bmatrix} r & t \\ s & u \end{bmatrix} \begin{bmatrix} a_1 & b_1/2 \\ b_1/2 & c_1 \end{bmatrix} \begin{bmatrix} r & s \\ t & u \end{bmatrix} = - \begin{bmatrix} a_2 & b_2/2 \\ b_2/2 & c_2 \end{bmatrix}$$

となり, f_1 と $-f_2$ が正に対等である. このとき ξ_2 は $-f_2$ に対応する2次式の第2根となり $\xi_1 = \dfrac{r\xi_2 + s}{t\xi_2 + u}$ が f_1 の第1根であることに矛盾する. よって f_1 と f_2 は正に対等である. ∎

上の補題より次の定理が成り立つ.

定理 3.10 $f_1(x, y)$ と $f_2(x, y)$ が正に対等であることと, 対応する2次式の第1根 ξ_1 と ξ_2 が正に対等であることは同値である.

定理 3.11 2次形式の正の対等に関する類と2次代数的数の正の対等に関する類が1対1に対応する.

4章　類数の有限性 …判別式が負の場合

この章では負の判別式 D に対する類数が有限であることを示す. 負の判別式をもつ2次形式は正と負の2種類に分けることができ, 対等関係を考察する際, 正の2次形式のみを考察すればよい. 従って, この章では正の2次形式のみを扱う.

§4.1では簡約2次形式を定義し, 与えられた判別式をもつ簡約2次形式が有限個であることを示す.

§4.2では正の2次形式が, 簡約2次形式であることと, 対応する2次式の第1根が基本領域と呼ばれる領域内にあることとが同値であることを示す. さらに任意に与えられた正の2次形式に対して, それと正に対等な簡約2次形式が唯1つ存在することを示し, 類数が有限であることを導く. これより虚部が正の2次代数的数に正に対等な点が基本領域内に唯一つ存在することがわかる.

最後の §4.3 ではいくつかの負の判別式の値に対して簡約2次形式を求める計算例を述べる.

この章を通じて2次形式の判別式は負であるものとする. このとき $f(x,y)=ax^2+bxy+cy^2$ において $D=b^2-4ac<0$ であることから $ac>0$ となり a と c が同符号であることが導かれる.

さて

$$f(x,y)=ax^2+bxy+cy^2=a\left(x+\frac{b}{2a}y\right)^2+\left(\frac{4ac-b^2}{4a}\right)y^2$$

と変形できる. $D<0$ であるから $f(x,y)$ は $(x,y)\neq(0,0)$ なる値に対して $a>0$ のときは常に $f(x,y)>0$, $a<0$ のときは 常に $f(x,y)<0$ となる. 以下 $a>0$ のとき f を正の2次形式, $a<0$ のとき f を負の2次形式と呼ぶことにする. 定理3.2より対等な2次形式は同じ値域をもつので, 正の2次形式に対等な2次形式は正の2次形式であり, 負の2次形式に対等な2次形式は負の2次形式である. また f と f' が対等ならば $-f$ と $-f'$ は対等である. 以上から判別式が負の2次形式の対等関係を考察するには正の2次形式の対等関係を考察すれば十分である. よってこの章では2次形式はすべて正の2次形式であると

する. また判別式 D をもつ正の 2 次形式を正の対等により類別したときの類数を $\tilde{h}^+(D)$ と表すことにする. $h^+(D) = 2\tilde{h}^+(D)$ であることに注意されたい.

4.1 簡約 2 次形式

2 次形式 $f(x,y) = ax^2 + bxy + cy^2$ が条件

$$c > a \geq b > -a \quad \text{または} \quad c = a \geq b \geq 0 \tag{4.1}$$

を満たすとき (負の判別式をもつ) 簡約 2 次形式であるという.

定理 4.1 判別式 D をもつ簡約 2 次形式 $f(x,y) = ax^2 + bxy + cy^2$ は $|b| \leq \sqrt{\frac{|D|}{3}}$ を満たす. 従ってその個数は有限である.

Proof　簡約 2 次形式の条件より $|b| \leq |a| \leq |c|$ が成り立つ. 従って $b^2 \leq ac$ を得る. これと $D = b^2 - 4ac < 0$ より

$$|D| = |b^2 - 4ac| = 4ac - b^2 \geq 4b^2 - b^2 = 3b^2$$

を得る. よって $|b| \leq \sqrt{\dfrac{|D|}{3}}$ が成り立つ. 従って b のとり得る整数値は有限個で, それぞれの値に対して $4ac = b^2 - D$ で定まる a, c も有限個である. 従って与えられた判別式 D をもつ簡約 2 次形式は有限個である. ∎

定理 4.2 原始的な簡約 2 次形式 $f(x,y) = ax^2 + bxy + cy^2$ を不変にする正の特殊 1 次変換は次の通りである.

(i)　$f(x,y) = x^2 + y^2$ のとき　$\pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$

(ii)　$f(x,y) = x^2 + xy + y^2$ のとき　$\pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}, \pm \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$

(iii)　その他の $f(x,y)$ のとき　$\pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Proof　正の特殊1次変換 $X = \begin{bmatrix} r & s \\ t & u \end{bmatrix}$ が $f(x,y)$ を不変にしたとすると

$$\begin{bmatrix} r & t \\ s & u \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} r & s \\ t & u \end{bmatrix} = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$$

が成り立つ. これより

$$\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} r & s \\ t & u \end{bmatrix} = \begin{bmatrix} u & -t \\ -s & r \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$$

が得られる. 成分を比較して

$$\begin{cases} a(r-u)+bt &= 0 \\ as+ct &= 0 \\ c(r-u)-bs &= 0 \end{cases} \tag{4.2}$$

を得る.

$s=0$ または $t=0$ とすると $as+ct=0$ かつ $a,c>0$ より $s=t=0$ となる. 従って $ru-st=ru=1$ より $X = \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ である.

以下 $s \neq 0$ かつ $t \neq 0$ とする. このとき $as+ct=0$ かつ $a,c>0$ より $st<0$ である.

(i)　$r=u$ の場合.　$-st \geq 1$ かつ $ru-st = r^2-st = 1$ より $r=u=0$ かつ $st=-1$ となる. ゆえに $X = \pm \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ である. またこのとき式 (4.2) より $b=0$ かつ $a=c$ となる.　a,b,c は互いに素であるから $a=c=1,\ b=0$ となる. 従って $f(x,y)=x^2+y^2$ である.

(ii)　$r \neq u$ の場合.

$b=0$ ならば $a(r-u)+bt=0$ より $r=u$ となり矛盾が生じる. よって $b \neq 0$ である.

$r=0$ とすれば $bt=au, bs=-cu,\ -st=1$ となる.　a,b,c は互いに素であることと簡約2次形式であることから $a=c=b=1,\ u=\pm 1$ となる. ゆえに $X = \pm \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ であり, $f(x,y)=x^2+xy+y^2$ である.

$u=0$ としても同様にして $X = \pm \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$ であり, $f(x,y)=x^2+xy+y^2$ である.

最後に $r \neq 0$ かつ $u \neq 0$ とする．$st < 0$ かつ $ru - st = 1$ より $ru < 0$ である．従って $b \neq 0$ に注意すれば

$$|t| = \frac{a}{|b|}(|r| + |u|) \geq |r| + |u|, \quad |s| = \frac{c}{|b|}(|r| + |u|) \geq |r| + |u|$$

となる．これより

$$|st| \geq |r|^2 + 2|r||u| + |u|^2 > |ur| + 2$$

となるが，これは $ru - st = 1$ より得られる $|ru| = |st| - 1$ に矛盾する．ゆえに r, s, t, u がすべて 0 でない場合は起こりえない． ∎

定理 3.10 と定理 4.2 より次の系を得る．

系 4.3 正の簡約 2 次形式に対応する 2 次式の第 1 根である 2 次代数的数 ξ を不変にする正のモデュラ変換は次のものに限る．

(i) $\xi = i$ のとき $\pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$

(ii) $\xi = \dfrac{-1 + \sqrt{3}i}{2}$ のとき $\pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}, \pm \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$

(iii) その他の場合 $\pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

4.2 基本領域と類数の有限性

補題 4.4 2 次形式 f に対応する 2 次式の第 1 根を $\xi = X + Yi$ とする．このとき f が簡約 2 次形式であるための条件は

$$-\frac{1}{2} \leq X < \frac{1}{2}, \quad |\xi| > 1 \quad \text{または} \quad -\frac{1}{2} \leq X \leq 0, \quad |\xi| = 1$$

が成り立つことである．

Proof $f(x, y) = ax^2 + bxy + cy^2$ とおく．仮定より対応する 2 次式の第 2 根は $\xi' = X - Yi$ であり

$$2X = -\frac{b}{a}, \quad |\xi|^2 = X^2 + Y^2 = \frac{c}{a}$$

が成り立つ. f が簡約２次形式であることは条件 (4.1) より

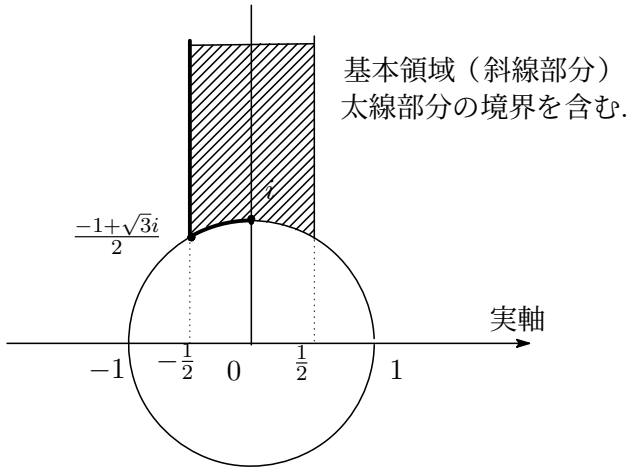
$$c > a \geq b > -a \quad \text{または} \quad c = a \geq b \geq 0$$

が成り立つことであり, これは, それぞれ

$$-\frac{1}{2} \leq X < \frac{1}{2}, \quad |\xi| > 1 \qquad \text{または} \qquad -\frac{1}{2} \leq X \leq 0, \quad |\xi| = 1$$

が成り立つことと同値である. ∎

複素平面上の点 $\xi = X + Yi$ で $-\frac{1}{2} \leq X < \frac{1}{2}$, $|\xi| > 1$ または $-\frac{1}{2} \leq X \leq 0$, $|\xi| = 1$ を満たすもの全体のなす集合を基本領域という. 基本領域内の点を第１根とする２次式に対応する正の２次形式は簡約２次形式であり, 簡約２次形式に対応する２次式の第１根は基本領域内にある.



補題 4.5 ２次形式はある簡約２次形式に正に対等である.

Proof

$$f(x,y) = ax^2 + bxy + cy^2 = \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

とする. $a > c$ のときは

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} c & -b/2 \\ -b/2 & a \end{bmatrix} \qquad (*)$$

とできるので $a \leq c$ と仮定してよい. $|b| > a$ のときは $a \geq b + 2na > -a$ となるように整数 n を選び

$$\begin{bmatrix} 1 & 0 \\ n & 1 \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & (b+2na)/2 \\ (b+2na)/2 & c + nb + n^2 a \end{bmatrix} \qquad (**)$$

と正の特殊1次変換を行う. ここで $a \leq c+nb+n^2a$ ならばこれが簡約2次形式を表す. $a > c+nb+n^2a$ ならば再び $(*)$ の変換を行うと次の行列が得られる.

$$\begin{bmatrix} a' & b'/2 \\ b'/2 & c' \end{bmatrix}, \quad a' = c+nb+n^2a \ < \ c' = a,\ b' = -(b+2na)$$

これが簡約2次形式を表さないときは, さらに $(**)$ を行う.

$$\begin{bmatrix} a'' & b''/2 \\ b''/2 & c'' \end{bmatrix}, \quad a'' = a',\ a'' \geq b'' > -a''$$

このような正の特殊1次変換を繰り返し行って得られる行列が簡約2次形式を表さないとすれば, 上の操作が無限に続くことになり, 行列の $(1,1)$ 成分は減少を続ける. これは a が自然数であることに矛盾する. ∎

補題 4.6 $f(x,y) = ax^2+bxy+cy^2$ が簡約2次形式のとき $0 < f(x,y) \leq a$ を満たす整数 (x,y) は次のものに限る.

(i) $c > a$ のとき $(x,y) = (\pm 1, 0)$

(ii) $c = a > b$ のとき $(x,y) = (\pm 1, 0), (0, \pm 1)$

(iii) $c = a = b$ のとき $(x,y) = (\pm 1, 0), (0, \pm 1), \pm(1, -1)$

特に $f(x,y)$ の 0 と異なる最小値は a である.

Proof $0 < f(x,y) \leq a$ より

$$f(x,y) = ax^2+bxy+cy^2 = a\left(x+\frac{b}{2a}y\right)^2 + \left(\frac{4ac-b^2}{4a}\right)y^2 \leq a$$

となる. ここで $4ac \geq 4a^2$, $b^2 \leq a^2$ であることから

$$y^2 \leq \left(\frac{4a}{4ac-b^2}\right)a \leq \frac{4a^2}{3a^2} \leq \frac{4}{3}$$

を得る. 従って $y = 0, \pm 1$ である.

$y = 0$ のときは明らかに $x = \pm 1$ である. すなわち条件 $0 < f(x,y) \leq a$ を満たすのは $(\pm 1, 0)$ のみである.

$y = \pm 1$ のとき $f(x, \pm 1) = ax^2 \pm bx + c$ となる. $a \geq |b|$ より $ax^2 \pm bx \geq 0$ であるから $f(x, \pm 1) \geq c$ となる. 従って $c > a$ のときは $f(x, \pm 1) > a$ となるので $(\pm 1, 0)$ の

みが条件を満たす． $c = a$ のときは $ax^2 \pm bx = 0$ のときに限り $f(x, \pm 1) = a$ となる．$ax^2 \pm bx = 0$ となるのは $a > b$ のときは $x = 0$ のみで, このときは $(0, \pm 1)$ も条件を満たす． $a = b$ のときは $x = \pm 1$ も $ax^2 \pm bx = 0$ を満たす. 従って $\pm(1, -1)$ も条件を満たす. 以上をまとめて補題が得られる． ∎

補題 4.7 2 次形式に正に対等な簡約 2 次形式は唯一つである.

Proof $f(x, y) = ax^2 + bxy + cy^2$ と $f'(x, y) = a'x^2 + b'xy + c'y^2$ を正に対等な簡約 2 次形式とする． $f = f'$ を示せばよい.

補題 4.6 より f, f' の 0 と異なる最小値はそれぞれ a, a' である. 対等な 2 次形式の値域は一致するので $a = a'$ である. 仮定より

$$\begin{bmatrix} r & t \\ s & u \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} r & s \\ t & u \end{bmatrix} = \begin{bmatrix} a & b'/2 \\ b'/2 & c' \end{bmatrix}$$

を満たす正の特殊 1 次変換 $\begin{bmatrix} r & s \\ t & u \end{bmatrix}$ が存在する． $(1, 1)$ 成分を比較して $f(r, t) = ar^2 + brt + ct^2 = a$ が成り立つ.

$c > a$ のとき補題 4.6 より $r = \pm 1$, $t = 0$ である. 従って $b' = \pm 2sa + b$ である. 一方 $a \geq b, b' > -a$ より $b = b'$ を得る. よって $c = c'$ となり $f = f'$ が成り立つ.

$c = a \geq b$ とする． $c' > a' = a$ ならば上と同様にして $f = f'$ が得られるので $c' = a' = a$ である. 従って $b^2 = D + 4ac = (b')^2$ となる． $c = a$ より $b, b' \geq 0$ であるから $b = b'$ となる. ゆえに $f = f'$ である. ∎

補題 4.5, 補題 4.7 から次の定理を得る.

定理 4.8 任意の正の 2 次形式に正に対等な簡約 2 次形式が唯一つ存在する.

定理 4.1 と定理 4.8 より次の定理が得られる.

定理 4.9 正の 2 次形式の類数 $\tilde{h}^+(D)$ は有限でその個数は判別式 D をもつ簡約 2 次形式の個数に一致する.

定理 4.9 より判別式が $D < 0$ である 2 次形式の類数 $h^+(D)$ が有限であることがわかる.

正の 2 次形式に対応する 2 次式の第 1 根 ξ は虚部が正の複素数であり, 補題 4.4 より簡約 2 次形式に対応する 2 次式の第 1 根は基本領域内にある. よって定理 4.8 から虚部が正の複素数は基本領域内の唯一つの複素数に正に対等である.

定理 4.10 虚部が正の複素数は基本領域に含まれる唯一つの複素数と正に対等である.

4.3 類数の計算例

D = −20 の場合

$f(x,y) = ax^2 + bxy + cy^2$ とする. 定理 4.1 より

$$|b| \leq \left\lfloor \sqrt{\frac{20}{3}} \right\rfloor = 2$$

となるから b は $b = 0, \pm 1, \pm 2$ のいずれかである. また, $4ac = b^2 - D$ であることから $4ac = 20, 21, 24$ である. 従って $ac = 5, 6$ である. よって簡約 2 次形式の条件 (4.1) を満たす (a,b,c) は

$$(a,b,c) = (1,0,5), \quad (2,2,3)$$

のみである. 従って $D = -20$ の簡約 2 次形式は

$$f_1(x,y) = x^2 + 5y^2, \quad f_2(x,y) = 2x^2 + 2xy + 3y^2$$

である. 特に $\tilde{h}^+(-20) = 2$ が成り立つ.

D = −36 の場合

$f(x,y) = ax^2 + bxy + cy^2$ とする. 定理 4.1 より

$$|b| \leq \left\lfloor \sqrt{\frac{36}{3}} \right\rfloor = 3$$

より b は $b = 0, \pm 1, \pm 2, \pm 3$ のいずれかである. また $4ac = b^2 - D$ であるから $4ac = 36, 37, 40, 45$ である. 従って $ac = 9, 10$ である. よって (4.1) を満たす (a, b, c) は

$$(a, b, c) = (1, 0, 9), (3, 0, 3), (2, 2, 5)$$

のみである. 従って $D = -36$ の簡約 2 次形式は

$$f_1(x, y) = x^2 + 9y^2, \qquad f_2(x, y) = 3x^2 + 3y^2,$$
$$f_3(x, y) = 2x^2 + 2xy + 5y^2,$$

となる. 従って $\tilde{h}^+(-36) = 3$ である.

$\mathbf{D = -47}$ の場合

$f(x, y) = ax^2 + bxy + cy^2$ とする. 定理 4.1 より

$$|b| \leq \left\lfloor \sqrt{\frac{47}{3}} \right\rfloor = 3$$

より b は $b = 0, \pm 1, \pm 2, \pm 3$ のいずれかである. また $4ac = b^2 - D$ であるから $4ac = 47, 48, 51, 56$ である. 従って $ac = 12, 14$ である. よって (4.1) を満たす (a, b, c) は

$$(a, b, c) = (1, 1, 12), (2, 1, 6), (2, -1, 6), (3, 1, 4), (3, -1, 4)$$

のみである. 従って $D = -47$ の簡約 2 次形式は

$$f_1(x, y) = x^2 + xy + 12y^2, \qquad f_2(x, y) = 2x^2 + xy + 6y^2,$$
$$f_3(x, y) = 2x^2 - xy + 6y^2, \qquad f_4(x, y) = 3x^2 + xy + 4y^2,$$
$$f_5(x, y) = 3x^2 - xy + 4y^2$$

となる. 従って $\tilde{h}^+(-47) = 5$ である.

次の表はいくつかの $D<0$ に対して判別式 D をもつ簡約２次形式を決定したものである. 簡約２次形式の個数が $\tilde{h}^+(D)$ である.

D	判別式 D の簡約２次形式	$\tilde{h}^+(D)$
-3	$f(x,y)=x^2+xy+y^2$	1
-4	$f(x,y)=x^2+y^2$	1
-7	$f(x,y)=x^2+xy+2y^2$	1
-8	$f(x,y)=x^2+2y^2$	1
-11	$f(x,y)=x^2+xy+3y^2$	1
-12	$f_1(x,y)=x^2+3y^2,\quad f_2(x,y)=2x^2+2xy+2y^2$	2
-15	$f_1(x,y)=x^2+xy+4y^2,\quad f_2(x,y)=2x^2+xy+2y^2$	2
-16	$f_1(x,y)=x^2+4y^2,\quad f_2(x,y)=2x^2+2y^2$	2
-19	$f(x,y)=x^2+xy+5y^2$	1
-20	$f_1(x,y)=x^2+5y^2,\quad f_2(x,y)=2x^2+2xy+3y^2$	2
-23	$f_1(x,y)=x^2+xy+6y^2,\quad f_2(x,y)=2x^2+xy+3y^2$ $f_3(x,y)=2x^2-xy+3y^2$	3
-24	$f_1(x,y)=x^2+6y^2,\quad f_2(x,y)=2x^2+3y^2$	2
-27	$f_1(x,y)=x^2+xy+7y^2,\quad f_2(x,y)=3x^2+3xy+3y^2$	2
-28	$f_1(x,y)=x^2+7y^2,\quad f_2(x,y)=2x^2+2xy+4y^2$	2
-31	$f_1(x,y)=2x^2+xy+4y^2,\quad f_2(x,y)=2x^2-xy+4y^2$ $f_3(x,y)=x^2+xy+8y^2$	3
-32	$f_1(x,y)=x^2+8y^2,\quad f_2(x,y)=3x^2+2xy+3y^2$ $f_3(x,y)=2x^2+4y^2$	3
-35	$f_1(x,y)=x^2+xy+9y^2,\quad f_2(x,y)=3x^2+xy+3y^2$	2
-36	$f_1(x,y)=x^2+9y^2,\quad f_2(x,y)=3x^2+3y^2$ $f_3(x,y)=2x^2+2xy+5y^2$	3
-39	$f_1(x,y)=x^2+xy+10y^2,\quad f_2(x,y)=2x^2+xy+5y^2$ $f_3(x,y)=2x^2-xy+5y^2,\quad f_4(x,y)=3x^2+3xy+4y^2$	4
-40	$f_1(x,y)=x^2+10y^2,\quad f_2(x,y)=2x^2+5y^2$	2
-43	$f(x,y)=x^2+xy+11y^2$	1
-44	$f_1(x,y)=x^2+11y^2,\quad f_2(x,y)=2x^2+2xy+6y^2$ $f_3(x,y)=3x^2+2xy+4y^2,\quad f_4(x,y)=3x^2-2xy+4y^2$	4
-47	$f_1(x,y)=x^2+xy+12y^2,\quad f_2(x,y)=2x^2+xy+6y^2$ $f_3(x,y)=2x^2-xy+6y^2,\quad f_4(x,y)=3x^2+xy+4y^2$ $f_5(x,y)=3x^2-xy+4y^2$	5

5 章　類数の有限性 …判別式が正の場合

この章では正の判別式 D に対する類数が有限であることを示す. 従ってこの章を通じて 2 次形式の判別式は正かつ非平方数であるものとする.

証明の流れは 4 章と同様である. 簡約 2 次形式を定義し, 判別式 D の簡約 2 次形式が有限個であること, 任意の 2 次形式がある簡約 2 次形式に対等であることを示す. しかし証明の様相は 4 章とは異なり, 2 章で準備した連分数が重要な役割を演じる. また 2 次形式に正に対等な簡約 2 次形式も一意に定まるとは限らない.

§5.1 では簡約 2 次形式, 簡約 2 次無理数を定義し, 与えられた判別式 D をもつ簡約 2 次形式が有限個であることを示す.

§5.2 では 2 次無理数, 簡約 2 次無理数がそれぞれ循環連分数, 純循環連分数で表されること, 任意の 2 次無理数がある簡約 2 次無理数に正に対等であることを示す. これより正の判別式をもつ 2 次形式の類数が有限であることが導かれる. 次に最小周期が m の簡約 2 次無理数 ξ の中間連分数を

$$\xi = [k_0, k_1, \ldots, k_{n-1}, \xi_n] \quad (n = 1, 2, \ldots, m-1)$$

としたとき ξ と対等な簡約 2 次無理数が $\xi_0 = \xi$, ξ_1, ξ_2,...,ξ_{m-1} のみであることを証明する. これは狭義の類数を計算する方法の根拠となる. 最後にいくつかの正の判別式の値に対して簡約 2 次形式と類数を求める計算例を述べる.

5.1　簡約 2 次形式と簡約 2 次無理数

2 次形式 $f(x, y) = ax^2 + bxy + cy^2$ が簡約 2 次形式であるとは, 条件

$$a > 0, \quad b < 0, \quad c < 0, \quad a + b + c < 0, \quad a - b + c > 0 \tag{5.1}$$

を満たすときにいう.

$f(x,y)$ に対応する 2 次式を $g(x)=ax^2+bx+c$ とおけば

$$g(1)=a+b+c,\quad g(0)=c,\quad g(-1)=a-b+c$$

である. 従って関係式 (5.1) が成立しているときは

$$a>0,\quad g(-1)>0,\quad g(0)<0,\quad g(1)<0 \tag{5.2}$$

が成り立つ. 逆に関係式 (5.2) が成立していると仮定すると

$$a>0,\quad c=g(0)<0,\quad a+b+c=g(1)<0,\quad a-b+c=g(-1)>0$$

が成り立つ. また $2b=g(1)-g(-1)<0$ より $b<0$ も得られるから関係式 (5.1) が成り立つ. よって関係式 (5.1) と (5.2) は同値である.

2 次式 $g(x)=ax^2+bx+c$ の第 1 根を ξ, 第 2 根を ξ' とおくと

$$\xi=\frac{-b+\sqrt{D}}{2a},\qquad \xi'=\frac{-b-\sqrt{D}}{2a}$$

である. 関係式 (5.2) が成り立つときはよく知られているように

$$\xi>1,\quad 0>\xi'>-1\quad \text{すなわち}\quad \xi>1>-\xi'>0 \tag{5.3}$$

が成り立つ. 逆に関係式 (5.3) が成り立つとすると $\dfrac{\sqrt{D}}{a}=\xi-\xi'>0$ より $a>0$ が得られるので $g(-1)>0$, $g(0)<0$, $g(1)<0$ が成り立つ. 以上から次の補題を得る.

補題 5.1 2 次形式 $f(x,y)=ax^2+bxy+cy^2$ が簡約 2 次形式であるための必要十分条件は

$$\frac{-b+\sqrt{D}}{2a}>1>\frac{b+\sqrt{D}}{2a}>0$$

が成り立つことである.

判別式が正の整係数既約 2 次式 $g(x)=ax^2+bx+c$ の第 1 根 ξ, 第 2 根 ξ' が

$$\xi>1>-\xi'>0$$

を満たすとき ξ を簡約 2 次無理数と呼ぶことにする. 補題 5.1 より次の定理が成り立つ.

定理 5.2 2 次形式 $f(x,y)$ に対応する 2 次式の第 1 根を ξ とする. このとき $f(x,y)$ が簡約 2 次形式となるための必要十分条件は, ξ が簡約 2 次無理数となることである.

定理 5.3 与えられた判別式 D をもつ簡約２次形式の個数は有限である.

Proof　$f(x,y)=ax^2+bxy+cy^2$ が判別式 D をもつ簡約２次形式であるとき補題 5.1 より $b+\sqrt{D}>0$ が成り立つ. これより $\sqrt{D}>-b=|b|$ を得る. 従って b のとり得る値は有限個であり, それぞれの値に対して $4ac=b^2-D$ で定まる a,c も有限個である. ゆえに与えられた判別式 D をもつ簡約２次形式は有限個である. ∎

5.2　２次無理数の連分数展開と類数の有限性

２次無理数の対等と連分数展開

定理 3.6 (p.26) よりモデュラ変換は２次代数的数のなす集合の上の変換を引き起こす. 特殊１次変換の成分は整数であるから, モデュラ変換は実数を実数に移す. 実数である２次代数的数が２次無理数であるからモデュラ変換は２次無理数のなす集合上の変換を引き起こす. 定理 3.6 の証明と同様にしてモデュラ変換が無理数のなす集合上の変換を引き起こすことも証明される (証明略).

さて ω を２次無理数とすると p.16, 式 (2.6), 式 (2.7) より

$$\omega=[k_0,k_1,\ldots,k_{n-1},\omega_n]=\frac{p_n\omega_n+p_{n-1}}{q_n\omega_n+q_{n-1}}\ ,\qquad p_nq_{n-1}-p_{n-1}q_n=(-1)^n$$

と表される. 上に述べたことから ω_n も２次無理数である. また次の補題の成り立つことも上式から明らかである.

補題 5.4 ω を２次無理数とし連分数展開において $\omega=[k_0,k_1,\ldots,k_{n-1},\omega_n]$ と表されたとする. n が偶数ならば ω と ω_n は正に対等であり, n が奇数ならば ω と ω_n は負に対等である.

定理 5.5 無理数 ξ と η に対して

$$\eta = T(\xi) = \frac{r\xi + s}{t\xi + u}, \quad T = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \in SL(\mathbb{Z})^{\pm}, \quad t > u > 0, \quad \xi > 1$$

となる T が存在すると仮定する. このときある n が存在して

$$\eta = [k_0, k_1, .., k_{n-1}, \xi], \quad r = p_n, \ s = p_{n-1}, \ t = q_n, \ u = q_{n-1}$$

が成り立つ. さらに $|T| = 1$ ならば n は偶数, $|T| = -1$ ならば n は奇数である.

Proof　有理数 $\frac{r}{t}$ の連分数展開を

$$\frac{r}{t} = [k_0, k_1, \ldots, k_{n-1}]$$

とする. 仮定より $t > u > 0$ であるから $t > 1$ である. また $ru - st = \pm 1$ より $(r, t) = 1$ となる. 従って $r \neq 0$ である. これより $n \geq 2$ となる.

2 章 §2.1 で述べたように

$$T_j = \begin{bmatrix} k_j & 1 \\ 1 & 0 \end{bmatrix}, \quad T_0 T_1 \cdots T_{j-2} T_{j-1} = \begin{bmatrix} p_j & p_{j-1} \\ q_j & q_{j-1} \end{bmatrix}$$

とおくと

$$\frac{r}{t} = [k_0, k_1, \ldots, k_{n-1}] = \frac{p_{n-1}k_{n-1} + p_{n-2}}{q_{n-1}k_{n-1} + q_{n-2}} = \frac{p_n}{q_n}$$

となる. ここで $(p_n, q_n) = 1$, $q_n > 0$ であるので $\frac{r}{t} = \frac{p_n}{q_n}$ より $r = p_n$, $t = q_n$ を得る.

一方, 定理 2.3 より n を偶数にも奇数にもすることができるので $|T|$ の値に応じて n を定めなおし

$$ru - st = p_n q_{n-1} - p_{n-1} q_n = (-1)^n \tag{5.4}$$

となるようにできる. このとき

$$ru - st = p_n u - q_n s = p_n q_{n-1} - p_{n-1} q_n$$

が成り立つ. 従って

$$p_n(u - q_{n-1}) = q_n(s - p_{n-1})$$

を得る. このとき $q_n \mid u - q_{n-1}$ となるが $q_n = t > u > 0$ であり, また $n \geq 2$ に注意すれば

$q_n \geq q_{n-1} > 0$ となるので $|u - q_{n-1}| < q_n$ が成り立つ. 従って $u = q_{n-1}$, $s = p_{n-1}$ を得る.

以上から

$$[k_0, k_1, .., k_{n-1}, \xi] = \frac{p_n\xi + p_{n-1}}{q_n\xi + q_{n-1}} = \frac{r\xi + s}{t\xi + u} = \eta$$

が成り立つ. すなわち $[k_0, k_1, .., k_{n-1}, \xi]$ は η の中間連分数である. また q_j は j について単調増加であるから $t = q_n$ となる n は一意に定まる. $|T| = 1$ ならば n が偶数, $|T| = -1$ ならば n が奇数になることは式 (5.4) より明らかである. ∎

$\eta = \dfrac{1 + \sqrt{17}}{4}$, $\xi = \dfrac{3 + \sqrt{17}}{2}$ とおくと $\eta = [1, \xi] = [1, 3, 1, 1, \xi]$ となる. 従って η と ξ は正にも負にも対等であり, 定理 5.5 における n の偶奇は η と ξ だけからは定まらない.

定理 5.6 無理数 ξ, η が対等であるとする. このとき ξ, η の中間連分数

$$\xi = [k_0, k_1, \ldots, k_{l-1}, \xi_l], \quad \eta = [h_0, h_1, \ldots, h_{m-1}, \eta_m]$$

で $\xi_l = \eta_m$ となるものが存在する. ここで ξ と η が正に対等であれば l, m ともに偶数, あるいはともに奇数とできる. また ξ と η が負に対等であれば l, m の一方は偶数, 他方は奇数となるようにできる.

Proof　ξ と η が対等であることから

$$\eta = T(\xi) = \frac{r\xi + s}{t\xi + u}, \quad T = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \in SL(\mathbb{Z})^{\pm}$$

をみたす T が存在する. ここで必要ならば T を $-T$ で置き換えて $t\xi + u > 0$ とできる. $|-T| = |T|$ より T の正負は不変である.

ξ の中間連分数を

$$\xi = [k_0, k_1, \ldots, k_{n-1}, \xi_n] = \frac{p_n\xi_n + p_{n-1}}{q_n\xi_n + q_{n-1}}$$

とする. このとき

$$\eta = T(\xi) = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \begin{bmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{bmatrix} (\xi_n)$$

となる. ここで

$$\begin{bmatrix} A_n & B_n \\ C_n & D_n \end{bmatrix} = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \begin{bmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{bmatrix}$$

とおくと

$$\eta = \frac{A_n\xi_n + B_n}{C_n\xi_n + D_n} = \begin{bmatrix} A_n & B_n \\ C_n & D_n \end{bmatrix}(\xi_n), \qquad \begin{bmatrix} A_n & B_n \\ C_n & D_n \end{bmatrix} \in SL(\mathbb{Z})^{\pm}$$

となる. 補題 2.5 より

$$\left|\xi - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}}$$

が成り立つから

$$|\xi q_n - p_n| < \frac{\frac{q_n}{q_{n+1}}}{q_n}, \qquad \frac{q_n}{q_{n+1}} < 1$$

となる. 従って $p_n = \xi q_n + \dfrac{\delta_n}{q_n},\ |\delta_n| < 1$ と表すことができる. このとき

$$\begin{aligned} C_n &= tp_n + uq_n = t(\xi q_n + \frac{\delta_n}{q_n}) + uq_n = (t\xi + u)q_n + \frac{t\delta_n}{q_n}, \\ D_n &= tp_{n-1} + uq_{n-1} = (t\xi + u)q_{n-1} + \frac{t\delta_{n-1}}{q_{n-1}} \end{aligned}$$

となる. 一方, $t\xi + u > 0$, $\lim_{n\to\infty} q_n = +\infty$ であるから十分大きい l をとると

$$q_l > q_{l-1} > 0 \quad \text{かつ} \quad \left|\frac{t\delta_{l-1}}{q_{l-1}} - \frac{t\delta_l}{q_l}\right| < t\xi + u$$

とすることができる. このとき $C_l > D_l > 0$ となるので

$$\eta = \frac{A_l\xi_l + B_l}{C_l\xi_l + D_l}, \quad (C_l > D_l > 0, \quad \xi_l > 1)$$

が成り立つ. 従って定理 5.5 よりある m に対して $\eta = [h_0, h_1, \ldots, h_{m-1}, \xi_l]$ が成り立つ.

ξ と η が正に対等の場合は l を偶数にとると ξ と ξ_l は正に対等となる. 従って η と ξ_l は正に対等となるから定理 5.5 より m は偶数にできる. また l を奇数にとると ξ と ξ_l は負に対等となるから η と ξ_l も負に対等となるので m を奇数にできる.

ξ と η が負に対等の場合は l を偶数にとると ξ と ξ_l は正に対等, η と ξ_l は負に対等となる. 従って m は奇数とできる. また l を奇数にとると ξ と ξ_l は負に対等, η と ξ_l は正に対等となるから m は偶数とできる. ∎

循環連分数

無限連分数

$$\omega = [k_0, k_1, \ldots, k_n, \ldots]$$

に対してある自然数 m, l が存在して $n > l$ のとき $k_{n+m} = k_n$ が成り立つとき, この無限連分数を周期 m の循環連分数という. このことは無理数 ω の中間連分数

$$\omega = [k_0, k_1, \ldots, k_{n-1}, \omega_n]$$

が $n > l$ のとき $\omega_{n+m} = \omega_n$ を満たすことと同値である. 特に上の関係を満たす m の中で最小のものを最小周期という. 周期が最小周期の倍数になることは明らかである.

例えば

$$\omega = [k_0, k_1, \ldots, k_l, h_1, h_2, \ldots, h_m, h_1, h_2, \ldots, h_m, h_1, h_2, \ldots]$$

は周期 m の循環連分数である. 以下これを

$$\omega = [k_0, k_1, \ldots, k_l, \dot{h_1}, h_2, \ldots, \dot{h_m}]$$

と表すことにする. 特に

$$\omega = [\dot{k_0}, k_1, \ldots, \dot{k_l}]$$

となるとき, この循環連分数を純循環連分数ということにする.

定理 5.7 無理数 ω が循環連分数として表されるならば ω は 2 次無理数である.

Proof　ω が循環連分数として表されることから, ある m, l が存在して

$$\omega = [k_0, k_1, \ldots, k_l, \dot{h_1}, \ldots, \dot{h_m}]$$

と表すことができる. ここで

$$\eta = [\dot{h_1}, h_2, \ldots, \dot{h_m}]$$

とおくと補題 5.4 より ω と η は対等である. 一方 $\eta = [h_1, \ldots, h_m, \eta]$ であるから式 (2.6) より

$$\eta = \frac{r\eta + s}{t\eta + u}\ , \qquad \begin{bmatrix} r & s \\ t & u \end{bmatrix} \in SL(\mathbb{Z})^{\pm}\ , \quad t > 0$$

と表すことができる. このとき

$$t\eta^2 + (u-r)\eta - s = 0 \ , \qquad t > 0$$

が成り立つので η は 2 次無理数である. 従って η と対等な ω も 2 次無理数である. ∎

定理 5.8 *2次無理数 ω は循環連分数として表される.*

Proof　ω を 2 次無理数とすると

$$a\omega^2 + b\omega + c = [\omega, 1] \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} \omega \\ 1 \end{bmatrix} = 0$$

をみたす整数 $a \neq 0$, b, c が存在する. 一方 ω の中間連分数は式 (2.6) より

$$\omega = [k_0, k_1, \ldots, k_{n-1}, \omega_n] = \frac{p_n\omega_n + p_{n-1}}{q_n\omega_n + q_{n-1}}$$

と表すことができる. これを $a\omega^2 + b\omega + c = 0$ に代入し, $(q_n\omega_n + q_{n-1})^2$ 倍して

$$\begin{aligned} 0 &= \begin{bmatrix} p_n\omega_n + p_{n-1}, & q_n\omega_n + q_{n-1} \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} p_n\omega_n + p_{n-1} \\ q_n\omega_n + q_{n-1} \end{bmatrix} \\ &= \begin{bmatrix} \omega_n, & 1 \end{bmatrix} \begin{bmatrix} p_n & q_n \\ p_{n-1} & q_{n-1} \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{bmatrix} \begin{bmatrix} \omega_n \\ 1 \end{bmatrix} \\ &= \begin{bmatrix} \omega_n, & 1 \end{bmatrix} \begin{bmatrix} A_n & B_n/2 \\ B_n/2 & C_n \end{bmatrix} \begin{bmatrix} \omega_n \\ 1 \end{bmatrix} \end{aligned}$$

とおく. このとき成分を比較すると次が成り立つ.

$$\begin{aligned} &A_n = ap_n{}^2 + bp_nq_n + cq_n{}^2, && B_n = 2ap_np_{n-1} + b(p_nq_{n-1} + p_{n-1}q_n) + 2cq_nq_{n-1}, \\ &C_n = ap_{n-1}{}^2 + bp_{n-1}q_{n-1} + cq_{n-1}{}^2, && B_n{}^2 - 4A_nC_n = b^2 - 4ac \end{aligned}$$

一方, 補題 2.5 より

$$\left|\omega - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2} \quad \text{が成り立つから} \quad p_n = \omega q_n + \frac{\delta_n}{q_n}, \quad (|\delta_n| < 1)$$

と表すことができる. これより

$$\begin{aligned} A_n &= a\left(\omega q_n + \frac{\delta_n}{q_n}\right)^2 + bq_n\left(\omega q_n + \frac{\delta_n}{q_n}\right) + c{q_n}^2 \\ &= (a\omega^2 + b\omega + c){q_n}^2 + (2a\omega + b)\delta_n + a\left(\frac{{\delta_n}^2}{{q_n}^2}\right) \end{aligned}$$

となるが $a\omega^2 + b\omega + c = 0$ であるから

$$A_n = (2a\omega + b)\delta_n + a\left(\frac{{\delta_n}^2}{{q_n}^2}\right) \quad \text{より} \quad |A_n| < 2|a\omega| + |b| + |a|$$

を得る. 同様にして

$$|C_n| < 2|a\omega| + |a| + |b|$$

が得られ, これより

$${B_n}^2 = 4A_nC_n + (b^2 - 4ac) \leq 4(2|a\omega| + |a| + |b|)^2 + |b^2 - 4ac|$$

も導かれる. 以上から整数 A_n, B_n, C_n は n によらず有界である. 従って

$$(A_p, B_p, C_p) = (A_q, B_q, C_q) = (A_r, B_r, C_r)$$

となる相異なる番号 p, q, r が存在する. このとき ω_p, ω_q, ω_r はすべて 2 次方程式

$$A_px^2 + B_px + C_p = 0$$

の根であるから, そのうちの 2 つは一致する. それを $\omega_p = \omega_q$, $p < q$ であるとする. このとき ω の中間連分数は

$$\omega = [k_0, k_1, \ldots, k_{p-1}, \omega_p] = [k_0, k_1, \ldots, k_{p-1}, \ldots, k_{q-1}, \omega_q]$$

となる. よって 2 次無理数 ω は循環連分数展開をもつ. ∎

定理 5.9 純循環連分数として表される無理数 ω は簡約 2 次無理数である.

Proof　ω は循環連分数として表されるので定理 5.7 より 2 次無理数である. 従って簡約性を示せばよい. ω は純循環連分数として表されるので, ある n に対して

$$\omega = [k_0, k_1, \ldots, k_{n-1}, \omega]$$

なる. このとき式 (2.6) より

$$\omega = \frac{p_n\omega + p_{n-1}}{q_n\omega + q_{n-1}} \quad \text{となるので} \quad q_n\omega^2 + (q_{n-1} - p_n)\omega - p_{n-1} = 0$$

が成り立つ. 以下 $g(x) = q_nx^2 + (q_{n-1} - p_n)x - p_{n-1} = 0$ が p.42, 式 (5.2) を満たすことを示す.

$n \geq 1$ より $q_n > 0$ であり, $g(0) = -p_{n-1} < 0$ も成り立つ. また $q_n \geq q_{n-1} \geq 0$, $p_n > p_{n-1} \geq 1$ より

$$g(-1) = (q_n - q_{n-1}) + (p_n - p_{n-1}) > 0$$

が成り立つ.

一方 $p_1 = k_0 \geq q_1 = 1$ と $p_{n+1} = p_nk_n + p_{n-1}$, $q_{n+1} = q_nk_n + q_{n-1}$ より $n \geq 1$ のとき $p_n > q_n > 0$ が成り立つ. 従って

$$g(1) = q_n + q_{n-1} - p_n - p_{n-1} = q_n\left(1 - \frac{p_n}{q_n}\right) + q_{n-1}\left(1 - \frac{p_{n-1}}{q_{n-1}}\right) < 0$$

が成り立つ. 以上で ω が簡約 2 次無理数であることが示された. ∎

補題 5.10 簡約 2 次無理数 ω の中間連分数を

$$\omega = [k_0, k_1, \ldots, k_{n-1}, \omega_n] \qquad (n = 1, 2, \ldots)$$

とする. このとき $\omega_1, \omega_2, \ldots$ はすべて簡約 2 次無理数である.

Proof　仮定より ω を根としてもつ簡約 2 次式 $g(x)$ が存在する. このとき次が成り立つ.

$$g(x) = ax^2 + bx + c, \quad g(\omega) = 0, \quad a > 0, \quad g(-1) > 0, \quad g(0) < 0, \quad g(1) < 0$$

さて $\omega = k_0 + \dfrac{1}{\omega_1}$ を $g(\omega) = 0$ に代入して ${\omega_1}^2$ 倍すれば

$$(a{k_0}^2 + bk_0 + c){\omega_1}^2 + (2ak_0 + b)\omega_1 + a = 0$$

となる. ここで

$$A = -(a{k_0}^2 + bk_0 + c), \quad B = -(2ak_0 + b), \quad C = -a, \quad h(x) = Ax^2 + Bx + C$$

とおくと $h(\omega_1) = 0$ が成り立つ. 一方 $1 \leq k_0 = \lfloor\omega\rfloor$ より $0 \leq k_0 - 1 < k_0 < \omega < k_0 + 1$ で

あるから

$$g(k_0-1)<0, \quad g(k_0)<0, \quad g(k_0+1)>0$$

が成り立つ. これより $A=-g(k_0)>0$ であり

$$h(1)=-g(k_0+1)<0, \quad h(-1)=-g(k_0-1)>0, \quad h(0)=-a<0$$

となるので h は簡約 2 次式である. ゆえに ω_1 は簡約 2 次無理数である. $\omega_2, \omega_3, \ldots$ についても同様である. ∎

定理 5.11 簡約 2 次無理数 ω は純循環連分数として表される.

Proof ω は簡約 2 次無理数であるから $\omega>1$ を満たす. 従って $k_0 \geq 1$ が成り立つことを注意しておく. ω の中間連分数を

$$\omega=[k_0, k_1, \ldots, k_{n-1}, \omega_n]$$

とおく. ω は 2 次無理数であるから定理 5.8 より循環連分数として表される. 従って, ある番号 $m, n(m>n)$ に対して $\omega_m=\omega_n$ が成り立つ. ここで $n=0$ であれば ω は純循環連分数展開されることになるから $n>0$ と仮定してよい.

さて

$$\omega_{n-1}=k_{n-1}+\frac{1}{\omega_n}, \quad \omega_{m-1}=k_{m-1}+\frac{1}{\omega_m}$$

であるから $\omega_{n-1}-\omega_{m-1}=k_{n-1}-k_{m-1}\in\mathbb{Z}$ が成り立つ. 今 ω_j と共役な 2 次無理数を ${\omega_j}'$ とし

$$\omega_{n-1}=\frac{-b_{n-1}+\sqrt{D}}{2a_{n-1}}, \quad \omega_{m-1}=\frac{-b_{m-1}+\sqrt{D}}{2a_{m-1}}$$

とおくと, $\omega_{n-1}-\omega_{m-1}\in\mathbb{Z}$ より $\omega_{n-1}-\omega_{m-1}$ の $\sqrt{D}$ の係数は 0 でなければならない. すなわち

$$\frac{\sqrt{D}}{2a_{n-1}}=\frac{\sqrt{D}}{2a_{m-1}}$$

である. 従って $\omega_{n-1}, \omega_{m-1}$ の共役

$${\omega_{n-1}}'=\frac{-b_{n-1}-\sqrt{D}}{2a_{n-1}}, \qquad {\omega_{m-1}}'=\frac{-b_{m-1}-\sqrt{D}}{2a_{m-1}}$$

に対して

$${\omega_{n-1}}'-{\omega_{m-1}}'=\omega_{n-1}-\omega_{m-1}=k_{n-1}-k_{m-1}\in\mathbb{Z}$$

が成り立つ. 一方 補題 5.10 より $\omega_{n-1}, \omega_{m-1}$ も簡約 2 次無理数であるから

$$-1 < {\omega_{n-1}}' < 0 \ , \qquad -1 < {\omega_{m-1}}' < 0$$

が成り立つ. 従って $|{\omega_{n-1}}' - {\omega_{m-1}}'| < 1$ となり, ${\omega_{n-1}}' - {\omega_{m-1}}'$ が整数であることから ${\omega_{n-1}}' - {\omega_{m-1}}' = 0$ を得る. よって $k_{n-1} = k_{m-1}$, 従って $\omega_{n-1} = \omega_{m-1}$ が成り立つ. 以上で $\omega_m = \omega_n$ ならば $\omega_{n-1} = \omega_{m-1}$ も成り立つことが示された. これを繰り返すことにより $\omega_0 = \omega_{m-n}$ が得られる. ゆえに ω は純循環連分数として表される. ∎

類数の有限性

定理 5.3 より判別式 D をもつ簡約 2 次形式の個数は有限である. これより任意の 2 次形式がある簡約 2 次形式に対等であることを示せば類数 $h(D)$ の有限であることが導かれる. 2 次形式がある簡約 2 次形式に対等であることを示すには, 2 次無理数がある簡約 2 次無理数に対等であることを示せばよい.

定理 5.12 任意の 2 次無理数はある簡約 2 次無理数に正に対等である.

Proof ξ を 2 次無理数とする. ξ の中間連分数を

$$\xi = [k_0, k_1, \ldots, k_{n-1}, \xi_n]$$

とおく. 定理 5.8 より, ある $m, n(m > n)$ に対して $\xi_n = \xi_m$ となる. このとき

$$\xi = [k_0, k_1, \ldots, k_{n-1}, \xi_n] = [k_0, k_1, \ldots, k_{m-1}, \xi_m] = [k_0, k_1, \ldots, k_{m-1}, \xi_n]$$

であるから

$$\xi_n = [k_n, \ldots, k_{m-1}, \xi_n]$$

となるので ξ_n は純循環連分数に展開される. 従って定理 5.9 より ξ_n は簡約 2 次無理数である. ここで n が奇数のときは補題 5.10 より ξ_{n+1} も簡約 2 次無理数であるから n を $n+1$ で置き換えて, 最初から n が偶数であると仮定してよい. このとき

$$\xi = \frac{p_n\xi_n + p_{n-1}}{q_n\xi_n + q_{n-1}}, \quad p_nq_{n-1} - p_{n-1}q_n = (-1)^n = 1$$

となるので ξ と簡約 2 次無理数 ξ_n とが正に対等である. ∎

系 5.13 任意の正の判別式 D に対して $h(D)$, $h^+(D)$ は有限である.

定理 5.14 ξ を簡約 2 次無理数とし, その中間連分数を $\xi = [k_0, k_1, \ldots, k_{n-1}, \xi_n]$ とおく. また ξ の連分数展開における最小周期を m とする. このとき $\xi_0 = \xi, \xi_1, \ldots, \xi_{m-1}$ は互いに異なる対等な簡約 2 次無理数であり, m が奇数であれば $\xi_0, \xi_1, \ldots, \xi_{m-1}$ は互いに正に対等である. また m が偶数であれば $\xi_0, \xi_2, \ldots, \xi_{m-2}$ は互いに正に対等であるが, ξ と $\xi_1, \xi_3, \ldots, \xi_{m-1}$ は負に対等となるが正に対等でない.

Proof $\xi_0, \ldots, \xi_{m-1}$ は補題 5.4, 補題 5.10 より互いに対等な簡約 2 次無理数である. また m が ξ の連分数展開における最小周期であるから $\xi_0, \xi_1, \ldots, \xi_{m-1}$ は互いに異なる. 補題 5.4 より ξ と ξ_{2n} は正に対等である. m が奇数のときは $\xi_n = \xi_{m+n}$ となるから n が奇数であっても $m+n$ が偶数となり ξ と $\xi_{m+n} = \xi_n$ が正に対等となる. 従って m が奇数であれば $\xi_0, \xi_1, \ldots, \xi_{m-1}$ は互いに正に対等である.

m が偶数であるとする. 補題 5.4 より $\xi_0, \xi_2, \ldots, \xi_{m-2}$ は互いに正に対等であり, ξ と $\xi_1, \xi_3, \ldots, \xi_{m-1}$ は負に対等である. 今 n が奇数で ξ と ξ_n が正に対等であると仮定する. このとき定理 5.6 より共に偶数であるか, 共に奇数であるような r と s で $\xi_r = \xi_{n+s}$ となるものが存在する. このとき $n+s-r$ は奇数であり, 最小周期 m が偶数であることに矛盾する. 従って n が奇数のとき ξ と ξ_n は正に対等でない. ∎

定理 5.15 ξ を簡約 2 次無理数, その中間連分数を $\xi = [k_0, k_1, \ldots, k_{n-1}, \xi_n]$, 連分数展開における最小周期を m とする. このとき ξ に対等な簡約 2 次無理数は $\xi_0 = \xi, \xi_1, \ldots, \xi_{m-1}$ に限る.

Proof η を ξ に対等な簡約 2 次無理数とし, その中間連分数を $\eta = [u_0, u_1, \ldots, u_{n-1}, \eta_n]$, とおく. 定理 5.6 より $\xi_r = \eta_s$ となる番号 r, s が存在する. η は簡約 2 次無理数であるから η_s のある中間連分数が $\eta_s = [u_j, u_{j+1}, ..., \eta]$ となる. ここで $\eta_s = \xi_r$ であるから η は $\xi_0 = \xi, \xi_1, \ldots, \xi_{m-1}$ のいずれかに一致する. ゆえに ξ に対等な簡約 2 次無理数は $\xi_0 = \xi, \xi_1, \ldots, \xi_{m-1}$ に限る. ∎

5.3 類数の計算例

D = 60 の場合

$f(x,y)=ax^2+bxy+cy^2$ を判別式 60 の簡約 2 次形式とする. $\lfloor\sqrt{60}\rfloor=7$ であるから定理 5.3 の証明からわかるように $b=-1,-2,-3,\ldots,-7$ である. また $4ac=b^2-D$ であるから b は偶数, $4ac=-56,-44,-24$ となる. これより $ac=-14,-11,-6$ を得る. 従って p.41 の簡約 2 次形式の条件 (5.1) を満たす (a,b,c) は

$$(6,-6,-1),\quad (3,-6,-2),\quad (2,-6,-3),\quad (1,-6,-6)$$

の 4 個である. 従って $f(x)$ は

$$f_1(x,y)=6x^2-6xy-y^2,\quad f_2(x,y)=3x^2-6xy-2y^2,$$
$$f_3(x,y)=2x^2-6xy-3y^2,\quad f_4(x,y)=x^2-6xy-6y^2$$

のいずれかである. 対応する簡約 2 次無理数は

$$\xi_1=\frac{3+\sqrt{15}}{6},\quad \xi_2=\frac{3+\sqrt{15}}{3},\quad \xi_3=\frac{3+\sqrt{15}}{2},\quad \xi_4=3+\sqrt{15}$$

となり, 連分数展開は

$$\xi_1=[\dot{1},\dot{6}],\quad \xi_2=[\dot{2},\dot{3}],\quad \xi_3=[\dot{3},\dot{2}],\quad \xi_4=[\dot{6},\dot{1}]$$

である. 従って定理 5.15 より $\xi_1\sim\xi_4$, $\xi_2\sim\xi_3$, $\xi_1\not\sim\xi_2$ となる. よって $h(D)=2$ である. また周期が偶数であるから定理 5.14 より $h^+(D)=4$ である.

D = 136 の場合

$f(x,y)=ax^2+bxy+cy^2$ を判別式 136 の簡約 2 次形式とする. $\lfloor\sqrt{136}\rfloor=11$ より $b=-1,-2,-3,\ldots,-11$ である. また $4ac=b^2-D$ より $4ac=-132,-120,-100,-72,-36$ を得る. これより $ac=-33,-30,-25,-18,-9$ となる. 従って条件 (5.1) を満たす (a,b,c) は次の 10 個である.

$$(5,-6,-5),\quad (5,-4,-6),\quad (6,-4,-5),\quad (2,-8,-9),\quad (3,-8,-6),$$
$$(6,-8,-3),\quad (9,-8,-2),\quad (1,-10,-9),\quad (3,-10,-3),\quad (9,-10,-1)$$

以上から $f(x,y)=ax^2+bxy+cy^2$ は次のいずれかである.

$$f_1(x,y)=5x^2-6xy-5y^2,\quad f_2(x,y)=5x^2-4xy-6y^2,\quad f_3(x,y)=6x^2-4xy-5y^2,$$
$$f_4(x,y)=2x^2-8xy-9y^2,\quad f_5(x,y)=3x^2-8xy-6y^2,\quad f_6(x,y)=6x^2-8xy-3y^2,$$
$$f_7(x,y)=9x^2-8xy-2y^2,\quad f_8(x,y)=x^2-10xy-9y^2,\quad f_9(x,y)=3x^2-10xy-3y^2,$$
$$f_{10}(x,y)=9x^2-10xy-y^2$$

対応する簡約 2 次無理数は

$$\xi_1=\frac{3+\sqrt{34}}{5},\quad \xi_2=\frac{2+\sqrt{34}}{5},\quad \xi_3=\frac{2+\sqrt{34}}{6},\quad \xi_4=\frac{4+\sqrt{34}}{2},$$
$$\xi_5=\frac{4+\sqrt{34}}{3},\quad \xi_6=\frac{4+\sqrt{34}}{6},\quad \xi_7=\frac{4+\sqrt{34}}{9},\quad \xi_8=5+\sqrt{34},$$
$$\xi_9=\frac{5+\sqrt{34}}{3},\quad \xi_{10}=\frac{5+\sqrt{34}}{9}$$

となり, 連分数展開は

$$\xi_1=[\dot{1},1,3,3,1,\dot{1}],\quad \xi_2=[\dot{1},1,1,3,3,\dot{1}],\quad \xi_3=[\dot{1},3,3,1,1,\dot{1}],\quad \xi_4=[\dot{4},1,10,\dot{1}],$$
$$\xi_5=[\dot{3},3,1,1,1,\dot{1}],\quad \xi_6=[\dot{1},1,1,1,3,\dot{3}],\quad \xi_7=[\dot{1},10,1,\dot{4}],\qquad \xi_8=[\dot{1}\dot{0},1,4,\dot{1}],$$
$$\xi_9=[\dot{3},1,1,1,1,\dot{3}],\quad \xi_{10}=[\dot{1},4,1,\dot{1}\dot{0}]$$

である. 従って

$$\xi_1\sim\xi_2\sim\xi_3\sim\xi_5\sim\xi_6\sim\xi_9,\quad \xi_4\sim\xi_7\sim\xi_8\sim\xi_{10},\quad \xi_1\not\sim\xi_4$$

であるから $h(D)=2$ である. また周期が偶数であるから $h^+(D)=4$ である.

次の表はいくつかの正の非平方数 D に対して, 判別式 D をもつ簡約 2 次形式及び類数, 狭義の類数を決定したものである.

判別式Dの簡約 2 次形式及び類数 $h(D)$, 狭義の類数 $h^+(D)$					
D	簡約 2 次形式	簡約 2 次無理数	連分数展開	$h(D)$	$h^+(D)$
5	$f(x,y)=x^2-xy-y^2$	$\xi=\frac{1+\sqrt{5}}{2}$	$\xi=[\dot{1}]$	1	1
8	$f(x,y)=x^2-2xy-y^2$	$\xi=1+\sqrt{2}$	$\xi=[\dot{2}]$	1	1
12	$f_1(x,y)=2x^2-2xy-y^2$	$\xi_1=\frac{1+\sqrt{3}}{2}$	$\xi_1=[\dot{1},\dot{2}]$	1	2
	$f_2(x,y)=x^2-2xy-2y^2$	$\xi_2=1+\sqrt{3}$	$\xi_2=[\dot{2},\dot{1}]$		
13	$f(x,y)=x^2-3xy-y^2$	$\xi=\frac{3+\sqrt{13}}{2}$	$\xi=[\dot{3}]$	1	1
17	$f_1(x,y)=x^2-3xy-2y^2$	$\xi_1=\frac{3+\sqrt{17}}{2}$	$\xi_1=[\dot{3},1,\dot{1}]$	1	1
	$f_2(x,y)=2x^2-xy-2y^2$	$\xi_2=\frac{1+\sqrt{17}}{4}$	$\xi_2=[\dot{1},3,\dot{1}]$		
	$f_3(x,y)=2x^2-3xy-y^2$	$\xi_3=\frac{3+\sqrt{17}}{4}$	$\xi_3=[\dot{1},1,\dot{3}]$		
20	$f_1(x,y)=2x^2-2xy-2y^2$	$\xi_1=\frac{1+\sqrt{5}}{2}$	$\xi_1=[\dot{1}]$	2	2
	$f_2(x,y)=x^2-4xy-y^2$	$\xi_2=2+\sqrt{5}$	$\xi_2=[\dot{4}]$		
21	$f_1(x,y)=x^2-3xy-3y^2$	$\xi_1=\frac{3+\sqrt{21}}{2}$	$\xi_1=[\dot{3},\dot{1}]$	1	2
	$f_2(x,y)=3x^2-3xy-y^2$	$\xi_2=\frac{3+\sqrt{21}}{6}$	$\xi_2=[\dot{1},\dot{3}]$		
24	$f_1(x,y)=x^2-4xy-2y^2$	$\xi_1=2+\sqrt{6}$	$\xi_1=[\dot{4},\dot{2}]$	1	2
	$f_2(x,y)=2x^2-4xy-y^2$	$\xi_2=\frac{2+\sqrt{6}}{2}$	$\xi_2=[\dot{2},\dot{4}]$		
28	$f_1(x,y)=x^2-4xy-3y^2$	$\xi_1=2+\sqrt{7}$	$\xi_1=[\dot{4},1,1,\dot{1}]$	1	2
	$f_2(x,y)=2x^2-2xy-3y^2$	$\xi_2=\frac{1+\sqrt{7}}{2}$	$\xi_2=[\dot{1},1,4,\dot{1}]$		
	$f_3(x,y)=3x^2-2xy-2y^2$	$\xi_3=\frac{1+\sqrt{7}}{3}$	$\xi_3=[\dot{1},4,1,\dot{1}]$		
	$f_4(x,y)=3x^2-4xy-y^2$	$\xi_4=\frac{2+\sqrt{7}}{3}$	$\xi_4=[\dot{1},1,1,\dot{4}]$		
29	$f(x,y)=x^2-5xy-y^2$	$\xi=\frac{5+\sqrt{29}}{2}$	$\xi=[\dot{5}]$	1	1
32	$f_1(x,y)=x^2-4xy-4y^2$	$\xi_1=2+2\sqrt{2}$	$\xi_1=[\dot{4},\dot{1}]$	2	3
	$f_2(x,y)=2x^2-4xy-2y^2$	$\xi_2=1+\sqrt{2}$	$\xi_2=[\dot{2}]$		
	$f_3(x,y)=4x^2-4xy-y^2$	$\xi_3=\frac{1+\sqrt{2}}{2}$	$\xi_3=[\dot{1},\dot{4}]$		
33	$f_1(x,y)=2x^2-3xy-3y^2$	$\xi_1=\frac{3+\sqrt{33}}{4}$	$\xi_1=[\dot{2},5,2,\dot{1}]$	1	2
	$f_2(x,y)=3x^2-3xy-2y^2$	$\xi_2=\frac{3+\sqrt{33}}{6}$	$\xi_2=[\dot{1},2,5,\dot{2}]$		
	$f_3(x,y)=x^2-5xy-2y^2$	$\xi_3=\frac{5+\sqrt{33}}{2}$	$\xi_3=[\dot{5},2,1,\dot{2}]$		
	$f_4(x,y)=2x^2-5xy-y^2$	$\xi_4=\frac{5+\sqrt{33}}{4}$	$\xi_4=[\dot{2},1,2,\dot{5}]$		
37	$f_1(x,y)=3x^2-xy-3y^2$	$\xi_1=\frac{1+\sqrt{37}}{6}$	$\xi_1=[\dot{1},5,\dot{1}]$	1	1
	$f_2(x,y)=x^2-5xy-3y^2$	$\xi_2=\frac{5+\sqrt{37}}{2}$	$\xi_2=[\dot{5},1,\dot{1}]$		
	$f_3(x,y)=3x^2-5xy-y^2$	$\xi_3=\frac{5+\sqrt{37}}{6}$	$\xi_3=[\dot{1},1,\dot{5}]$		
40	$f_1(x,y)=3x^2-2xy-3y^2$	$\xi_1=\frac{1+\sqrt{10}}{3}$	$\xi_1=[\dot{1},2,\dot{1}]$	2	2
	$f_2(x,y)=2x^2-4xy-3y^2$	$\xi_2=\frac{2+\sqrt{10}}{2}$	$\xi_2=[\dot{2},1,\dot{1}]$		
	$f_3(x,y)=3x^2-4xy-2y^2$	$\xi_3=\frac{2+\sqrt{10}}{3}$	$\xi_3=[\dot{1},1,\dot{2}]$		
	$f_4(x,y)=x^2-6xy-y^2$	$\xi_4=3+\sqrt{10}$	$\xi_4=[\dot{6}]$		

6 章　2 次形式による整数の表示

2 次形式 $f(x,y)=ax^2+bxy+cy^2$ と整数 n に対して $f(x,y)=n$ を満たす整数 x,y が存在するとき n は f によって表示されるという.

この章では「与えられた 2 次形式が自然数 n を表示するか」, あるいは,「与えられた判別式をもつ 2 次形式の中に自然数 n を表示するものが存在するか」といった問題について考察する.

2 次形式 f が 0 を表示することは明かであり, 2 次形式 f が負の数 $-n$ を表示することは 2 次形式 $-f$ が自然数 n を表示することと同値である. これより 2 次形式による整数の表示問題は, 自然数の表示問題に帰着される.

6.1　自然数を表示するための条件

以下 $f(x,y)=ax^2+bxy+cy^2$ を判別式 D の 2 次形式, n を自然数とする.

整数の組 (r,t) が $f(x,y)=n$ の原始解であるとは $f(r,t)=n$ かつ r,t が互いに素であるときにいう. またこのとき n は f により原始的に表示されるという. n が f により表示されても原始的に表示されるとは限らない. 例えば $f(x,y)=x^2+y^2$ のとき $2^2+2^2=8$ より, 8 は f により表示されるが, 原始的には表示されない. (α,β) が $f(x,y)=n$ の非原始解であり, その最大公約数が d であるとき, 明らかに d^2 は n を割り切る. ここで

$$\alpha=\alpha' d,\quad \beta=\beta' d,\quad n=n' d^2$$

とおけば (α',β') は $f(x,y)=n'$ の原始解である. これより 2 次形式による整数の表示問題は原始解の存在問題に帰着される. 特に n が素数である場合等, 1 以外の平方数で割り切れないときには $f(x,y)=n$ の解は常に原始解である.

補題 6.1 $m^2\equiv D \pmod{4n}$, $0\le m<2n$ を満たす整数 m が存在するとき, n は判別式 D のある 2 次形式により原始的に表示される.

Proof 仮定より $l = \dfrac{m^2 - D}{4n}$ が整数であることから, 2次形式 $g(x,y) = nx^2 + mxy + ly^2$ が定まる. g の判別式は $m^2 - 4nl = D$ であり $g(1,0) = n$ であることから, n は判別式 D の2次形式 g により原始的に表示される. ∎

定理 6.2 自然数 n が, 判別式 D のある2次形式で原始的に表示されるための必要十分条件は

$$m^2 \equiv D \pmod{4n}, \qquad 0 \leq m < 2n$$

を満たす整数 m が存在することである.

Proof 十分性は補題6.1で示されているので必要性を示す. 自然数 n が判別式 D のある2次形式 $f(x,y) = ax^2 + bxy + cy^2$ で原始的に表示されたと仮定する. $f(x,y) = n$ の1つの原始解を (r,t) とする. r, t は互いに素であるから1次不定方程式

$$ry - tx = 1 \tag{6.1}$$

に整数解 $x = s$, $y = u$ が存在する. $T = \begin{bmatrix} r & s \\ t & u \end{bmatrix}$ とおくと T は正の特殊1次変換である. このとき

$$\begin{bmatrix} n & m/2 \\ m/2 & l \end{bmatrix} = T^t \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} T, \qquad \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix}$$

により $f(x,y)$ に正に対等な2次形式

$$g(x', y') = nx'^2 + mx'y' + ly'^2$$

が定まる. ここで関係式

$$\begin{cases} n = ar^2 + brt + ct^2 \\ m = 2ars + b(ru + st) + 2ctu \\ l = as^2 + bsu + cu^2 \end{cases}$$

が成り立つことに注意されたい.

さて方程式 (6.1) の1つの解を (s_0, u_0) とすると一般解は

$$s = s_0 + rk, \quad u = u_0 + tk \quad (k \in \mathbb{Z})$$

と表される. これを $m = 2ars + b(ru + st) + 2ctu$ に代入すると

$$\begin{aligned} m &= 2ar(s_0 + rk) + b(ru_0 + rtk + s_0t + rtk) + 2ct(u_0 + tk) \\ &= 2ars_0 + b(ru_0 + s_0t) + 2ctu_0 + 2nk \end{aligned}$$

となることから

$$m \equiv 2ars_0 + b(ru_0 + s_0t) + 2ctu_0 \pmod{2n}$$

が成り立つ. 従って k を適当に選んで m が $0 \leq m < 2n$ を満たすようにできる.

一方 g は f に正に対等であるから判別式が一致するので

$$D = b^2 - 4ac = m^2 - 4nl$$

が成り立つ. ゆえに

$$m^2 \equiv D \pmod{4n}, \qquad 0 \leq m < 2n$$

を満たす整数 m の存在が示された. ∎

判定方法

上述の結果からのみでは $m^2 \equiv D \pmod{4n}$ かつ $0 \leq m < 2n$ を満たす整数 m が存在しても, 特定の 2 次形式 $f(x, y) = ax^2 + bxy + cy^2$ が n を表示するかどうかは判定できない. しかし定理 6.2 の証明からわかるように 2 次形式 f が n を表示すれば $f(x, y)$ に正に対等な 2 次形式

$$g(x', y') = nx'^2 + mx'y' + ly'^2$$

であって

$$D = b^2 - 4ac = m^2 - 4nl \quad \text{かつ} \quad m^2 \equiv D \pmod{4n}, \quad 0 \leq m < 2n \tag{6.2}$$

を満たすものが存在する.

- 式 (6.2) を満たす m, l は有限個であるから, それぞれに対して

$$\begin{bmatrix} n & m/2 \\ m/2 & l \end{bmatrix} = \begin{bmatrix} r & t \\ s & u \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} r & s \\ t & u \end{bmatrix}$$

を満たす正の特殊1次変換 $T = \begin{bmatrix} r & s \\ t & u \end{bmatrix}$ が存在するかどうか判定する.

- ある m, l に対して上のような T が存在すれば n は f で原始的に表示される. このとき (r, t) が $f(x, y) = n$ の原始解である.

特に判別式 D の狭義の類数 $h^+(D)$ が 1 の場合, f と g は必ず正に対等となり $m^2 \equiv D \pmod{4n}$, $(0 \leq m < 2n)$ を満たす m が存在するとき n は f で原始的に表示される.

原理的には上述の手順で, n が f によって表示されるかどうか判定し, 表示される場合はすべての原始解を求めることができる. 判別式が負の場合は定理 4.2 より上のような T は常に有限個であるから, $f(x, y) = n$ の原始解も有限個である. しかし判別式が正の場合には $f(x, y) = n$ の原始解は無限個となる場合があり, 原始解を求める計算も容易でない.

6.2 計算例・素数の表示

最後に与えられた2次形式がどのような奇素数を表示しうるか調べることにする. なお奇素数 p が2次形式で表示されるときは原始的な表示に限ることを注意しておく. また以下の計算では平方剰余に関する次の結果を利用する.

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod 4 \\ -1, & p \equiv 3 \pmod 4 \end{cases}$$

$$\left(\frac{-2}{p}\right) = \begin{cases} 1, & p \equiv 1, 3 \pmod 8 \\ -1, & p \equiv 5, 7 \pmod 8 \end{cases}$$

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & p \equiv 1, 11 \pmod{12} \\ -1, & p \equiv 5, 7 \pmod{12} \end{cases}$$

$$\left(\frac{-3}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod 3 \\ -1, & p \equiv 2 \pmod 3 \end{cases}$$

$$\left(\frac{5}{p}\right) = \begin{cases} 1, & p \equiv 1, 4 \pmod 5 \\ -1, & p \equiv 2, 3 \pmod 5 \end{cases}$$

$$\left(\frac{-5}{p}\right) = \begin{cases} 1, & p \equiv 1, 3, 7, 9 \pmod{20} \\ -1, & p \equiv 11, 13, 17, 19 \pmod{20} \end{cases}$$

D = −3 の場合

p.40 の表から $\tilde{h}^+(-3) = 1$ である. また判別式 -3 の簡約 2 次形式は

$$f(x, y) = x^2 + xy + y^2$$

である. 奇素数 p が 判別式 -3 をもつ 2 次形式で表示されるための必要十分条件は定理 6.2 により

$$m^2 \equiv -3 \pmod{4p}, \quad 0 \leq m < 2p$$

となる m が存在することである. このとき $x^2 \equiv -3 \pmod{p}$ が解をもつ. 逆に $x^2 \equiv -3 \pmod{p}$ が解 α $(0 \leq \alpha < p)$ をもつときは, m を α または $\alpha + p$ の奇数の方とおけば

$$m^2 \equiv -3 \pmod{4p}, \quad 0 \leq m < 2p$$

を満たす. 従って求める素数は $x^2 \equiv -3 \pmod{p}$ が解をもつようなもの, すなわち

$$p = 3 \quad \text{または} \quad p \equiv 1 \pmod{3}$$

を満たすものである. このような素数のうち 100 以下のものは

$$3,\ 7,\ 13,\ 19,\ 31,\ 37,\ 43,\ 61,\ 67,\ 73,\ 79,\ 97$$

である. これらを簡約 2 次形式 $f(x, y) = x^2 + xy + y^2$ により表示すると次のようになる.

$$\begin{aligned}
3 &= 1^2 + 1\cdot 1 + 1^2 = f(1,1) & \qquad 7 &= 2^2 + 2\cdot 1 + 1^2 = f(2,1)\\
13 &= 3^2 + 3\cdot 1 + 1^2 = f(3,1) & \qquad 19 &= 3^2 + 3\cdot 2 + 2^2 = f(3,2)\\
31 &= 5^2 + 5\cdot 1 + 1^2 = f(5,1) & \qquad 37 &= 4^2 + 4\cdot 3 + 3^2 = f(4,3)\\
43 &= 6^2 + 6\cdot 1 + 1^2 = f(6,1) & \qquad 61 &= 5^2 + 5\cdot 4 + 4^2 = f(5,4)\\
67 &= 7^2 + 7\cdot 2 + 2^2 = f(7,2) & \qquad 73 &= 8^2 + 8\cdot 1 + 1^2 = f(8,1)\\
79 &= 7^2 + 7\cdot 3 + 3^2 = f(7,3) & \qquad 97 &= 8^2 + 8\cdot 3 + 3^2 = f(8,3)
\end{aligned}$$

D = −4 の場合

p.40 の表から $\tilde{h}^+(-4) = 1$ である. また判別式 -4 の簡約 2 次形式は

$$f(x, y) = x^2 + y^2$$

である. 奇素数 p が 判別式 -4 をもつ 2 次形式で表示されるための必要十分条件は定理 6.2 により

$$m^2 \equiv -4 \pmod{4p}, \quad 0 \leq m < 2p$$

となる m が存在することである. このような m が存在すれば偶数でなければならないから $m = 2m_0$ とおくことができる. このとき

$$m_0{}^2 \equiv -1 \pmod{p}, \quad 0 \leq m_0 < p$$

が成り立つ. 逆に上式を満たす m_0 が存在すれば $m = 2m_0$ は

$$m^2 \equiv -4 \pmod{4p}, \quad 0 \leq m < 2p$$

を満たす. 以上から判別式 -4 の 2 次形式で表示される奇素数 p は

$$x^2 \equiv -1 \pmod{p}$$

が解をもつ奇素数, すなわち $\left(\dfrac{-1}{p}\right) = 1$ となるものである. これらは $p \equiv 1 \pmod{4}$ を満たすものに他ならない. このような素数で 100 以下のものは

$$5,\ 13,\ 17,\ 29,\ 37,\ 41,\ 53,\ 61,\ 73,\ 89,\ 97$$

である. これらを簡約 2 次形式 $f(x,y) = x^2 + y^2$ により表示すると次のようになる.

$$\begin{aligned}
5 &= 1^2 + 2^2 = f(1,2) & 13 &= 2^2 + 3^2 = f(2,3)\\
17 &= 1^2 + 4^2 = f(1,4) & 29 &= 2^2 + 5^2 = f(2,5)\\
37 &= 1^2 + 6^2 = f(1,6) & 41 &= 4^2 + 5^2 = f(4,5)\\
53 &= 2^2 + 7^2 = f(2,7) & 61 &= 5^2 + 6^2 = f(5,6)\\
73 &= 3^2 + 8^2 = f(3,8) & 89 &= 5^2 + 8^2 = f(5,8)\\
97 &= 4^2 + 9^2 = f(4,9)
\end{aligned}$$

D = −20 の場合

p.40 の表から $\tilde{h}^+(-20) = 2$ である. 判別式 -20 の簡約 2 次形式は

$$f_1(x,y) = x^2 + 5y^2, \qquad f_2(x,y) = 2x^2 + 2xy + 3y^2$$

であるが, 1 は f_1 で表示されるが, f_2 では表示されない. 従って f_1 と f_2 は対等でない. 奇素数 p が 判別式 -20 をもつ 2 次形式で表示されるための必要十分条件は

$$m^2 \equiv -20 \pmod{4p}, \quad 0 \leq m < 2p$$

となる m が存在することである. このような m が存在すれば偶数でなければならないから $m = 2m_0$ とおくことができる. このとき

$$m_0{}^2 \equiv -5 \pmod{p}, \quad 0 \leq m_0 < p$$

が成り立つ. 逆に上式を満たす m_0 が存在すれば $m = 2m_0$ は

$$m^2 \equiv -20 \pmod{4p}, \quad 0 \leq m < 2p$$

を満たす. 以上から判別式 -20 の 2 次形式で表示される奇素数 p は

$$p = 5 \quad \text{または} \quad p \equiv 1, 3, 7, 9 \pmod{20}$$

を満たす. このような素数で 100 以下のものは

$$3,\ 5,\ 7,\ 23,\ 29,\ 41,\ 43,\ 47,\ 61,\ 67,\ 83,\ 89$$

である. f_1, f_2 のどちらで表示されるかは次のようにして判定できる.

$f_1(x, y) = x^2 + 5y^2 = p$ とすると $x^2 \equiv p \pmod{5}$ となり $p = 5$ または $\left(\frac{p}{5}\right) = 1$ となることから $p = 5$ または $p \equiv 1, 9 \pmod{20}$ を得る.

$f_2(x, y) = 2x^2 + 2xy + 3y^2 = p$ とする. $f_2(x, y)$ は 5 を表示できないので $p \neq 5$ である. $4x^2 + 4xy + 6y^2 = 2p$ より $(2x + y)^2 + 5y^2 = 2p$, 従って $(2x + y)^2 \equiv 2p \pmod{5}$ となる. これより $\left(\frac{2p}{5}\right) = 1$ となる. $\left(\frac{2}{5}\right) = -1$ であるから $\left(\frac{p}{5}\right) = -1$ となる. ゆえに $p \equiv 3, 7 \pmod{20}$ を得る.

上にあげた 100 以下の素数を $f_1(x,y)$ または $f_2(x,y)$ で表示すると次のようになる.

$f_1(x,y)=x^2+5y^2$	$f_2(x,y)=2x^2+2xy+3y^2$
$5=0^2+5\cdot 1^2=f_1(0,1)$	$3=2\cdot 1^2+2\cdot 1\cdot(-1)+3\cdot(-1)^2=f_2(1,-1)$
$29=3^2+5\cdot 2^2=f_1(3,2)$	$7=2\cdot 1^2+2\cdot 1\cdot 1+3\cdot 1^2=f_2(1,1)$
$41=6^2+5\cdot 1^2=f_1(6,1)$	$23=2\cdot 2^2+2\cdot 2\cdot(-3)+3\cdot(-3)^2=f_2(2,-3)$
$61=4^2+5\cdot 3^2=f_1(4,3)$	$43=2\cdot 5^2+2\cdot 5\cdot(-1)+3\cdot(-1)^2=f_2(5,-1)$
$89=3^2+5\cdot 4^2=f_1(3,4)$	$47=2\cdot 5^2+2\cdot 5\cdot(-3)+3\cdot(-3)^2=f_2(5,-3)$
	$67=2\cdot 1^2+2\cdot 1\cdot(-5)+3\cdot(-5)^2=f_2(1,-5)$
	$83=2\cdot 7^2+2\cdot 7\cdot(-3)+3\cdot(-3)^2=f_2(7,-3)$

D = −24 の場合

p.40 の表から $\tilde{h}^+(-24)=2$ である. 判別式 -20 の簡約 2 次形式は

$$f_1(x,y)=x^2+6y^2, \qquad f_2(x,y)=2x^2+3y^2$$

であるが, 1 は f_1 で表示されるが, f_2 では表示されない. 従って f_1 と f_2 は対等でない. 奇素数 p が判別式 -24 をもつ 2 次形式 $f(x,y)$ で表示される必要十分条件は

$$m^2\equiv -24 \pmod{4p}, \quad 0\le m<2p$$

となる m が存在することである. このような m が存在すれば偶数でなければならないから $m=2m_0$ とおくことができる. このとき

$$m_0{}^2\equiv -6 \pmod{p}, \quad 0\le m_0<p$$

が成り立つ. 逆に上式を満たす m_0 が存在すれば $m=2m_0$ は

$$m^2\equiv -24 \pmod{4p}, \quad 0\le m<2p$$

を満たす. 以上から判別式 -24 の 2 次形式で表示される奇素数 p は

$$p=3 \quad \text{または} \quad \left(\frac{-6}{p}\right)=1$$

となるもの, すなわち

$$p = 3 \quad \text{または} \quad p \equiv 1, 5, 7, 11 \pmod{24}$$

を満たすものである. 従って判別式 -24 をもつ 2 次形式で表示される 100 以下の奇素数は

$$3,\ 5,\ 7,\ 11,\ 29,\ 31,\ 53,\ 59,\ 73,\ 79,\ 83,\ 97$$

である. f_1, f_2 のどちらで表示されるかは次のようにして判定できる.

$f_1(x, y) = x^2 + 6y^2 = p$ とする. 明らかに $p \neq 3$ であるので $x^2 \equiv p \pmod 3$ となり, $\left(\frac{p}{3}\right) = 1$ を得る. 従って $p \equiv 1, 7 \pmod{24}$ を得る.

$f_2(x, y) = 2x^2 + 3y^2 = p$ とすると $2x^2 \equiv p \pmod 3$ となる. これより $p = 3$ または

$$\left(\frac{p}{3}\right) = \left(\frac{2x^2}{3}\right) = \left(\frac{2}{3}\right) = -1$$

が成り立つ. 従って $p = 3$ であるか $p \equiv 5, 11 \pmod{24}$ を満たす.

上にあげた 100 以下の素数を $f_1(x, y)$ または $f_2(x, y)$ で表示すると次のようになる.

$f_1(x, y) = x^2 + 6y^2$	$f_2(x, y) = 2x^2 + 3y^2$
$7 = 1^2 + 6 \cdot 1^2 = f_1(1, 1)$	$3 = 2 \cdot 0^2 + 3 \cdot 1^2 = f_2(0, 1)$
$31 = 5^2 + 6 \cdot 1^2 = f_1(5, 1)$	$5 = 2 \cdot 1^2 + 3 \cdot 1^2 = f_2(1, 1)$
$73 = 7^2 + 6 \cdot 2^2 = f_1(7, 2)$	$11 = 2 \cdot 2^2 + 3 \cdot 1^2 = f_2(2, 1)$
$79 = 5^2 + 6 \cdot 3^2 = f_1(5, 3)$	$29 = 2 \cdot 1^2 + 3 \cdot 3^2 = f_2(1, 3)$
$97 = 1^2 + 6 \cdot 4^2 = f_1(1, 4)$	$53 = 2 \cdot 5^2 + 3 \cdot 1^2 = f_2(5, 1)$
	$59 = 2 \cdot 4^2 + 3 \cdot 3^2 = f_2(4, 3)$
	$83 = 2 \cdot 2^2 + +3 \cdot 5^2 = f_2(2, 5)$

D = 5 の場合

p.56 の表から $h(5) = h^+(5) = 1$ であり, 簡約 2 次形式は $f(x, y) = x^2 - xy - y^2$ である. 奇素数 p が判別式 5 をもつ 2 次形式で表示されるための必要十分条件は

$$m^2 \equiv 5 \pmod{4p}, \qquad 0 \leq m < 2p$$

となる m が存在することである. このとき

$$x^2 \equiv 5 \pmod{p}$$

は $0 \leq x < p$ を満たす解をもつ. 逆に $\alpha^2 \equiv 5 \pmod{p}$, $0 \leq \alpha < p$ を満たす α が存在するときは α または $\alpha + p$ の奇数の方を m とおけば

$$m^2 \equiv 5 \pmod{4p}, \qquad 0 \leq m < 2p$$

を満たす. 以上から判別式 5 の 2 次形式で表示できる奇素数は

$$p = 5 \quad \text{または} \quad p \equiv 1, 4 \pmod{5}$$

を満たすものであることがわかる. これらのうち 100 以下のものは

$$5,\ 11,\ 19,\ 29,\ 31,\ 41,\ 59,\ 61,\ 71,\ 79,\ 89$$

である. これらを簡約 2 次形式 $f(x, y) = x^2 - xy - y^2$ を用いて表示すると次のようになる.

$5 = 2^2 - 2\cdot(-1) - (-1)^2 = f(2, -1)$　　$11 = 3^2 - 3\cdot(-1) - (-1)^2 = f(3, -1)$
$19 = 5^2 - 5\cdot 1 - 1^2 = f(5, 1)$　　$29 = 5^2 - 5\cdot(-1) - (-1)^2 = f(5, -1)$
$31 = 5^2 - 5\cdot(-2) - (-2)^2 = f(5, -2)$　　$41 = 6^2 - 6\cdot(-1) - (-1)^2 = f(6, -1)$
$59 = 7^2 - 7\cdot(-2) - (-2)^2 = f(7, -2)$　　$61 = 7^2 - 7\cdot(-3) - (-3)^2 = f(7, -3)$
$71 = 9^2 - 9\cdot 1 - 1^2 = f(9, 1)$　　$79 = 8^2 - 8\cdot(-3) - 3^2 = f(8, -3)$
$89 = 10^2 - 10\cdot 1 - 1^2 = f(10, 1)$

$\mathbf{D = 12}$ の場合

p.56 の表から $h(12) = 1$, $h^+(12) = 2$ であり, 簡約 2 次形式は

$$f_1(x, y) = 2x^2 - 2xy - y^2, \qquad f_2(x, y) = x^2 - 2xy - 2y^2$$

である. 奇素数 p が判別式 12 をもつ 2 次形式で表示されるための必要十分条件は

$$m^2 \equiv 12 \pmod{4p}, \qquad 0 \leq m < 2p$$

となる m が存在することである. このとき m は偶数で, $m = 2m_0$ とおけば m_0 は

$$m_0{}^2 \equiv 3 \pmod{p}, \qquad 0 \leq m_0 < p$$

を満たす. 逆に上式を満たす m_0 が存在すれば $m = 2m_0$ は

$$m^2 \equiv 12 \pmod{4p}, \qquad 0 \leq m < 2p$$

を満たす. 以上から判別式 12 をもつ 2 次形式で表示される奇素数 p は

$$x^2 \equiv 3 \pmod{p}$$

が解をもつもの, すなわち $p = 3$ または $p \equiv 1, 11 \pmod{12}$ を満たすものである. これらのうち 100 以下のものは

$$3,\ 11,\ 13,\ 23,\ 37,\ 47,\ 59,\ 61,\ 71,\ 73,\ 83,\ 97$$

である. これらが f_1, f_2 のどちらで表示されるかは次のようにして判定できる.

$f_1(x, y) = 2x^2 - 2xy - y^2 = p$ とすると $4x^2 - 4xy - 2y^2 = 2p$ となるから $(2x-y)^2 - 3y^2 = 2p$ である. 従って $(2x - y)^2 \equiv 2p \pmod{3}$ となることから $p = 3$ または $\left(\dfrac{2p}{3}\right) = 1$ が成り立つ. $\left(\dfrac{2p}{3}\right) = 1$ において $\left(\dfrac{2}{3}\right) = -1$ であることより $\left(\dfrac{p}{3}\right) = -1$ である. 以上から $p = 3$ または $p \equiv 2 \pmod{3}$ である.

$f_2(x, y) = x^2 - 2xy - 2y^2 = p$ とする. 3 は f_2 によって表示されない (計算略). 従って $p \neq 3$ である. $(x - y)^2 - 3y^2 = p$ となるから $(x - y)^2 \equiv p \pmod{3}$ が成り立つ. これより $p \equiv 1 \pmod{3}$ が得られる.

上にあげた 100 以下の素数を $f_1(x, y)$ または $f_2(x, y)$ で表示すると次のようになる.

$f_1(x, y) = 2x^2 - 2xy - y^2$

$3 = 2 \cdot 2^2 - 2 \cdot 2 \cdot 1 - 1^2 = f_1(2, 1)$

$11 = 2 \cdot 2^2 - 2 \cdot 2 \cdot (-1) - (-1)^2 = f_1(2, -1)$

$23 = 2 \cdot 3^2 - 2 \cdot 3 \cdot (-1) - (-1)^2 = f_1(3, -1)$

$47 = 2 \cdot 4^2 - 2 \cdot 4 \cdot (-3) - (-3)^2 = f_1(4, -3)$

$59 = 2 \cdot 5^2 - 2 \cdot 5 \cdot (-1) - (-1)^2 = f_1(5, -1)$

$71 = 2 \cdot 5^2 - 2 \cdot 5 \cdot (-3) - (-3)^2 = f_1(5, -3)$

$83 = 2 \cdot 7^2 - 2 \cdot 7 \cdot 1 - 1^2 = f_1(7, 1)$

$f_2(x, y) = x^2 - 2xy - 2y^2$

$13 = 5^2 - 2 \cdot 5 \cdot 1 - 2 \cdot 1^2 = f_2(5, 1)$

$37 = 5^2 - 2 \cdot 5 \cdot (-3) - 2(-3)^2 = f_2(5, -3)$

$61 = 7^2 - 2 \cdot 7 \cdot (-1) - 2(-1)^2 = f_2(7, -1)$

$73 = 7^2 - 2 \cdot 7 \cdot (-3) - 2(-3)^2 = f_2(7, -3)$

$97 = 9^2 - 2 \cdot 9 \cdot (-1) - 2(-1)^2 = f_2(9, -1)$

D = 20 の場合

p.56 の表から $h(20) = h^+(20) = 2$ であり, 簡約 2 次形式は

$$f_1(x,y) = 2x^2 - 2xy - 2y^2, \qquad f_2(x,y) = x^2 - 4xy - y^2$$

である. 奇素数 p が 判別式 20 をもつ 2 次形式で表示される必要十分条件は

$$m^2 \equiv 20 \pmod{4p}, \qquad 0 \leq m < 2p$$

を満たす m が存在することである. このとき m は偶数であるから $m = 2m_0$ とおけば

$${m_0}^2 \equiv 5 \pmod{p}, \qquad 0 \leq m < p$$

が成り立つ. 逆に上式を満たす m_0 が存在すれば $m = 2m_0$ は

$$m^2 \equiv 20 \pmod{4p}, \qquad 0 \leq m < 2p$$

を満たす. 以上から判別式 20 をもつ 2 次形式で表示される奇素数 p は

$$x^2 \equiv 5 \pmod{p}$$

が解をもつもの, すなわち

$$p = 5 \quad \text{または} \quad p \equiv 1, 4 \pmod{5}$$

を満たすものとなる. このような素数で 100 以下のものは

$$5,\ 11,\ 19,\ 29,\ 31,\ 41,\ 59,\ 61,\ 71,\ 79,\ 89$$

である. ここで $f_1(x,y) = 2x^2 - 2xy - 2y^2$ は奇素数を表示することができないので, 上の条件を満たす奇素数はすべて $f_2(x,y) = x^2 - 4xy - y^2$ で表示される.

上にあげた 100 以下の素数を $f_2(x,y)$ で表示すると次のようになる.

$5 = 9^2 - 4\cdot 9\cdot 2 - 2^2 = f_2(9,2)$
$11 = 6^2 - 4\cdot 6\cdot 1 - 1^2 = f_2(6,1)$
$19 = 2^2 - 4\cdot 2\cdot(-3) - (-3)^2 = f_2(2,-3)$
$29 = 3^2 - 4\cdot 3\cdot(-2) - (-2)^2 = f_2(3,-2)$
$31 = 4^2 - 4\cdot 4\cdot(-1) - (-1)^2 = f_2(4,-1)$
$41 = 3^2 - 4\cdot 3\cdot(-4) - (-4)^2 = f_2(3,-4)$
$59 = 6^2 - 4\cdot 6\cdot(-1) - (-1)^2 = f_2(6,-1)$
$61 = 5^2 - 4\cdot 5\cdot(-2) - (-2)^2 = f_2(5,-2)$
$71 = 4^2 - 4\cdot 4\cdot(-5) - (-5)^2 = f_2(4,-5)$
$79 = 4^2 - 4\cdot 4\cdot(-7) - (-7)^2 = f_2(4,-7)$
$89 = 5^2 - 4\cdot 5\cdot(-4) - (-4)^2 = f_2(5,-4)$

References

[1] 弥永昌吉・弥永健一, 代数学, 岩波 1976.

[2] 河田敬義, 数論, 岩波, 1992.

[3] 高木貞治, 初等整数論講義 第 2 版, 共立, 1971.

[4] 永尾 汎, 代数学, 朝倉 1983.

[5] H. M.Stark, (芹沢正三, 安藤四郎 訳), 初等整数論, 現代数学社, 2000.

[6] W. J. LeVeque, Fundamentals of Number Theory, Dover, 1996.