

# 導手の小さい虚 2 次体の最大不分岐拡大

防衛大 山村 健 (Ken Yamamura)

## 1 Introduction

ここに出てくる体はすべて有限次代数体 ( $\subset \mathbb{C}$ ) である. 有限次代数体  $K$  に対し, その判別式  $d_K$  の絶対値の絶対次数乗根を  $K$  の root-discriminant と呼び,  $rd_K$  で表す:

$$rd_K = |d_K|^{1/[K:\mathbb{Q}]}.$$

さて, root-discriminant が十分小さい代数体は (自明でない) 不分岐拡大をもたない. 例えば,

- 類数 1 の虚 2 次体  $\mathbb{Q}(\sqrt{d})$ ,  $-d = 3, 4, 7, 8, 11, 19, 43, 67, 163$ ;
- 類数 1 の全円分体  $\mathbb{Q}(\zeta_m)$ ,  $m = 3, 4, \dots, 84$ ;
- 素数冪導手  $< 67$  をもつ実 Abel 体

などはすべてそうである. この事実は, 不分岐拡大で root-discriminant が不変であること, (符号の比が一定の) 体を動かしたときの root-discriminant 全体の下界として体の次数の増加函数となるものが知られていることからわかる. 同じ考え方により, root-discriminant が十分小さい代数体はその最大不分岐拡大が有限次であることがわかる (§2 参照). ここでは

虚 2 次体  $K$  の最大不分岐拡大  $K_{ur}$  の Galois 群  $\text{Gal}(K_{ur}/K)$  の構造を決定すること

を目標とする. もちろん一般の場合はきわめて難しいので,  $K = \mathbb{Q}(\sqrt{d})$  ( $d$  は  $K$  の判別式) として,  $\text{Gal}(K_{ur}/K)$  が有限群になる  $K$  の導手  $|d|$  が小さいものについてのみ扱う. また  $K_{ur}$  の表示が簡単な場合にはそれを与えることにする.

さて, 上の問題について既知の主な結果は次のみと思われる.

**結果** (J. Martinet [4]).  $|d| \leq 250$  のとき, 7つの体を除いて,  $K_{ur} = K_1$  ( $K$  の Hilebert 類体) である. 7つの例外については,  $K_{ur} = K_2$  ( $K_1$  の Hilebert 類体) であり,  $\text{Gal}(K_{ur}/K)$  の構造が決定される (付属の表参照).

この結果に「類数 1 の虚 2 次体は不分岐拡大をもたない」ということが含まれていることに注意する. この結果を出すために, root-discriminant の下界のほかに, Galois 群の類群への作用を考えることにより導かれる類数の可除性に関する結果, 3 次体, 4 次体についての結果を利用したことを Martinet は述べている.

我々の得た結果は以下のようなものである:

**結果.**  $|d| \leq 420$  (一般 Riemann 予想 (GRH) の下で  $|d| \leq 659$ )<sup>1</sup> について,  $K_{ur} = K, K_1, K_2$ , または  $K_3$  で,  $\text{Gal}(K_{ur}/K)$  の構造が決定される ( $K_{ur} \neq K_1$  となるものについては表にしてまとめてある).

以下が我々の新しい点である:

- 類数計算のために class number relation および computer を用いたこと. (software は自前のものでなく, free の KANT および PARI-gp を用いた.)
- 虚 2 次体の 2-類体塔に関する知識を用いたこと.
- 不分岐非可解 Galois 拡大についての注意.

## 2 Preliminaries

結果については表にしてまとめてあるので, まず結果を出すための基本的事実について準備する.

1.  $[K_{ur} : K]$  の上界. まず, 有限次代数体  $K$  の最大不分岐拡大  $K_{ur}$  の次数の上界を得るための基本的事実について復習する.  $K$  に対し,  $n_K$  で  $K$  の絶対次数を,  $r_1(K), r_2(K)$  でそれぞれ  $K$  の実素点および虚素点の個数を表す. 最も基本的なのは次の 2 つの補題である.

**補題 1.** 有限次代数体の有限次拡大  $L/K$  がすべての有限素点で不分岐ならば,  $L$  と  $K$  の root-discriminant は一致する:  $rd_L = rd_K$ .

この補題は判別式の連鎖律からただちにしたがう. 補題 1 からただちに次が出る.

<sup>1</sup>講演の際は  $|d| \leq 367$  (一般 Riemann 予想 (GRH) の下で  $|d| \leq 419$ ) であった. この件に関しいろいろ御教示下さった Prof R. Schoof に感謝します.

**補題 2.**  $n$  を自然数とし,  $r_1, r_2$  を  $r_1 + 2r_2 = n$  なる負でない整数とする.  $B(n, r_1, r_2)$  で符号の比が  $r_1 : r_2$  に等しい  $n$  次以上の代数体の root-discriminant の下限を表す:

$$B(n, r_1, r_2) = \inf\{rd_L \mid n_L \geq n, r_i(L)/n_L = r_i/n\}.$$

- (i)  $rd_K < B(Nn_K, Nr_1(K), Nr_2(K))$  ならば,  $[K_{ur} : K] < N$  で, このとき  $K$  の類数は  $N$  より小さい. 特に,  $rd_K < B(2n_K, 2r_1(K), 2r_2(K))$  ならば,  $K_{ur} = K$ , すなわち,  $K$  は (自明でない) 不分岐拡大をもたず, このとき  $K$  の類数は 1 である.
- (ii)  $K$  の類数が 1 で, かつ  $rd_K < B(60n_K, 60r_1(K), 60r_2(K))$  ならば,  $K$  は不分岐拡大をもたない.

注意. (ii) の数 60 は「位数 60 未満の有限群は可解である」という事実から来ている. 位数 60 の非可解群は単純群  $A_5$  に同型である. もし  $K$  の類数が 1 で, かつ  $K$  が不分岐  $A_5$ -拡大をもたなければ, (ii) の  $K_{ur} = K$  のための条件を  $rd_K < B(168n_K, 168r_1(K), 168r_2(K))$  に置き換えることができる.  $B(8, 8, 0)$  と  $B(8, 0, 4)$  を除いて,  $B(n, r_1, r_2)$  の真の値は現在  $n \leq 7$  までしかわかっていない.  $B(n, r_1, r_2)$  の良い下界は, 解析的方法により Odlyzko, Serre, Poitou 等により得られている. (下界の表については, 例えば Martinet[4] 参照.) 特に, 注意すべきことは, 「GRH の下での下界は無条件下での下界に比してずっと良い。」

上の補題と Odlyzko による  $B(120, 0, 60)$  の下界を用いて, §1 で述べた次の事実を容易に示すことができる:

**命題 1.** 類数 1 の虚 2 次体  $K$  は不分岐拡大を持たない.

証明. このとき,  $rd_K \leq \sqrt{163} = 12.76 \dots$  であり, Odlyzko により  $B(120, 0, 60) \geq 17.02$  が示されているので, 補題 2(ii) より,  $K_{ur} = K$ .

注意. 同様にして, root-discriminant の計算によって, 類数 1 の全円分体を含む類数 1 の虚 Abel 体の多くは不分岐拡大を持たないことが確認できる ([8, Appendix]).

2. Class number relations. まず一般形を復習し, それから具体的な拡大について述べる.

**定理 (Kuroda[3]-Brauer[1]).**  $L/K$  を  $G$  を Galois 群とする代数体の有限次 Galois 拡大とする.  $G$  の部分群  $H$  の単位指標から誘導される  $G$  の指標  $1_H^G$  の間に 1 次関係

$$\sum_{H \leq G} a_H 1_H^G = 0$$

が成り立てば,  $L/K$  の中間体の類数  $h$ , 単数規準  $R$ ,  $1$  の  $2$  冪乗根の個数  $w_2$  の間に次の関係式が成り立つ:

$$\prod_{H \leq G} \left( \frac{h(L^H)R(L^H)}{w_2(L^H)} \right)^{a_H} = 1.$$

この定理はよく知られているように, 指標の関係式を Artin の  $L$ -函数に代入することによって得られる. なお, Walter による精密化があるが, わかりにくくなるのでここでは述べない.

任意の有限群  $G$  について, つねに自明 ( $a_H = 0 (\forall H \leq G)$ ) でない上の型の  $1$  次関係があるわけではない. また, たとえ自明でない  $1$  次関係があっても, 単数規準があるため, 上の類数関係式がただちに類数計算に使えとは限らない. ただし,  $G$  が初等  $p$ -Abel 群のときや  $2$  面体群のときは, 単数規準の部分の積が素数冪になることがわかっているので, 類数の可除性についての結果を合わせて用いることにより, 類数計算に役立つ.

さて, 我々が目的のために証明したのは次である.

**命題 2.**  $K$  を虚  $2$  次体とし,  $p$  を奇素数とする.  $L/K$  を  $D_p$ -拡大とし,  $M, M'$  を任意の  $2$  つの  $p$  次中間拡大,  $N$  を  $2$  次中間拡大とするとき, これらの類数の間に関係式

$$h(L) = \frac{[E_L : E_M E_{M'} E_N]}{p^2} \cdot \frac{h(M)^2 h(N)}{h(K)^2}$$

が成り立つ. また, 単数群の指数について,  $[E_L : E_M E_{M'} E_N] = 1, p$  または  $p^2$  である.

これは Moser が  $\mathbb{Q}$  上の  $D_p$ -拡大について同様の関係式を証明した ([5]) のとまったく同様にして証明出来る. 特に, 単数群の指数の可能性については, Galois 群の  $E_L$  への作用から,  $E_L$  を  $\mathbb{Z}[D_p]$ -加群とみなして, その構造の可能性を  $D_p$  についての整数表現についての Lee の結果を用いることにより定めることにより得られる.

これ以外に用いた既知の類数関係式については省略する.

### 3 Maximal unramified extensions of imaginary quadratic number fields of small conductors

付属の表についてすべてを説明するわけにはいかないので、虚2次体  $K = \mathbf{Q}(\sqrt{d})$  の類数が2の場合と3の場合に限って話をします。

1.  $h(K) = 2$ . 詳細は [9] を参照のこと。また、講演の際配布した表を最後につけてある。

**定理.**  $K = \mathbf{Q}(\sqrt{d})$  を判別式  $d$  の類数2の虚2次体とする。このとき、genus theory により、 $d$  は2つの基本素判別式  $d_1, d_2$  の積となり、 $K$  の絶対類体  $K_1$  は  $K$  の genus field  $\mathbf{Q}(\sqrt{d_1}, \sqrt{d_2})$  となる。GRH を仮定する。このとき

- (i)  $-d \neq 115, 235, 403$  のとき、 $K_{ur} = K_1$  である。
- (ii)  $-d = 115, 235, 403$  については、 $K_{ur} = K_2 = KF_1$  である。ただし、 $F = \mathbf{Q}(\sqrt{d_1})$ ,  $d_1 < 0$  である。また、 $F_1$  は explicit に与えられる (付属の表参照)。

これらの結果は  $K = \mathbf{Q}(\sqrt{-427})$  を除いては無条件で成り立つ。

**注意.** GRH を仮定せずとも、 $K = \mathbf{Q}(\sqrt{-427})$  に対して、 $[K_{ur} : K_1] = 1, 60, 120, 168$ , または 180 であることがわかる。また次が示せる。

**命題 3.** 虚2次体  $\mathbf{Q}(\sqrt{-427})$  は不分岐  $A_5$ -拡大をもたない。

これは次のようにしてわかる。もし、 $\mathbf{Q}(\sqrt{-427})$  が不分岐  $A_5$ -拡大  $L$  をもてば、root-discriminant の値から、 $L$  は正規で、したがって、 $\text{Gal}(L/\mathbf{Q}) \cong S_5$  または  $A_5 \times C_2$  で、5次体の data からこのような体は存在しないことがわかる。

さて定理の証明について、 $K = \mathbf{Q}(\sqrt{-403})$  についてのみ示す。(他の  $K$  については Martinet が用いた方法で示せる。)  $d = -403 = (-31) \cdot 13$  であるから、 $K_1 = \mathbf{Q}(\sqrt{-31}, \sqrt{13})$  であり、 $h(K_1) = 3$  である。 $F_1 = F(\alpha_2)$ ,  $\alpha_2^3 + \alpha_2 - 1 = 0$  であるから、 $K_2 = K_1(\alpha_2)$  である。 $\text{Gal}(K_2/K) \cong \text{Gal}(F_1/\mathbf{Q}) \cong D_3$  で、 $K_2$  の類数を計算するために、 $K_2/K$  の3次中間拡大  $K(\alpha_2)$  の類数を計算すると、 $h(K(\alpha_2)) = 2$  となった (KANT, PARI-gp を用いた)。よって、 $Q$  を単数群の指数として、

$$h(K_2) = \frac{Q}{9} \cdot \frac{2^2 \cdot 3}{2^2} = \frac{Q}{3} (= 1 \text{ または } 3)$$

となるが,  $K_2$  の類数は3で割れない ( $h(K_1) = 3$  であるから) から,  $h(K_2) = 1$  である.  $rd_{K_2} = rd_K = \sqrt{403} = 20.074\dots$  かつ  $B(720, 0, 360) \geq 20.551$  であるから,  $K_{ur} = K_2$  である.

注意. 上の定理から,  $\mathbb{Q}(\sqrt{-403})$  を含め, 類数2の虚2次体は ( $\mathbb{Q}(\sqrt{-427})$  については GRH の下で) 不分岐非可解 Galois 拡大をもたないが, 導手403の円分体  $\mathbb{Q}(\zeta_{403})$  は不分岐  $A_5$ -拡大をもつ. これは次のことからしたがう.  $L$  を  $\mathbb{Q}$  上の5次既約多項式  $X^5 + 2X^3 + 5X^2 + 2X + 1$  の最小分解体とすると,  $\text{Gal}(L/\mathbb{Q}) \cong A_5$  で,  $L/\mathbb{Q}$  で分岐する有限素点は13, 31のみで, その分岐指数はそれぞれ2および3である. そこで,  $E$  を実2次体  $\mathbb{Q}(\sqrt{13})$  と導手31の(ただ1つの)3次巡回体との合成体とすると,  $LE/E$  はすべての有限素点で不分岐な  $A_5$ -拡大となる. また,  $E$  の類数は1である. よって  $E$  を含むすべての虚 Abel 体は不分岐  $A_5$ -拡大をもつ.

2.  $h(K) = 3$ . 類数3の虚2次体は  $\mathbb{Q}(\sqrt{d})$ ,  $-d = 23, 31, 59, 83, 107, 139, 211, 283, 307, 331, 379, 499, 547, 643, 883, 907$  の16個である. このうち,  $d = -283, -331, -643$  を除いてはすべて  $h(K_1) = 1$  であることが確かめられ, しかも GRH の下で,  $|d| < 643$  について  $K_{ur} = K_1$  である. さて,  $d = -283, -331, -643$  については,  $K_1$  の類群が Klein の4元群  $V_4$  に同型で,  $\text{Gal}(K_2/\mathbb{Q}) \cong S_4$ ,  $\text{Gal}(K_2/K) \cong A_4$  であることはよく知られている.  $K_2$  の6次部分体の類群を計算し,  $V_4$ -拡大についての類数関係式を繰り返し用いることにより,  $h(K_2) = 2$  であることを確認することが出来た. しかも,  $\text{Gal}(K_3/\mathbb{Q}) \cong \tilde{S}_4$ ,  $\text{Gal}(K_3/K) \cong \tilde{A}_4$  である<sup>2</sup>. これらの体は最近 embedding problem  $\tilde{S}_4 \rightarrow S_4$  の観点から調べられている. 特に  $\mathbb{Q}(\sqrt{-283})$  の第3 Hilbert 類体は符号  $(1, 3)$  の8次体で, その Galois 閉包が  $\mathbb{Q}$  の  $\tilde{S}_4$ -拡大となるもののうち判別式の絶対値が最小になるものの Galois 閉包である ([2] 参照). なお,  $K = \mathbb{Q}(\sqrt{-283}), \mathbb{Q}(\sqrt{-331}), \mathbb{Q}(\sqrt{-643})$  については  $K_{ur} = K_3$  となる ( $d = -643$  については GRH の下で).

## 4 Unramified nonsolvable Galois extensions

導手の小さい虚2次体の最大不分岐拡大を扱っている際には, 不分岐非可解 Galois 拡大はなかなか現れないが, 最近得られている5次体の data

<sup>2</sup>この  $\tilde{A}_n, \tilde{S}_n (n \geq 4)$  は Serre による記法で,  $\tilde{A}_n$  は  $A_n$  の2次巡回群  $C_2$  による (同型を除いて) ただ1つの分裂しない中心拡大であり,  $\tilde{S}_n$  は  $S_n$  の  $C_2$  による分裂しない中心拡大のうち,  $S_n$  の互換は  $\tilde{S}_n$  の位数2の元に,  $S_n$  の互いに素な2つの互換の積は  $\tilde{S}_n$  の位数4の元に持ち上がる, ということによって特徴づけられるものである.

から次が得られる.

**命題 4.**  $\mathbb{Q}(\sqrt{-1507})$  は  $\mathbb{Q}$  上正規な不分岐  $A_5$ -拡大をもつ最初の虚 2 次体である. すなわち, 判別式  $d$ ,  $|d| < 1507$  の虚 2 次体  $\mathbb{Q}(\sqrt{d})$  はこのような拡大をもたない. また,  $\mathbb{Q}(\sqrt{-1507})$  のこのような拡大は 5 次既約多項式  $X^5 - 5X^3 + 5X^2 + 24X + 4$  の最小分解体 ( $\mathbb{Q}$  の  $A_5$ -拡大) との合成体として得られ, したがってその Galois 群は  $A_5 \times C_2$  に同型である. さらに,  $\mathbb{Q}$  上の  $S_5$ -拡大である不分岐  $A_5$ -拡大をもつ最初の虚 2 次体は  $\mathbb{Q}(\sqrt{-4511})$  である.

注意. 「 $\mathbb{Q}$  上正規な」はおそらく不要である. 残念ながら現段階では GRH を仮定してもこれを省くことは難しいと思われる (GRH を仮定すれば, root-discriminant の評価により,  $|d| < 1507$  の虚 2 次体のほとんどについては,  $\mathbb{Q}$  上正規でない不分岐  $A_5$ -拡大もたないことを示せるが, 示せないものが数個存在する.) 将来 10 次体の data が充実することによりこれは解消されるであろう. (2 次体の不分岐  $A_5$ -拡大が  $\mathbb{Q}$  上正規でなければ, その  $\mathbb{Q}$  上の Galois 閉包は 10 次体の Galois 閉包で, その Galois 群は  $(A_5 \times A_5) \cdot C_2$  になる.) 実際は「 $\mathbb{Q}(\sqrt{-1507})$  は不分岐非可解 Galois 拡大をもつ最初の虚 2 次体である」と予想される.

$|d| < 2100$  の範囲で不分岐  $A_5$ -拡大をもつのは  $d = -1507, -1959, -2083$  の 3 個のみで, これらの不分岐  $A_5$ -拡大いずれも  $\mathbb{Q}$  の  $A_5$ -拡大との合成として得られる. このことからわかる特に注意すべきこととは, 「虚 2 次体が不分岐  $A_5$ -拡大をもつ確率は (もし存在すれば) 正である」ということである. より正確には,  $D_{(0,1)}(X)$  を絶対値が  $X$  以下の負の基本判別式全体の集合として,

$$\liminf_{X \rightarrow \infty} \frac{\#\{d \in D_{(0,1)}(X) \mid \mathbb{Q}(\sqrt{d}) \text{ は不分岐 } A_5\text{-拡大をもつ}\}}{\#D_{(0,1)}(X)} > 0$$

である. なぜなら,  $d \in D_{(0,1)}(X)$  が 1507 で割り切れれば,  $\mathbb{Q}(\sqrt{d})$  は不分岐  $A_5$ -拡大をもつからである. ここでついでに,  $\#D_{(0,1)}(X)$  についても述べておこう. 虚 2 次体の判別式は完全にわかっているので, (squarefree な) 自然数の分布についてよく知られたことから,  $X \rightarrow \infty$  のとき

$$\#D_{(0,1)}(X) = \sum_{\substack{m \equiv 3 \pmod{4} \\ m: \text{squarefree} \leq X}} 1 + \sum_{\substack{m \equiv 1, 2 \pmod{4} \\ m: \text{squarefree} \leq X/4}} 1 \sim \frac{3}{\pi^2} X$$

である. 上の極限の真の値を求めるには, 5 次体 (および 10 次体) の判別式の分布についての研究が進まなければならない.

ところで,  $\mathbb{Q}(\sqrt{-1507})$  の類数は 4 で, 類群は巡回群である. その絶対類体  $\mathbb{Q}(\sqrt{-11}, \sqrt{(-23 + 3\sqrt{137})/2})$  の類数は 1 である. (これは  $\mathbb{Q}$  の  $D_4$ -拡大に関する類数関係式および,  $\mathbb{Q}(\sqrt{-1507})$  の絶対類体の類数が 2 で割れない ( $\text{Cl}(\mathbb{Q}(\sqrt{-1507})) \cong C_4$  であるから) ことから確かめられる.) この体は総虚な類数 1 の体で不分岐非可解 Galois 拡大をもつ最初の例であると思われる. なお, 類数 1 の虚 Abel 体は全部で 172 個存在し, GRH を仮定すれば, このうちの少なくとも 155 個の体は不分岐拡大をもたない ([8, Appendix] 参照). 不分岐拡大をもつ類数 1 の CM 体は知られていないと思われる. この体は CM 体ではないが, 内田 [7] により類数 1 の総虚な正規 8 次体は高々有限個であることが証明されている<sup>3</sup> ことに注意しておく. 類数 1 の総虚な正規 8 次体のうち CM 体はすべて決定されている. CM 体でないものはすべて  $\mathbb{Q}$  の  $D_4$ -拡大で, 類数 1, 2 または 4 の虚 2 次体の 4 次巡回拡大である. 特に, 類数 4 (より正確には類群が位数 4 の巡回群) の虚 2 次体 (30 個ある) の絶対類体のうち類数 1 のものは 20 個存在する. 残りのものについては現在決定進行中である.

上に現れた不分岐非可解 Galois 拡大は  $A_5$ -拡大のみであるが, 任意の自然数  $n \geq 5$  について, 不分岐  $A_n$ -拡大をもつ虚 2 次体が無数に存在することがわかっている. 交代群以外の非可換単純群  $G$  については,  $\text{PSL}(2, 7)$  を除いて不分岐  $G$ -拡大をもつ 2 次体の存在は知られていない. 私が知っている不分岐  $\text{PSL}(2, 7)$ -拡大をもつ虚 2 次体のうち判別式の絶対値が最小のものは  $\mathbb{Q}(\sqrt{-30759})$  である.  $\mathbb{Q}(\sqrt{-30759})$  の不分岐  $\text{PSL}(2, 7)$ -拡大もやはり  $\mathbb{Q}$  の  $\text{PSL}(2, 7)$ -拡大との合成として得られるので, 「虚 2 次体が不分岐  $\text{PSL}(2, 7)$ -拡大をもつ確率も (もし存在すれば) 正である。」また  $\mathbb{Q}(\sqrt{-14731})$  は不分岐  $A_6$ -拡大をもつ.

最後に, 講演終了時に質問が出た, 無限類体塔をもつ虚 2 次体について. 虚 2 次体で無限類体塔をもつことが判明しているもののうち, 私が知る限り, 判別式の絶対値が最小のものは, Schmithals[6] により確認された  $\mathbb{Q}(\sqrt{-13335})$  である. 判別式の素因数分解は  $d = -13335 = -3 \cdot 5 \cdot 7 \cdot 127$  で,  $rd = \sqrt{13335} = 115.47 \dots$  である.

参考文献の後に講演時に配布した表の訂正改良版をつけておく. (群の記号を若干変えていることにも注意.)

<sup>3</sup>彼はより一般の類数 1 の総虚な正規体の個数の有限性を証明している.



## 参考文献

- [1] R. Brauer, *Beziehung zwischen Klassenzahl von Teilkörpern eines galoisschen Körpers*, Math. Nachr. **4**(1951), 158–174.
- [2] A. Jehanne, *Sur les extension de  $\mathbf{Q}$  à groupe de Galois  $S_4$  et  $\tilde{S}_4$* , Acta Arith. **70**(1995), 259–276.
- [3] S. Kuroda, *Über die Klassenzahlen algebraischer Zahlkörper*, Nagoya Math. J. **1**(1950), 1–10.
- [4] J. Martinet, *Petit discriminant des corps de nombres*, Number theory days, 1980(Exeter, 1980), London Math. Soc. Lecture Note, Ser. 56, Cambridge Univ. Press, Cambridge, New York, 1982, pp. 151–193.
- [5] N. Moser, *Unités et nombre de classes d'une extension galoisienne diédrale de  $\mathbf{Q}$* , Abh. Math. Sem. Univ. Hamburg **48**(1979), 54–75.
- [6] B. Schmithals, *Konstruktion imaginärquadratischer Körper mit unendlichem Klassenkörperturm*, Archiv. Math. **34**(1980), 307–312.
- [7] 内田興二, 類数1の虚 Galois 体について, 数学 **25**(1973), no. 2, 172–173.
- [8] K. Yamamura, *The determination of the imaginary abelian number fields with class number one*, Math. Comp. **62**(1994), 899–921.
- [9] K. Yamamura, *The maximal unramified extensions of the imaginary quadratic number fields with class number two*, to appear in J. Number Theory.

**Theorem.** Let  $K = \mathbf{Q}(\sqrt{d})$  be an imaginary quadratic number field with class number two, i.e.,  $-d = 15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403, \text{ or } 427$ . Then by genus theory  $d$  is factored as  $d_1 d_2$ , where  $d_1$  and  $d_2$  are fundamental prime discriminants, and the Hilbert class field  $K_1$  of  $K$  is the genus field  $\mathbf{Q}(\sqrt{d_1}, \sqrt{d_2})$  of  $K$ . We assume that the Generalized Riemann Hypothesis is true. Let  $K_{ur}$  be the maximal unramified extension of  $K$ .

(i) Except for  $-d = 115, 235, 403$ , we have  $K_{ur} = K_1$ .

(ii) For  $-d = 115, 235$ , and  $403$ , we have  $K_{ur} = K_2$ , the second Hilbert class field of  $K$ , i.e., the Hilbert class field of  $K_1$ . If we take  $d_1 < 0$  and put  $F = \mathbf{Q}(\sqrt{d_1})$ , then  $K_{ur} = K_2 = K_1 F_1 = K F_1$ . Moreover, the Hilbert class field  $F_1$  of  $F$  is given explicitly as follows:

$$F_1 = \mathbf{Q}(\sqrt{-23}, \alpha_1), \alpha_1^3 - \alpha_1 - 1 = 0 \text{ if } d = -115;$$

$$F_1 = \mathbf{Q}(\sqrt{-47}, \gamma_1), \gamma_1^5 - \gamma_1^3 - 2\gamma_1^2 - 2\gamma_1 - 1 = 0 \text{ if } d = -235;$$

$$F_1 = \mathbf{Q}(\sqrt{-31}, \alpha_2), \alpha_2^3 + \alpha_2 - 1 = 0 \text{ if } d = 403.$$

Results are unconditional except for  $K = \mathbf{Q}(\sqrt{-427})$ .

**Corollary.** We assume GRH. None of the imaginary quadratic number fields with class number two has any unramified nonsolvable Galois extension.

We tabulate  $K, d = d_1 d_2, rd_K, K_1, K_{ur} = K_2$ , and  $G = \text{Gal}(K_{ur}/K)$ .

Table

$K$	$d = d_1 d_2$	$rd_K$	$K_1$	$K_2$	$G$
$\mathbf{Q}(\sqrt{-15})$	$-15 = (-3) \cdot 5$	3.872	$\mathbf{Q}(\sqrt{-3}, \sqrt{5})$	$K_1$	$C_2$
$\mathbf{Q}(\sqrt{-5})$	$-20 = (-4) \cdot 5$	4.472	$\mathbf{Q}(\sqrt{-1}, \sqrt{5})$	$K_1$	$C_2$
$\mathbf{Q}(\sqrt{-6})$	$-24 = (-3) \cdot 8$	4.898	$\mathbf{Q}(\sqrt{-3}, \sqrt{2})$	$K_1$	$C_2$
$\mathbf{Q}(\sqrt{-35})$	$-35 = (-7) \cdot 5$	5.916	$\mathbf{Q}(\sqrt{-7}, \sqrt{5})$	$K_1$	$C_2$
$\mathbf{Q}(\sqrt{-10})$	$-40 = (-8) \cdot 5$	6.324	$\mathbf{Q}(\sqrt{-2}, \sqrt{5})$	$K_1$	$C_2$
$\mathbf{Q}(\sqrt{-51})$	$-51 = (-3) \cdot 17$	7.141	$\mathbf{Q}(\sqrt{-3}, \sqrt{17})$	$K_1$	$C_2$
$\mathbf{Q}(\sqrt{-13})$	$-52 = (-4) \cdot 13$	7.211	$\mathbf{Q}(\sqrt{-1}, \sqrt{13})$	$K_1$	$C_2$
$\mathbf{Q}(\sqrt{-22})$	$-88 = (-11) \cdot 8$	9.380	$\mathbf{Q}(\sqrt{-11}, \sqrt{2})$	$K_1$	$C_2$
$\mathbf{Q}(\sqrt{-91})$	$-91 = (-7) \cdot 13$	9.539	$\mathbf{Q}(\sqrt{-7}, \sqrt{13})$	$K_1$	$C_2$
$\mathbf{Q}(\sqrt{-115})$	$-115 = (-23) \cdot 5$	10.723	$\mathbf{Q}(\sqrt{-23}, \sqrt{5})$	$K_1(\alpha_1)$	$D_3$
$\mathbf{Q}(\sqrt{-123})$	$-123 = (-3) \cdot 41$	11.090	$\mathbf{Q}(\sqrt{-3}, \sqrt{41})$	$K_1$	$C_2$
$\mathbf{Q}(\sqrt{-37})$	$-148 = (-4) \cdot 37$	12.165	$\mathbf{Q}(\sqrt{-1}, \sqrt{37})$	$K_1$	$C_2$
$\mathbf{Q}(\sqrt{-187})$	$-187 = (-11) \cdot 17$	13.674	$\mathbf{Q}(\sqrt{-11}, \sqrt{17})$	$K_1$	$C_2$
$\mathbf{Q}(\sqrt{-58})$	$-232 = (-8) \cdot 29$	15.231	$\mathbf{Q}(\sqrt{-2}, \sqrt{29})$	$K_1$	$C_2$
$\mathbf{Q}(\sqrt{-235})$	$-235 = (-47) \cdot 5$	15.329	$\mathbf{Q}(\sqrt{-47}, \sqrt{5})$	$K_1(\gamma_1)$	$D_5$
$\mathbf{Q}(\sqrt{-267})$	$-267 = (-3) \cdot 89$	16.340	$\mathbf{Q}(\sqrt{-3}, \sqrt{89})$	$K_1$	$C_2$
$\mathbf{Q}(\sqrt{-403})$	$-403 = (-31) \cdot 13$	20.074	$\mathbf{Q}(\sqrt{-31}, \sqrt{13})$	$K_1(\alpha_2)$	$D_3$
$\mathbf{Q}(\sqrt{-427})$	$-427 = (-7) \cdot 61$	20.663	$\mathbf{Q}(\sqrt{-7}, \sqrt{61})$	$K_1$	$C_2$

Table of imaginary quadratic number fields  $K = \mathbf{Q}(\sqrt{d})$ ,  $|d| \leq 659$  with  $K_{ur} \neq K_1$ 

$-d$	$Cl_K$	$K_1$	$K_2$	$l$	$G$
115	$C_2$	$\mathbf{Q}(\sqrt{-23}, \sqrt{5})$	$K_1(\alpha_1)$	2	$D_3$
120	$V_4$	$\mathbf{Q}(\sqrt{-3}, \sqrt{2}, \sqrt{5})$		2	$Q_8$
155	$C_4$	$K(\sqrt{(-1 + 5\sqrt{5})/2})$	$K_1(\alpha_2)$	2	$Q_{12}$
184	$C_4$	$K(\sqrt{-3 + 4\sqrt{2}})$	$K_1(\alpha_1)$	2	$Q_{12}$
195	$V_4$	$\mathbf{Q}(\sqrt{-3}, \sqrt{5}, \sqrt{13})$		2	$Q_{16}$
235	$C_2$	$\mathbf{Q}(\sqrt{-47}, \sqrt{5})$	$K_1(\gamma_1)$	2	$D_5$
248	$C_8$		$K_1(\alpha_2)$	2	$I_3^8$
255	$C_6 \times C_2$	$\mathbf{Q}(\sqrt{-3}, \sqrt{5}, \sqrt{17}, \alpha_{29})$		2	$Q_8 \times C_3$
260	$C_4 \times C_2$	$\mathbf{Q}(\sqrt{-1}, \sqrt{5}, \sqrt{8 + \sqrt{65}})$		2	$SA_{16}$
276	$C_4 \times C_2$	$\mathbf{Q}(\sqrt{-1}, \sqrt{-23}, \sqrt{13 + 8\sqrt{3}})$	$K_1(\alpha_1)$	2	$Q_{12} \times C_2$
280	$V_4$	$\mathbf{Q}(\sqrt{-7}, \sqrt{2}, \sqrt{5})$		2	$Q_{16}$
283	$C_3$	$K(\alpha_{31})$	$K_1(\beta_1)$	3	$\tilde{A}_4$
295	$C_8$		$K_1(\alpha_4)$	2	$I_3^8$
299	$C_8$		$K_1(\alpha_1)$	2	$I_3^8$
312	$V_4$	$\mathbf{Q}(\sqrt{-3}, \sqrt{2}, \sqrt{13})$		2	$Q_{16}$
331	$C_3$	$K(\alpha_{36})$	$K_1(\beta_2)$	3	$\tilde{A}_4$
335	$C_{18}$		$K_1(\alpha_9)$	2	$D_3 \times C_9$
340	$V_4$	$\mathbf{Q}(\sqrt{-1}, \sqrt{5}, \sqrt{17})$		2	$SD_{16}$
355	$C_4$	$K(\sqrt{-3 + 4\sqrt{5}})$		2	$Q_{28}$
372	$V_4$	$\mathbf{Q}(\sqrt{-1}, \sqrt{-3}, \sqrt{-31})$	$K_1(\alpha_2)$	2	$D_6$
376	$C_8$		$K_1(\gamma_1)$	2	$I_5^8$
391	$C_{14}$		$K_1(\alpha_1)$	2	$D_3 \times C_7$
395	$C_8$		$K_1(\gamma_2)$	2	$I_5^8$
403	$C_2$	$\mathbf{Q}(\sqrt{-31}, \sqrt{13})$	$K_1(\alpha_2)$	2	$D_3$
408	$V_4$	$\mathbf{Q}(\sqrt{-3}, \sqrt{2}, \sqrt{17})$	$K_1(\sqrt{-(5 + \sqrt{17})/2})$	2	$D_4$
415	$C_{10}$	$\mathbf{Q}(\sqrt{-83}, \sqrt{5}, \gamma_{18})$	$K_1(\alpha_6)$	2	$D_3 \times C_5$
420	$C_2^3$	$\mathbf{Q}(\sqrt{-1}, \sqrt{-3}, \sqrt{-7}, \sqrt{5})$		2	$\Gamma_4 32c_3$

We needed to assume GRH to determine the degree of  $K_{ur}$  for fields  $K = \mathbf{Q}(\sqrt{d})$  with discriminant  $d < -420$ .  $l$  denotes the length of the class field tower of  $K$ :  $K = K_0 \subset K_1 \subset K_2 \subset \dots$  ( $K_{i+1}$  is the Hilbert class field of  $K_i$ ), i.e.,  $l$  is the smallest number with  $K_l = K_{l+1}$ . For all exhibited fields,  $K_{ur} = K_l$ .  $G$  denotes the Galois group  $\text{Gal}(K_{ur}/K)$ .

$\alpha_i, \beta_i$  and  $\gamma_i$  are primitive roots of the  $i$ th cubic field of signature  $(1, 1)$ , the  $i$ th quartic field of signature  $(2, 1)$  with Galois group isomorphic to  $S_4$ , and the  $i$ th quintic field of signature  $(1, 2)$  with Galois group isomorphic to  $D_5$ , respectively.

Continued(under GRH)

$-d$	$Cl_K$	$K_1$	$K_2$	$l$	$G$
435	$V_4$	$\mathbb{Q}(\sqrt{-3}, \sqrt{5}, \sqrt{29})$		2	$Q_{16} \times C_3$
440	$C_6 \times C_2$	$\mathbb{Q}(\sqrt{-11}, \sqrt{2}, \sqrt{5}, \alpha_{49})$		2	$Q_{16} \times C_3$
455	$C_{10} \times C_2$	$\mathbb{Q}(\sqrt{-7}, \sqrt{5}, \sqrt{13}, \gamma_{21})$		2	$Q_8 \times C_5$
472	$C_6$	$\mathbb{Q}(\sqrt{-59}, \sqrt{2}, \alpha_4)$		2	$D_3 \times C_3$
483	$V_4$	$\mathbb{Q}(\sqrt{-3}, \sqrt{-7}, \sqrt{-23})$	$K_1(\alpha_1)$	2	$D_6$
515	$C_6$	$\mathbb{Q}(\sqrt{-103}, \sqrt{5}, \alpha_{59})$	$K_1(\gamma_3)$	2	$D_5 \times C_3$
520	$V_4$	$\mathbb{Q}(\sqrt{-2}, \sqrt{5}, \sqrt{13})$		2	$Q_{24}$
527	$C_{18}$		$K_1(\alpha_2)$	2	$D_3 \times C_9$
535	$C_{14}$		$K_1(\alpha_9)$	2	$D_3 \times C_7$
552	$C_4 \times C_2$	$\mathbb{Q}(\sqrt{-3}, \sqrt{-23}, \sqrt{(-1 + 2\sqrt{6})/2})$	$K_1(\alpha_1)$	2	$D_3 \times C_4$
555	$V_4$	$\mathbb{Q}(\sqrt{-3}, \sqrt{5}, \sqrt{37})$		2	$Q_{32}$
563	$C_9$		$K_1(\beta_4)$	3	$Q_8 \times C_9$
564	$C_4 \times C_2$	$K(\sqrt{-1}, \sqrt{-47}, \sqrt{(1 + 4\sqrt{3})/2})$	$K_1(\gamma_1)$	2	$D_5 \times C_4$
568	$C_4$	$K(\sqrt{-1 + 6\sqrt{2}})$		2	$Q_{28}$
580	$C_4 \times C_2$	$\mathbb{Q}(\sqrt{-1}, \sqrt{5}, \sqrt{12 + \sqrt{145}})$	$K_1(\alpha_1)$	2	$D_3 \times C_4$
595	$V_4$	$\mathbb{Q}(\sqrt{-7}, \sqrt{5}, \sqrt{17})$	$K_1(\gamma_4)$	2	$Q_8 \times C_5$
611	$C_{10}$	$\mathbb{Q}(\sqrt{-47}, \sqrt{13}, \gamma_{28})$	$K_1(\gamma_1)$	2	$D_5 \times C_5$
632	$C_8$		$K_1(\gamma_2)$	2	$I_5^8$
635	$C_{10}$	$\mathbb{Q}(\sqrt{-127}, \sqrt{5}, \gamma_{31})$	$K_1(\gamma_5)$	2	$D_5 \times C_5$
643	$C_3$	$K(\alpha_{71})$	$K_1(\beta_5)$	3	$\tilde{A}_4$
644	$C_8 \times C_2$		$K_1(\alpha_1)$	2	$D_3 \times C_8$
651	$C_4 \times C_2$	$K(\sqrt{-3}, \sqrt{-7}, \sqrt{(13 + \sqrt{217})/2})$	$K_1(\alpha_2)$	2	$Q_{12} \times C_2$
655	$C_{12}$	$K(\sqrt{7 + \sqrt{5}}, \alpha_{74})$	$K_1(\gamma_6)$	2	$Q_{20} \times C_3$

$C_n$  is the cyclic group of order  $n$ ,  $D_n$  is the dihedral group of order  $2n$ ,  $Q_{4n}$  is the generalized quaternion group of order  $4n$ , and  $SD_{8n}$  is the semi-dihedral group of order  $8n$ :

$$D_n = \langle a, b \mid a^n = b^2 = 1, b^{-1}ab = a^{-1} \rangle,$$

$$Q_{4n} = \langle a, b \mid a^{2n} = 1, b^2 = a^n, b^{-1}ab = a^{-1} \rangle,$$

$$SD_{8n} = \langle a, b \mid a^{4n} = b^2 = 1, b^{-1}ab = a^{2n-1} \rangle.$$

$I_n^{2m}$  denotes the group of order  $2mn$  given by  $\langle a, b \mid a^{2m} = b^n = 1, a^{-1}ba = b^{-1} \rangle$ .

$SA_{8n}$  denotes the group of order  $8n$  given by  $\langle a, b \mid a^{4n} = b^2 = 1, b^{-1}ab = a^{2n+1} \rangle$ .

$\tilde{A}_4$  is the double covering of  $A_4$ :  $\tilde{A}_4 \cong \text{SL}(2, 3)$ .  $\Gamma_4 32c_3$  denotes the group of order 32 given by

$$\langle a, b, c \mid a^4 = b^4 = 1, c^2 = a^2b^2, b^{-1}ab = a^{-1}, ac = ca, c^{-1}bc = b^{-1} \rangle.$$