指数 3 と 5 のイデアル類群をもつ虚重 2 次体の決定について

小松 亨 (東京理科大学)

概要　2 次体を 2 つ以上合成してできる体を重 2 次体 (multiquadratic field) といい, 実数体に含まれない重 2 次体を虚重 2 次体という. 4 重以上の虚重 2 次体の類数は 偶数であることが知られている. 本講演では, 拡張されたリーマン予想 (ERH) の下で, 指数 3, 5 のイデアル類群をもつ 虚重 2 次体を具体的にすべて決定したので, その内容についてお話させていただく. なお本成果は J. Klueners 氏 (Paderborn 大学) との 共同研究によるものであり, 共著論文は Math. Comp. に掲載予定である.

定義　(1) $\mathbb{Q}$ のガロア拡大 K が $\mathrm{Gal}(K/\mathbb{Q}) \simeq C_2^n$ (C_2 の n コ直積) のとき, Kをn 重 2 次体 (n-quadratic field) という.
(2) 2-quadratic は biquadratic と, 3-quadratic は triquadratic ともいう.
(3) $n \geq 2$ のとき n-quadratic field を重 2 次体 (multiquadratic field) という.
(4) $\mathbb{R}$ に含まれない重 2 次体を虚重 2 次体という.

定義　(1) 代数体 K のイデアル類群を $\mathrm{Cl}(K)$ とかく.
(2) 群 G に対し $\sharp\{g^u \mid g \in G\} = 1$ となる最小整数 $u \geq 1$ を G の指数といい $E(G)$ とかく.
(3) 拡張されたリーマン予想 (Extended Riemann hypothesis) を ERH とかく.

定理 (Klüners-Komatsu, Math. Comp.)
(1) $\mathrm{Cl}(K) \simeq C_3, C_3^2, C_3^3, C_3^4$ となる虚 2 重 2 次体 K がそれぞれ少なくとも $163, 122, 32, 1$ コ存在する.
(2) $\mathrm{Cl}(K) \simeq C_3, C_3^2, C_3^3, C_3^4$ となる虚 3 重 2 次体 K が $\ldots$ $23, 29, 7, 1$ コ存在.
(3) ERH の下, 上記以外で $E(\mathrm{Cl}(K)) = 3$ の虚 $2, 3$ 重 2 次体 K は存在しない.

定理　$E(\mathrm{Cl}(K)) = 5$ も同様. (略)

注意　(Fröhlich, Cont. Math. **24**, 1983)
$n \geq 4$ に対し, 類数が奇数となる虚 n 重 2 次体は存在しない.

注意　(Brown-Parry 1974)
類数 1 の虚 2 重 2 次体をすべて決定.

注意　((内田 1972) 山村 1994)
類数 1 の虚アーベル体をすべて決定.

注意　(Jung-Kwon 1998)
類数 3 の虚 2 重 2 次体をすべて決定.

定理　(Elsenhans-Klüners-Nicolae 2020)
$\mathfrak{K}_u := \{k : 虚 2 次体 \mid E(\mathrm{Cl}(k)) = u\}$,
$\mathfrak{K}'_u := \{k \in \mathfrak{K}_u \mid |D_k| < 3.1 \cdot 10^{20}\}$,
$m_u := \max\{|D_k| \mid k \in \mathfrak{K}_u\}$,
$m'_u := \max\{|D_k| \mid k \in \mathfrak{K}'_u\}$.

u	$\sharp\mathfrak{K}'_u$	m'_u	m_u(ERH 下$_{(\mathrm{BK+BS})}$)
3	17	4027	$< 9.7 \cdot 10^{10}$
4	203	435435	$< 3.4 \cdot 10^{15}$
5	27	37363	$< 2.3 \cdot 10^{20}$
6	432	5761140	$< 2.5 \cdot 10^{25}$
7	33	118843	$< 3.9 \cdot 10^{30}$
8	778	430950520	$< 8.9 \cdot 10^{35}$

定理　(EKN 2020)
ERH の下で, $E(\mathrm{Cl}(K)) \in \{1, 2, 3, 4, 5, 8\}$ となる虚 2 次体 K をすべて決定.

定理 (Fröhlich, Cont. Math. **24**, 1983)
$n \in \mathbb{Z}$ $(n \geq 1)$ に対し
n 重 2 次体 K の狭義類数 $h_+(K)$ が奇数
$\Leftrightarrow$ ある条件を満たす $a, b, c \in \mathbb{Z}$ に対し
$K = \mathbb{Q}(\sqrt{a}), \mathbb{Q}(\sqrt{a}, \sqrt{b}), \mathbb{Q}(\sqrt{a}, \sqrt{b}, \sqrt{c})$.

定義 イデアル類群 $\mathrm{Cl}(K)$ の奇部分を
$\mathrm{Cl}_o(K)$ とかく, つまり $\mathrm{Cl}_o(K)$ は $\mathrm{Cl}(K)$
の奇数位数の類全体からなる部分群.

定理 (Lemmermeyer 1994)
代数体のガロア拡大 K/k で
$\mathrm{Gal}(K/k) \simeq V_4 = C_2^2$ のとき, 次が成立.
$$\mathrm{Cl}_o(K) \simeq \mathrm{Cl}_o(k) \times \prod_{k \subsetneq k' \subsetneq K} \mathrm{Cl}_o(k')/\mathrm{Cl}_o(k).$$

系 重 2 次体 K に含まれる 2 次体全体の
族を $\mathcal{Q}(K)$ とかくとき, 次が成立.
$$\mathrm{Cl}_o(K) \simeq \prod_{k \in \mathcal{Q}(K)} \mathrm{Cl}_o(k).$$

定義 (1) 奇素数 p に対し
$p^* := (-1)^{(p-1)/2} p$.
(2) $P^* := \{8, -4, -8\} \cup \{p^* \mid p$ は奇素数 $\}$,
$P^*_+ := \{p^* \in P^* \mid p^* > 0\}$,
$P^*_- := \{p^* \in P^* \mid p^* < 0\}$.

定義 $E(\mathrm{Cl}(K))$ を $E(K)$ とかく.

定理 (Klüners-Komatsu, Math. Comp.)
$u > 0$ を奇数とする.
虚 n 重 2 次体 K が $E(K) \mid u$ ならば
K は下記 (1),(2),(3) のいずれかの形.
(1) $p^* \in P^*_-$ に対し
$K = \mathbb{Q}(\sqrt{p^*})$ で $E(\mathbb{Q}(\sqrt{p^*})) \mid u$.
(2) $p_1^* \in P^*_-, p_2^* \in P^*$ に対し
$\mathbb{Q}(\sqrt{p_1^*})$ は上記 (1) でかつ
次の (2a) か (2b) をみたす.
(2a) $p_2^* < 0$ で $E(\mathbb{Q}(\sqrt{p_2^*})) \mid u$,
つまり $\mathbb{Q}(\sqrt{p_2^*})$ も上記 (1).
(2b) $p_2^* > 0$ で $E(\mathbb{Q}(\sqrt{p_1^* p_2^*})) \mid 2u$.
(3) $p_1^*, p_2^* \in P^*_-, p_3^* \in P^*$ に対し
$K = \mathbb{Q}(\sqrt{p_1^*}, \sqrt{p_2^*}, \sqrt{p_3^*})$ でかつ
3 つの部分体 $\mathbb{Q}(\sqrt{p_1^*}, \sqrt{p_2^*})$,
$\mathbb{Q}(\sqrt{p_1^*}, \sqrt{p_3^*}), \mathbb{Q}(\sqrt{p_2^*}, \sqrt{p_3^*})$ は上記 (2).

定義 上記定理の (1),(2),(3) の体の族を
それぞれ $\mathcal{K}_1, \mathcal{K}_2, \mathcal{K}_3$ とかく.

系 固定した奇数 u に対し
$\mathcal{K}_2$ が有限族ならば $\mathcal{K}_3$ も有限族.

注意 上記定理の $u = 1$ のときは
内田 (1972) の方法と同じ.

定義 (1) $I_1 := \{p^* \in P^*_-; E(\mathbb{Q}(\sqrt{p^*})) \mid u\}$.
(2) $p^* \in I_1$ に対し
$R_{p^*} := \{q^* \in P^*_+; E(\mathbb{Q}(\sqrt{p^* q^*})) \mid 2u, p \neq q\}$.
(3) $\mathcal{K}_{2\mathrm{a}} := \{\mathbb{Q}(\sqrt{p^*}, \sqrt{q^*}) \mid p^* \neq q^* \in I_1\}$,
$\mathcal{K}_{2\mathrm{b}} := \{\mathbb{Q}(\sqrt{p^*}, \sqrt{q^*}) \mid p^* \in I_1, q^* \in R_{p^*}\}$.

注意 $\mathcal{K}_2 = \mathcal{K}_{2\mathrm{a}} \cup \mathcal{K}_{2\mathrm{b}}$.

定義 $\mathcal{K}_3$ の部分族
$$\mathcal{K}_{3\mathrm{a}} := \{\, \mathbb{Q}(\sqrt{p_1^*}, \sqrt{p_2^*}, \sqrt{p_3^*}) \in \mathcal{K}_3 \mid p_1^*, p_2^*, p_3^* \in P^*_-\},$$
$$\mathcal{K}_{3\mathrm{b}} := \{\, \mathbb{Q}(\sqrt{p_1^*}, \sqrt{p_2^*}, \sqrt{p_3^*}) \in \mathcal{K}_3 \mid p_1^*, p_2^* \in P^*_-, p_3^* \in P^*_+\}.$$

定義 (論文で削ってしまっている.)
$\mathcal{M}_1 := \{K \in \mathcal{K}_1 \mid E(K) \mid u\}$,
$\mathcal{M}_{2\mathrm{a}} := \{K \in \mathcal{K}_{2\mathrm{a}} \mid E(K) \mid u\}$,
$\mathcal{M}_{2\mathrm{b}} := \{K \in \mathcal{K}_{2\mathrm{b}} \mid E(K) \mid u\}$,
$\mathcal{M}_{3\mathrm{a}} := \{K \in \mathcal{K}_{3\mathrm{a}} \mid E(K) \mid u\}$,
$\mathcal{M}_{3\mathrm{b}} := \{K \in \mathcal{K}_{3\mathrm{b}} \mid E(K) \mid u\}$.

注意 $\mathcal{M}_1 = \mathcal{K}_1$.

補題 (Boyd-Kisilevsky 1972)
虚 2 次体 k において,
代数的整数 $\alpha \in k$ ($\alpha \notin \mathbb{Z}$) ならば
$N_{k/\mathbb{Q}}(\alpha) \geq |D_k|/4$ が成立.

定理 (Bach-Sorenson 1996)
2 次体 k (ただし $|D_k| > e^{25} \approx 7.2 \times 10^{10}$)
に対し, ERH の下で, 次の条件 (*) を
みたす k で分解する素数 ℓ が存在する.
(*) $\ell \leq (1.881 \log(|D_k|) + 0.34 \cdot 2 + 5.5)^2$.

注意 (BK+BS) $|D_k|/4 \leq \ell^u \leq (\cdots)^{2u}$.

注意 以下では $u = 3$ のときを説明.

定理 (EKN 2020)
$E(k) = 3$ となる虚 2 次体 k の
判別式 D_k の絶対値 $|D_k|$ の最大値 m_3 は,
条件 $|D_k| < 3.1 \times 10^{20}$ 下では $m_3' = 4027$.
ERH 下 (BK+BS) で, 最大値 $m_3 = 4027$.

定理 (EKN 2020)
ERH の下で, $E(\mathbb{Q}(\sqrt{-d})) \mid 3$ となる
虚 2 次体 $\mathbb{Q}(\sqrt{-d})$ の一覧は下記.

r	d	$\sharp$
0	$1, 2, 3, 7, 11, 19, 43, 67, 163$	9
1	$23, 31, 59, 83, 107, 139, 211, 283,$ $307, 331, 379, 499, 547, 643, 883, 907$	16
2	4027	1

ただし $\mathrm{Cl}(\mathbb{Q}(\sqrt{-d})) \simeq C_3^r$.

補題 ERH の下で, $\sharp\mathcal{M}_{2\mathrm{a}} = 307$.

注意 $\sharp\mathcal{K}_{2\mathrm{a}} = {}_{26}C_2 = 325$.

定理 (EKN 2020)
$E(k) = 6$ となる虚 2 次体 k の
判別式 D_k の絶対値 $|D_k|$ の最大値 m_6 は,
条件 $|D_k| < 3.1 \cdot 10^{20}$ 下で $m_6' = 5761140$.
ERH 下 (BK+BS) で, $m_6 < 2.5 \cdot 10^{25}$.

補題 $p^* \in I_1$ ($|p^*| \leq 4027$), $q^* \in R_{p^*}$
に対し, ERH の下で, $q^* < 5761140/|p^*|$.

証明 (アウトライン)
$k = \mathbb{Q}(\sqrt{p^* q^*})$ に対し $\mathrm{Cl}(k) \simeq C_3^r \times C_2$ で,
2 部分が小さいことをうまく利用すると
ERH 下 (BK+BS) で, $|p^* q^*| \leq 2.4 \times 10^{15}$.
EKN より $|p^* q^*| < 5761140$.

補題 ERH の下で, $\sharp\mathcal{M}_{2\mathrm{b}} = 58$.

注意 虚 2 重 2 次体 K, $\mathrm{Cl}(K) \simeq C_3^r$.

family	$r=0$	1	2	3	4	total
$\mathcal{M}_{2\mathrm{a}}$	32	133	110	31	1	307
$\mathcal{M}_{2\mathrm{b}}$	15	30	12	1	0	58
total	47	**163**	**122**	**32**	**1**	365

例 (1) $\mathrm{Cl}(\mathbb{Q}(\sqrt{-643}, \sqrt{-4027})) \simeq C_3^4$.
(2) $\mathrm{Cl}(\mathbb{Q}(\sqrt{-3}, \sqrt{7481})) \simeq C_3^3$.

補題 ERH の下, $\sharp\mathcal{M}_{3\mathrm{a}} = 35$, $\sharp\mathcal{M}_{3\mathrm{b}} = 42$.

注意 虚 3 重 2 次体 K, $\mathrm{Cl}(K) \simeq C_3^r$.

family	$r=0$	1	2	3	4	total
$\mathcal{M}_{3\mathrm{a}}$	8	8	17	2	0	35
$\mathcal{M}_{3\mathrm{b}}$	9	15	12	5	1	42
total	17	**23**	**29**	**7**	**1**	77

例 (1) $\mathrm{Cl}(\mathbb{Q}(\sqrt{-3}, \sqrt{-43}, \sqrt{-83})) \simeq C_3^3$.
(2) $\mathrm{Cl}(\mathbb{Q}(\sqrt{-59}, \sqrt{-107}, \sqrt{8})) \simeq C_3^4$.

注意 $u = 5$ のときも基本的戦略は同じ.
ただし $\mathcal{K}_{2\mathrm{b}}$ の計算では, ある範囲の確認を
具体的に計算機で行った.
We implemented the search in the
computer algebra system Hecke which
is based on the Julia language.

ご清聴ありがとうございました