有理数体の円分的 $\mathbb{Z}_3$ 拡大における Weber の類数問題

森澤貴之*

早稲田大学基幹理工学研究科数学応用数理専攻修士課程２年

Acknowledgements

第 7 回城崎新人セミナーに参加させていただき, ありがとうございました. 全国の同世代の方々と会うことができ, また, 講演の機会までいただきまして, 運営委員の皆様にはこの場を借りて, 御礼申し上げます.

1　イデアル類群と Gauss 予想

有理数体 $\mathbb{Q}$ の代数的閉包 $\bar{\mathbb{Q}}$ の部分体を“代数体”と呼ぶ. 代数体 K は $\mathbb{Q}$ 上の線形空間と見なすことができ, その次元が有限であるとき特に, “有限次代数体”と呼ぶ. （今後, 有限次代数体のことを代数体ということとする.）

例 **1.1** (実二次体)**.** 平方因子のない自然数 m に対し,

$$\mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} \mid a, b \text{ は有理数 }\}$$

と置くと, $\mathbb{Q}(\sqrt{m})$ は有限次代数体であり, 特に“実二次体”と呼ぶ.

代数体 K の元 α が, ある整数係数モニック多項式の根となるとき, α を “K の整数”といい, K の整数全体を $\mathcal{O}_K$ と書くことにする. この $\mathcal{O}_K$ は K の部分環となっており, “K の整数環”と呼ぶ.
ここで, 代数的整数論における重要な対象の一つである, イデアル類群を定義する. 代数体 K は $\mathcal{O}_K$ 加群と見ることができ, その $\mathcal{O}_K$ 部分加群として有限生成な $\mathcal{O}_K$ 加群を“分数イデアル”といい, その全体を I_K で表す. イデアルの積と同様にして分数イデアルの積を定義することで, I_K はアーベル群となり, “K のイデアル群”と呼ぶ. また, 分数イデアルの中で, 1 元生成なものを“単項分数イデアル”といい, その全体を P_K で表す. この P_K はイデアル群 I_K の部分群を成し, “単項イデアル群”と呼ぶ.

定義 **1.2** (イデアル類群)**.** 代数体 K に対し,

$$Cl_K = I_K/P_K$$

とおき, “K のイデアル類群”と呼ぶ.

次の定理は代数的整数論における最も重要な定理の一つである.

定理 **1.3.** 代数体 K に対し, イデアル類群 Cl_K は有限群である.

イデアル類群が有限群であることから, その位数を考えることができる. イデアル類群 Cl_K の位数を h_K と書き, “K の類数”と呼ぶ. 類数に関する予想として, 次のような問題が考えられている.

* da-vinci-0415@moegi.waseda.jp

予想 1.4 (Gauss 予想)**.** 類数が 1 となる実二次体は無限に存在するか？

実は, この問題は, “実二次体”という条件を“(有限次) 代数体”に書き換えても未だに解かれていない問題である. すなわち:

予想 1.5. 類数が 1 となる代数体は無限に存在するか？

この未解決問題に対し, 私は岩澤理論に現れる“円分的 $\mathbb{Z}_p$ 拡大に注目することで, 肯定的な解決を目指している.

2 有理数体の円分的 $\mathbb{Z}_p$ 拡大と Weber の類数問題

まずは有理数体 $\mathbb{Q}$ の円分的 $\mathbb{Z}_p$ 拡大を定義する. 素数 p を 1 つ固定し, 整数 q を

$$q = \begin{cases} 4, & (p = 2) \\ p, & (p \geq 3) \end{cases}$$

とおく. ここで, μ_m と書いて 1 の m 乗根全体のなす群を表すものとし, 有理数体に μ_m を添加した体 $\mathbb{Q}(\mu_m)$ を円分体（特に, 円の m 分体）と呼ぶ. この円分体は有理数体上のガロア拡大となっており, そのガロア群に関して,

$$\mathrm{Gal}(\mathbb{Q}(\mu_m) \cong (\mathbb{Z}/m\mathbb{Z})^\times$$

という同型が知られている. 特に $m = qp^n$ の場合には,

$$\mathrm{Gal}(\mathbb{Q}(\mu_{qp^n}) \cong (\mathbb{Z}/q\mathbb{Z})^\times \times \mathbb{Z}/p^n\mathbb{Z}$$

となる. この同型とガロア理論から, $\mathbb{Q}(\mu_{qp^n})$ の実部分体で, $\mathbb{Q}$ 上のガロア群が $\mathbb{Z}/p^n\mathbb{Z}$ と同型となるものが唯一つ存在することがわかるので, その体を $\mathbb{B}_{p,n}$ と書く. すなわち,

$$\mathbb{Q} \subseteq \mathbb{B}_{p,n} \subseteq \mathbb{Q}(\mu_{qp^n})$$

であって,

$$\mathrm{Gal}(\mathbb{B}_{p,n}/\mathbb{Q}) \cong \mathbb{Z}/p^n\mathbb{Z}$$

を満たす部分体である. この $\mathbb{B}_{p,n}$ に対し, $\mathbb{B}_{p,\infty} = \bigcup_{n\geq 1} \mathbb{B}_{p,n}$ とおくと, そのガロア群は,

$$\mathrm{Gal}(\mathbb{B}_{p,\infty}/\mathbb{Q}) = \varprojlim \mathrm{Gal}(\mathbb{B}_{p,n}/\mathbb{Q}) \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$$

と, p 進整数環 $\mathbb{Z}_p$ と同型となるため, $\mathbb{B}_{p,\infty}/\mathbb{Q}$ を“円分的 $\mathbb{Z}_p$ 拡大”と呼ぶ. 円分的 $\mathbb{Z}_p$ 拡大という拡大は岩澤理論において扱われる最も重要な拡大の 1 つである. この有理数体の円分的 $\mathbb{Z}_p$ 拡大の中間体 $\mathbb{B}_{p,n}$ に対し, その類数を $h_{p,n} = h_{\mathbb{B}_{p,n}}$ とおき, 次のような問題を考える.

予想 2.1 (Weber の類数問題)**.** 任意の自然数 n に対して, $h_{p,n} = 1$ となるか？

この Weber の類数問題に関しては, 例えば, p が 2 の場合には,

$$h_{2,1} = h_{2,2} = h_{2,3} = h_{2,4} = h_{2,5} = 1$$

ということがわかっており, p が 3 の場合には,

$$h_{3,1} = h_{3,2} = h_{3,3} = 1$$

であることが知られている. だが, n が大きくなると, 類数の計算が困難なものとなるため, 次のような問題を考えることにする.

命題 2.2. 素数 ℓ に対し, 任意の自然数 n で, ℓ は $h_{p,n}$ を割り切らないか？

この問題を任意の素数 ℓ に対して肯定的に解決できれば, それは即ち, Weber の類数問題の肯定的解決となるので, この問題へアプローチしていくことにする.

3 先行結果

素数 ℓ が $\mathbb{B}_{p,n}$ の類数 $h_{p,n}$ を割るかどうかという問題に関してはいくつかの結果が知られている.

まず, 素数 p と ℓ が等しい場合には, 岩澤健吉 [8] によって次の結果が証明されている:

定理 3.1 (岩澤)**.** 任意の自然数 n に対して p は $h_{p,n}$ を割らない.

そこで, p と ℓ が異なる場合を考える. 特に, 素数 p が 2 の場合, 即ち, 有理数体の円分的 $\mathbb{Z}_2$ 拡大に関しては, 岡崎氏 [12], 小松氏・福田氏 [2] [3], 堀江氏 [5] [6] [7] などにより, 多くの結果が知られている.

私は p が 3 の場合に注目し, 研究を行った. 今後, p は 3 とし, 簡単のために, $\mathbb{B}_n = \mathbb{B}_{3,n}$, $h_n = h_{3,n}$ とおく. p が 3 の場合に関しては以下のような結果が知られている.

定理 3.2 (堀江)**.** 素数 ℓ が $\ell \not\equiv \pm 1 \pmod 9$ を満たすならば, 任意の自然数 n に対して ℓ は h_n を割らない.

定理 3.3 (M-[10])**.** 素数 ℓ が 10000 より小なる場合, 任意の自然数 n に対して ℓ は h_n を割らない.

4 主結果 (p=3)

これらの先行結果に対し, 私は以下の結果を得た.

定理 4.1. 素数 ℓ を $2, 3$ とは異なるものとし, 整数 s を $\ell^2 - 1$ を素因数分解したときの 3 の個数とし, $c = 2 \cdot 3^{s-1}$, $f = \begin{cases} 1, & (\ell \equiv 1 \bmod 3) \\ 2, & (\ell \equiv -1 \bmod 3) \end{cases}$ とおく. このとき, ℓ が $\ell^f > 2^{c/2} \cdot c!$ を満たすならば, 任意の自然数 n に対して ℓ は h_n を割らない.

ここで, $\ell \equiv 8, 10, 17, 19 \pmod{27}$ を満たす素数 ℓ に注目する. この合同式を満たす ℓ に対しては, $s = 2$ となり, 定理 4.1 の不等式の右辺は

$$2^{c/2} \cdot c! = 2^3 \cdot 6! = 5760$$

となる. この値と定理 3.3 を合わせることで, 以下の系を得る:

系 4.2. 素数 ℓ が $\ell \equiv 8, 10, 17, 19 \pmod{27}$ を満たすならば, 任意の自然数 n に対して ℓ は h_n を割らない.

また, 定理 3.2 と合わせた形で書き換えると, 以下のようになる:

系 4.3. 素数 ℓ が $\ell \not\equiv \pm 1 \pmod{27}$ を満たすならば, 任意の自然数 n に対して ℓ は h_n を割らない.

5 主結果の証明

有理数体の円分的 $\mathbb{Z}_3$ 拡大の中間体 $\mathbb{B}_n$ に対し, その整数環を $\mathcal{O}_n$ と書き, $N = 3^n$, $\zeta_n = \exp(2\pi\sqrt{-1}/3^n)$,

$$\eta_n = \frac{\zeta_{n+1} - \zeta_{n+1}^{-1}}{\zeta_1\zeta_{n+1} - \zeta_1^{-1}\zeta_{n+1}^{-1}}$$

とおく. このとき, η_n は $\mathcal{O}_n^\times$ の元となっている. ガロア群 $\mathrm{Gal}(\mathbb{B}_n/\mathbb{Q})$ は N 次の巡回群であるので, その生成元を σ とする.

定義 5.1 (Mahler 測度)**.** $\mathcal{O}_n \setminus \mathcal{O}_{n-1}$ の元 β に対し,

$$M(\beta) = \prod_{i=0}^{N-1} \max\{1, |\beta^{\sigma^i}|\}$$

とおき, β の“Mahler 測度”と呼ぶ.

ここで, 主結果の証明に用いる重要な補題を紹介する.

補題 5.2 (堀江)**.** 素数 ℓ が h_n/h_{n-1} を割っているとする. このとき, ある $\alpha = \sum_{i=0}^{N-1} a_i\sigma^i$ と $\mathcal{O}_n^\times$ の元 ϵ があって,

$$\eta_n^\alpha = \epsilon^\ell$$

と書ける.

注意 5.3. 堀江氏の論文における補題 ([6] Lemma 2.) では, 一般の素数 p に対して, もっと強い主張となっているが, 簡単のため, このような書き方にした.

5.1 $M(\eta_n)$ の上限

まず,

$$\eta_n = \frac{\sin(2\pi/3^{n+1})}{\sin(2(1+N)\pi/3^{n+1})}$$

であることに注目することで,

$$M(\eta_n) \le \prod_{0<j<2N/3,(j,2)=1} \cot\frac{j\pi}{4N}$$

を得る. ここで, 両辺の対数をとり, 区分級積を行うことで,

$$\frac{\pi}{2N}\log M(\eta_n) \le \frac{\pi}{2N}\sum_{0<j<2N/3,(j,2)=1} \log\cot\frac{j\pi}{4N} \le \int_0^{\pi/6} \log\cot t\ dt$$

となり, Lobachevsky 関数 [4] [9] を用いることで, 以下を得る.

補題 5.4.

$$M(\eta_n) \le \exp(0.53845\cdot N).$$

5.2 $M(\epsilon)$ の下限

Mahler 測度の下限としては, Schinzel [1] [13] による不等式が知られている. その不等式を私の問題に応用すると以下の結果が得られる:

補題 5.5.

$$M(\epsilon) \ge \left(\frac{3^{(N-1)/2N} + \sqrt{3^{(N-1)/N}+4}}{2}\right)^{N/2}.$$

注意 5.6. 特に, $n \ge 4$ の場合には,

$$M(\epsilon) \ge \exp(0.77896\cdot N/2)$$

となる.

5.3 $\sum_i |a_i|$ の上限

Minkowski の格子点定理を用いることで, もし素数 ℓ が $\ell^f > 2^{c/2} \cdot c!$ を満たすならば,

$$\sum_i |a_i| \leq \frac{\ell}{\sqrt{2}}$$

となることがわかる.

5.4 証明

Minkowski の格子点定理を用いるために, 素数 ℓ が $\ell^f > 2^{c/2} \cdot c!$ を満たすとする. ここで, 素数 ℓ が h_n/h_{n-1} を割り切ると仮定する. このとき, $h_0 = h_1 = h_2 = h_3 = 1$ より, $n \geq 4$ と仮定してよい. 堀江の補題から, ある $\alpha = \sum_{i=0}^{N-1} a_i \sigma^i$ と $\mathcal{O}_n^\times$ の元 ϵ があって,

$$\eta_n^\alpha = \epsilon^\ell$$

と書ける. この等式の両辺の Mahler 測度をとってやると, Mahler 測度の性質から,

$$M(\epsilon)^\ell = M(\epsilon^\ell) = M(\eta_n^\alpha) \leq M(\eta_n)^{\sum_i |a_i|}$$

となることがわかる. 5.1,5.2,5.3 から,

$$\begin{aligned} \exp(0.778968 \cdot \ell \cdot N/2) &\leq M(\epsilon)^\ell \\ &\leq M(\eta_n)^{\sum_{i=0}^{2 \cdot 3^{r-1}-1} |a_i|} \\ &\leq \exp(0.538444 \cdot N \cdot \ell/\sqrt{2}). \end{aligned}$$

となる. よって,

$$0.778968 \leq 0.538444 \cdot \sqrt{2} = 0.7614\ldots.$$

となり, 矛盾. 従って, 素数 ℓ が $\ell^f > 2^{c/2} \cdot c!$ を満たすならば, 任意の自然数 n に対して, h_n/h_{n-1} を割り切らないことがわかった. 特に, $h_0 = h_{\mathbb{Q}} = 1$ であることに注目すれば, 任意の自然数 n に対して, h_n を割り切らないことがわかるので, 主結果の証明を得た.

参考文献

[1] G.Everest and T.Ward, *Heights of Polynomials and Entropy in Algebraic Dynamics*, Universitext, Springer-Verlag London, Ltd., London, 1999.

[2] T.Fukuda and K.Komatsu, *Weber's Class Number Problem in the Cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$*, Experiment. Math. **18**-2 (2009), 213-222.

[3] T.Fukuda and K.Komatsu, *Weber's Class Number Problem*, preprint.

[4] I.S.Gradshteyn and I.M.Ryzhik, *Table of Integrals, Series and Products*, Academic Press (1965).

[5] K.Horie, *Ideal Class Groups of Iwasawa-theoritical Abelian Extensions over the Rational Field*, J. London Math. Soc. **66** (2002), 257-275.

[6] K.Horie, *The Ideal Class Group of the Basic $\mathbb{Z}_p$-extension over an Imaginary Quadratic Field*, Tohoku Math. J., **57** (2005), 375-394.

[7] K.Horie, *Certain Primary Components of the Ideal Class Group of the $\mathbb{Z}_p$-Extension over the Rationals*, Tohoku Math. J., **59** (2007), 259-291.

[8] K.Iwasawa, *A Note on Class Numbers of Algebraic Number Fields*, Abh. Math. Sem. Univ. Hamburg **20** (1956), 257-258.

[9] N.I.Lobachevsky, *Complete Works*, I, III, V, Gostekhizdat, Moscow and Leningrad (1946–1951).

[10] T.Morisawa, *A Class Number Problem in the Cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}$*, Tokyo J. Math. **32** (2009), 549-558.

[11] T.Morisawa, *Mahler measure of the Horie unit and Weber's Class Number Problem in the Cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}$*, preprint.

[12] R.Okazaki, *On a Lower Bound for Relative Units, Schinzel's Lower Bound and Weber's Class Number Problem*, preprint.

[13] A.Schinzel, *On the Product of the Conjugates outside the Unit Circle of an Algebraic Integer*, Acta Arith. **24** (1973), 385-399.

[14] L.C.Washington, *The Non-p-part of the Class Number in a Cyclotomic $\mathbb{Z}_p$-extension*, Inv. Math. **49** (1978), 87-97.