類数が 3 で割れる二次体のある無限族の存在について

伊東杏希子（神奈川大学）

本稿では, 判別式の比が $m_1 : m_2$ となる二次体のペア $(\mathbb{Q}(\sqrt{m_1 d}), \mathbb{Q}(\sqrt{m_2 d}))$ のうち, イデアル類群の位数がともに 3 で割れるものについて得られた結果を述べる.

1　定義

本稿で用いる用語の定義を述べる.

定義 1. d を平方数でない整数とする. 有理数体 $\mathbb{Q}$ と $\sqrt{d}$ を含む最小の体を $\mathbb{Q}(\sqrt{d})$ と表し, **「二次体」**と呼ぶ.

二次体 $\mathbb{Q}(\sqrt{d})$ は, 数の集合として

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a,\ b \in \mathbb{Q}\}$$

と書ける. 二次体は実数体 $\mathbb{R}$ に含まれるかどうかで, 大きく性質が異なる.

定義 2. $d > 0$ ならば, $\mathbb{Q}(\sqrt{d})$ を**「実二次体」**と呼び, $d < 0$ ならば, $\mathbb{Q}(\sqrt{d})$ を**「虚二次体」**と呼ぶ.

次に, ノルム・トレース・整数環・分数イデアルの定義を述べる. これらをもとに, 本稿の重要なキーワードである「イデアル類群」と「類数」の定義を述べたい. 以降では, k を二次体とする.

定義 3. 二次体 $k = \mathbb{Q}(\sqrt{d})$ の元 $\alpha = a + b\sqrt{d}$ に対し, $N(\alpha) = \alpha\alpha'$ を α の**ノルム**と呼び, $T(\alpha) = \alpha + \alpha'$ を α の**トレース** と呼ぶ.

ここで, α' は α の共役 $a - b\sqrt{d}$ を表すものとする.

定義 4. 集合

$$\mathcal{O}_k := \{\alpha \in k \mid N(\alpha) \in \mathbb{Z} \text{ かつ } T(\alpha) \in \mathbb{Z}\}$$

を**「k の整数環」**と呼ぶ.

定義 5. k の整数環 $\mathcal{O}_k$ の (0) と異なるイデアル I と k の 0 ではない元 β に対し, 集合

$$\beta I := \{\beta\gamma \mid \gamma \in I\}$$

を**「k の分数イデアル」**と呼ぶ.

k の分数イデアルの全体を $\mathcal{I}_k$ と書くことにする. $\mathcal{I}_k$ はイデアルの乗法に関してアーベル群をなす. k の 0 ではない元 δ から生成される分数単項イデアル $(\delta) := \delta\mathcal{O}_k$ の全体を $\mathcal{P}_k$ と書くことにする. $\mathcal{P}_k$ は $\mathcal{I}_k$ の部分群になる.

定義 6. 剰余群 $\mathcal{I}_k/\mathcal{P}_k$ を「k **のイデアル類群**」といい, Cl_k と書く.

k のイデアル類群は有限アーベルになることが知られている. Cl_k の位数を「k **の類数**」といい, $h(k)$ と書く. 定義から, $\mathcal{O}_k$ が単項イデアル整域になる時, k の類数は 1 となることが従う. 類数は, 整数環 $\mathcal{O}_k$ が単項イデアル整域からどのくらい離れているのかを測る指標であると言える.

2 二次体の類数の可除性

二次体 $\mathbb{Q}(\sqrt{d})$ の類数を計算するアルゴリズムは知られていて, d の値が小さい場合には計算機で類数を計算できる. しかし, 計算機で扱える d の値の範囲には限度がある. そこで, d の値が大きい場合に二次体 $\mathbb{Q}(\sqrt{d})$ の類数を調べる方法が研究されるようになった. このテーマにおけるアプローチの一つとして, 類数が与えられた自然数で割れるかどうかを調べるという研究分野 (類数の可除性) がある. 本稿では, 類数が 3 で割れる二次体を扱う.

二次体の類数について次のことが知られている.

定理 7. 与えられた自然数 n に対して, 類数が n で割れる実二次体, 虚二次体はそれぞれ無限に存在する.

類数が n で割れる二次体の無限族の具体的な構成により, この定理は示せる. 虚二次体の場合には T. Nagell[4], N. C. Ankeny and S. Chowla[1] など, 実二次体の場合には Y. Yamamoto[6], P. J. Weinberger[5] などによる結果が知られている.

3 先行研究

定理 7 をさらに進展させた研究は数多くある. 特に $n = 3$ の場合, 即ち, 類数が 3 で割れる二次体の場合に関する研究は盛んになされている. 2002 年, 小松亨氏は次の結果を示した.

定理 8 (小松, [3])**.** m を square-free な整数とする. この時, square-free な整数 d のうち, 以下の条件を満たすものが無限に存在する:
(i) 二次体 $\mathbb{Q}(\sqrt{d})$ の類数は 3 で割れる,
(ii) 二次体 $\mathbb{Q}(\sqrt{md})$ の類数は 3 で割れる.

与えられた数で類数が割れる二次体の無限族をペアで構成していることに特徴がある. 定理 8 の証明中に, 所要の条件を満たす正の整数 d, 負の整数 d はそれぞれ無限に存在することが書かれているので, 条件を満たす実二次体同士のペアの無限族, 虚二次体同士のペアの無限族, 実二次体と虚二次体のペアの無限族のそれぞれの存在が示せている.

4　主結果とその背景

定理 7 をさらに進展させた研究テーマの一つに, 「与えられた数で類数が割れる虚二次体, 実二次体はどのくらいの割合で存在するか」を調べるという研究がある. この割合に関する研究として, 特に, Cohen-Lenstra Heuristics [2] と呼ばれる予想が知られている.

この予想によると, 与えられた奇素数 l で類数が割れる虚二次体の割合は

$$1-\prod_{i=1}^{\infty}\left(1-\frac{1}{l^i}\right),$$

与えられた奇素数 l で類数が割れる実二次体の割合は

$$1-\prod_{i=2}^{\infty}\left(1-\frac{1}{l^i}\right)$$

と期待されている.

この予想から, 類数が 3 で割れる虚二次体は約 44%, 類数が 3 で割れる実二次体は約 16% 存在することが期待される. これが正しいならば, 条件を多くして対象となる二次体を減らしても類数が 3 で割れるものは無限に存在する可能性が考えられる. 小松亨氏の結果をこのことに関連させて捉えることもできる. 実際, 定理 8 では, 類数が 3 で割れる二次体をペアで構成するという, 制約の多い中での無限族の構成に成功している. この結果に興味を持ち, 条件をさらに増やしても類数が 3 で割れる二次体のペアは無限に構成できるかということを考え, 次を示した.

主結果 9. m_1, m_2 を相異なる square-free な整数でかつ, $12\nmid m_1m_2$ を満たすものとする (ただし, 1 を含む). S_+, S_-, S_0 を互いに共通部分を持たない素数の有限集合でかつ, 2, 3 と m_1m_2 の素因数を含まないものとする. この時, square-free な整数 d のうち, 以下の条件を満たすものが無限に存在する:

(i) 二次体 $\mathbb{Q}(\sqrt{m_1d})$ の類数は 3 で割れる,
(ii) 二次体 $\mathbb{Q}(\sqrt{m_2d})$ の類数は 3 で割れる,
(iii) $\gcd(m_1m_2,d)=1$,
(iv) 任意の $\eta\in S_+$ に対して, $\left(\dfrac{d}{\eta}\right)=1$,
(v) 任意の $\eta\in S_-$ に対して, $\left(\dfrac{d}{\eta}\right)=-1$,
(vi) 任意の $\eta\in S_0$ に対して, $\left(\dfrac{d}{\eta}\right)=0$.

ここで, $\left(\frac{\cdot}{\cdot}\right)$ は Legendre 記号を表す. 定義は以下の通りである: 奇素数 p で割り切れない整数 a に対し, 合同式 $x^2\equiv a \bmod p$ が整数解 x を持つ時 $\left(\dfrac{a}{p}\right)=1$ と書き, 合同式 $x^2\equiv a \bmod p$ が整数解 x を持たない時 $\left(\dfrac{a}{p}\right)=-1$ と書く. 整数 a が奇素数 p で割り切れる時 $\left(\dfrac{a}{p}\right)=0$ と書く.

例 10. $m_1 = 7$, $m_2 = 11$, $S_+ = \{5\}$, $S_0 = \{503\}$ とすると, 主結果 g より

$$\sharp\left\{ d:\ \text{square-free な整数} \;\middle|\; \begin{array}{c} 3 \mid h(\mathbb{Q}(\sqrt{7d})),\ 3 \mid h(\mathbb{Q}(\sqrt{11d})), \\ \gcd(77, d) = 1, \\ \left(\frac{d}{5}\right) = 1,\ \left(\frac{d}{503}\right) = 0 \end{array} \right\}$$

$$= \sharp\left\{ d:\ \text{square-free な整数} \;\middle|\; \begin{array}{c} 3 \mid h(\mathbb{Q}(\sqrt{7d})),\ 3 \mid h(\mathbb{Q}(\sqrt{11d})), \\ \gcd(77, d) = 1, \\ d \equiv 1006,\ 1509 \bmod 2515 \end{array} \right\}$$

$$= \infty$$

となる. ここで, $h(\mathbb{Q}(\sqrt{d}))$ は二次体 $\mathbb{Q}(\sqrt{d})$ の類数を表す.

例 10 では $d \equiv 1006,\ 1509 \bmod 2515$ とあるので, 合同条件を満たす整数自体が $5,000$ 個につき 3, 4 個しか存在しない. その中で, 類数の可除性に関して所要の条件を満たすものが無限に存在することを示せた. S_+, S_-, S_0 としてより大きな素数を含む集合を取ることにより, 合同条件を満たす整数自体が非常に少ない中でも条件を満たすものが無限に存在することを確認できる.

参考文献

[1] N. C. Ankeny and S. Chowla, On the divisibility of the class number of quadratic fields, Pacific J. Math. **5** (1955), 321–324.

[2] H. Cohen and H. W. Lenstra, Heuristics on class groups of number fields, Number Theory, Springer Lecture Notes in Math. **1068** (1984), 33–62.

[3] T. Komatsu, An infinite family of pairs of quadratic fields $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{mD})$ whose class numbers are both divisible by 3, Acta Arith., **104** (2002), 129–136.

[4] T. Nagell, Über die Klassenzahl imaginär-quadratischer Zahlkörper, Abh. Math. Sem. Univ. Hamburg **1** (1922), 140–150.

[5] P. J. Weinberger, Real quadratic fields with class numbers divisible by n, J. Number Theory **5** (1973), 237–241.

[6] Y. Yamamoto, On unramified Galois extentions of quadratic number fields, Osaka J. Math. **7** (1970), 57–76.