研究報告

実 2 次体の caliber の研究

学習院大学理学部　中　島　匠　一
学習院大学理学部　中　野　　伸

1　実２次体と、その整数環

有理数体と実数体を、それぞれ、記号 $\mathbf{Q}, \mathbf{R}$ で表すことにする。体 K であって、$\mathbf{Q}$ の 2 次拡大になっている（つまり、$K \supset \mathbf{Q}$ かつ $[K : \mathbf{Q}] = 2$ である）ものを「2 次体」と呼ぶ。さらに、2 次体 K が $\mathbf{R}$ に埋め込まれる（つまり、準同型写像 $K \to \mathbf{R}$ が存在する）とき、K は「実 2 次体」と呼ばれる。この記事全体を通して、K は実 2 次体を表すものとする。

2 次の多項式に関する簡単な考察によって、ある square-free な自然数 $D_0 \neq 1$ があって、

$$K = \mathbf{Q}(\sqrt{D_0}) = \{u + v\sqrt{D_0} \mid u, v \in \mathbf{Q}\}$$

と表されることがわかる。（注：整数が square-free であるとは、「すべての素数 p についてその整数が p^2 で割り切れない」こと。）

有理数の中には整数が含まれていて、この「整数」の研究は、古くから数学の重要なテーマであり続けてきた。（「整数は有理数（の特殊なもの）である」という事実は、代数学では、「有理数体は整数環を含む」と表現される。）この類似として、実 2 次体 K の中にも「代数的整数」という概念を考えることができる。その定義を述べると、

K の元 α が代数的整数であるとは、ある整数 b, c で、等式
$\alpha^2 + b\alpha + c = 0$ をみたすものが存在する

となる。K に属する代数的整数全体の集合を $\mathcal{O}_K$ で表すと、$\mathcal{O}_K$ は K の部分環をなす（$\mathcal{O}_K$ は「K の整数環」と呼ばれる）。さらに、$\mathcal{O}_K$ は

$$\mathcal{O}_K = \{s + t\,\omega_K \mid s, t \text{ は整数 }\}$$

と表されることが知られている。ただし、ここで ω_K は、

$$\omega_K = \begin{cases} \dfrac{1+\sqrt{D_0}}{2}, & (D_0 \equiv 1 \pmod 4 \text{ のとき}) \\ \sqrt{D_0}, & (D_0 \not\equiv 1 \pmod 4 \text{ のとき}) \end{cases}$$

で与えられる。（参考文献の [T] 第 5 章参照。）

2 次体の整数環 $\mathcal{O}_K$ は、整数に関する多くの問題に応用されて、大きな成果を挙げている。たとえば、自然数 D_0 に対して、等式 $x^2 - D_0\,y^2 = 1$ をみ

たす整数 x, y を求める問題は「ペル方程式」と呼ばれているが、この方程式を解くためには

$$x^2 - D_0\, y^2 = (x + y\sqrt{D_0})(x - y\sqrt{D_0})$$

と因数分解して、右辺に現れる数を「2 次体の整数」として考察することが有効である。(ペル方程式については、[T] の 48 節を参照。)

2 次体の整数環 $\mathcal{O}_K$ の元は（通常の）整数の類似と考えることができるが、1 つ大きな違いがある。それは、$\mathcal{O}_K$ においては「素因数分解の一意性」が必ずしも成り立たないことである。通常の整数に関する「素因数分解の一意性」は「数論の基本定理」と呼ばれるくらい重要な性質であるので、これが成り立たないのは大きな困難を引き起こす。その困難に対処する方法として、「$\mathcal{O}_K$ のイデアル」の考察が進められ、「2 次体の類数」が問題の解決に大きな役割を果たすことが示された。我々のテーマである caliber は、類数と深く関係しているので、次節で両者の関係を説明する。

2　実２次体の類数と caliber

整数環 $\mathcal{O}_K$ のイデアルとは、$\mathcal{O}_K$ の空でない部分集合 A で、2 つの条件

(I) $\alpha, \beta \in A \quad \Longrightarrow \quad \alpha + \beta \in A$

(II) $\alpha \in A$ かつ $\xi \in \mathcal{O}_K \quad \Longrightarrow \quad \xi\alpha \in A$

をみたすものをいう。(0 だけからなる集合 $\{0\}$ はイデアルとなるが、これはちょっと特別で「例外」として扱われることが多い。) $\mathcal{O}_K$ の元 α_0 があるとき、集合

$$\{\xi\alpha_0 \mid \xi \in \mathcal{O}_K\}$$

が $\mathcal{O}_K$ のイデアルとなることが容易に確かめられる。このイデアルを「α_0 の生成する（$\mathcal{O}_K$ の）単項イデアル」と呼び、簡単に、(α_0) という記号で表す。

$\mathcal{O}_K$ のイデアルがすべて単項イデアルであるなら（つまり、$\mathcal{O}_K$ の任意のイデアル A に対して $A = (\alpha_0)$ となる α_0 があるなら）$\mathcal{O}_K$ で素因数分解の一意性が成り立つことがわかっているが、同時に、一般の K では、単項イデアルでないイデアルが存在することもわかっている。

2 次体において、「イデアル全体の集合」と「単項イデアル全体の集合」のズレを表すものとして、「イデアル類群」と、その位数である「類数」が重要となる。類数を定義するために、まず、「イデアルの同値」という概念を導入する。$\mathcal{O}_K$ のイデアル A, B があるとき、「A と B が同値」であるとは、

$$\beta\, A = \alpha\, B, \quad (\alpha \neq 0, \beta \neq 0)$$

をみたす $\alpha, \beta \in \mathcal{O}_K$ が存在すること、と定義する。このとき、

$$C_K = (\mathcal{O}_K \text{ の イデアル})/(\text{単項イデアルと同値な } \mathcal{O}_K \text{ の イデアル})$$

とおく（ただし、C_K の定義では、イデアルとしては $\{0\}$ 以外のものだけを考える）。このとき、C_K は「イデアルの積」という演算に関して群をなすことが知られていて、C_K は「$\mathcal{O}_K$ のイデアル類群」と呼ばれる。さらに、C_K は有限集合であることが示せるので、C_K の位数（＝元の個数）は有限である。この「C_K の位数」を「K の類数」と呼び、h_K と表す。類数 h_K は 2 次体 K の性質を良く表している量であり、整数論の重要な研究対象となっている（たとえば、$h_K = 1$ であることが、$\mathcal{O}_K$ で素因数分解の一意性が成り立つことと同値）。

実 2 次体でなく虚 2 次体の場合（上記の記号で $D_0 < 0$ となる場合）には類数を表す良い「公式」が知られているが、実 2 次体について h_K を直接表示する有効な公式はない。（注：その原因は、虚 2 次体の場合と違って実 2 次体の場合には「単数」が無限個存在することにあるが、詳細の説明は省略する。）その代わり、実 2 次体についても、個々の K について h_K を計算する方法が知られていて、そこに我々のテーマである caliber が登場する。これから、少し準備をしたあとで、caliber の定義を与えよう。

まず、「K の判別式」と呼ばれる自然数 D が

$$D = \begin{cases} D_0, & (D_0 \equiv 1 \pmod 4 \text{ のとき}) \\ 4D_0, & (D_0 \not\equiv 1 \pmod 4 \text{ のとき}) \end{cases}$$

と定められる（D_0 は上記の通り）。また、整数係数の 2 次多項式で判別式が D であるものの根を「判別式 D の 2 次無理数」と呼ぶ。言い換えれば、実数 ρ が「判別式 D の 2 次無理数」であるとは、$x = \rho$ が

$$ax^2 + bx + c = 0 \quad (a, b, c \text{ は整数で } b^2 - 4ac = D)$$

をみたすことである。（2 次方程式の解の公式により、これは ρ が

$$\rho = \frac{-b \pm \sqrt{D}}{2a} \quad (a, b, c \text{ は整数で } b^2 - 4ac = D)$$

と表される、と言い換えてもよい。）

以下、ρ は「判別式 D の 2 次無理数」を表すこととする。判別式 D の 2 次無理数は無限個あることがすぐにわかるが、その中で、reduced と呼ばれるものが重要である。定義を述べると、ρ が reduced であるとは、

$$\rho > 1 \quad \text{かつ} \quad -1 < \rho' < 0$$

が成り立つことである。ここで、ρ' は ρ の（K の元としての）共役を表していて、記号で書けば

$$\rho = u + v\sqrt{D_0} \quad (u, v \text{ は有理数}) \quad \text{のとき} \quad \rho' = u - v\sqrt{D_0}$$

となる。

判別式 D の 2 次無理数 ρ で reduced であるもの全体の集合を R_K と書くことにする。すると、2 次体論の基本的な結果として「R_K は有限集合である」（しかも、R_K の求め方もわかる）ということが知られている（[T] 第 3 章参照）。さらに、そのことから上記の C_K が有限集合であることが導かれる（[T] 第 5 章参照）。R_K は有限集合であるから元の個数を数えることができるが、その個数が「K の calber」と呼ばれていて、記号で κ と表される（$\kappa = |R_K|$；この用語は、[L] において定義された）。（注：本来は κ_K と書くべきかもしれないが、見にくいので単に κ と書くことにする。）この κ は類数 h_K と関連はしているが、h_K だけでは定まらない数である（実際、h_K の値は同じだが κ の値は異なっている、という 2 次体はいくらでも存在している）。

実 2 次体について、caliber κ と類数 h_K の関係を述べておこう。一般に、実数について「連分数展開」という操作が考えられる（[T] 第 2 章参照）のだが、reduced な ρ を連分数展開したときの終項も reduced であることが知られている（[T] 第 3 章参照）。言い換えれば、R_K の元を連分数展開していけば、すべての終項が再び R_K の元となる。すると、R_K は有限集合であるから、R_K の元は「連分数展開でつながっている」という関係によっていくつかのグループに分かれる（それぞれのグループは「サイクル」と呼ばれる）。このとき

$$(R_K \text{ に含まれるサイクルの総数}) = h_K$$

という関係が成り立っている（[T] 第 5 章参照）。個々のサイクルをなす元の個数が変動するので、h_K が同じでも $\kappa = |R_K|$ は同じではない、という現象が起きるのである。

3　研究の成果と課題

実 2 次体 K の類数 h_K については、古くから多くの研究がなされている。しかし、前節で定義を与えた caliber κ は、実 2 次体 K の性質を表す重要な量だと考えられるのに、残念ながら、これまであまり深く研究されたとは言えない。おこなわれているのは、κ が 1 や 2 に等しくなる K の決定や、（ガウスの種の理論が応用できる）κ のパリティー（＝偶奇性）に関する結果などに限られている。最近 [KM] においてパリティーの研究の次の段階として「κ を 4 で割った余り」について（部分的に）成果が得られたが、一般の自然数 m について「κ を m で割った余り」には手が届いていないようである。

我々の研究では、caliber や集合 R_K 自体の研究を進展させることを目的として、まず計算機実験を行うこととそれをもとに caliber やサイクルの特徴的な性質の発見を目的とした。具体的には、

判別式 D に対して、「R_K とそのサイクル分解」を求めるプログラム

を作成した。(計算のためのツールは、本学でライセンスを購入している数式処理ソフト Maple を利用した。) そして、このプログラムをもとに、多くの D の値について、κ や R_K のサイクルの数値データを集めた。さらに、得られたデータについて

(1) 多くの自然数 m について、 κ を m で割った余り

(2) R_K の中のサイクルの長さの分布

(3) 同じサイクルに属する ρ の特徴

などについて「観察」をおこない、顕著な法則がないかを考察した。

上記のような研究の結果、$h_K = 1$ の場合（このとき、R_K はただ 1 つのサイクルからなる）にはサイクルに表れる ρ の順番にある対称性があることがわかったが、それが $h_K \geq 2$ の場合にどう一般化できるかについては、まだ見通しが立っていない。また、上記の (1)(2) については、データから何らかの傾向を見出すことに成功していない。

このように、数値データから「法則の予測」をおこなうのが困難であることが、これまで caliber の研究が進展しなかった原因なのかもしれない、と感じさせられる。ただ、これまでは得られたデータを「目視」して何らかの傾向を読み取ろうとしていたが、そのような人力に依存した研究では不十分だった可能性はある。今後は、手持ちのデータにきちんとした統計処理を行い、主観による定性的判断ではなく正確な定量的考察を進める必要があるかもしれない。今回のプロジェクトによってデータを大量に得る環境は整ったので、データの処理について有効な手法を見つけていくのが将来の課題として残っている。

4　参考文献

[KM] M.Kaneko, K.Mori, Congruences modulo 4 of calibers of real quadratic fields, Ann. Sci. Math. Québec, 35(2011),185-195.

[L] G.Lachaud, On real quadratic fields, Bull.Amer.Math.Soc. 17(1987),307-311.

[T] 高木貞治「初等整数論講義（第 2 版）」、共立出版、1971 年。