同じ判別式と単数基準を持つ有理数体上の虚の4次ガロア拡大の無限族について

許斐 豊 (名城大学)

1　導入と主結果

本稿[1]では, 特に断らない限り, p を素数, ℓ を奇素数とする. また有限次代数体 K について, K の単数基準, 判別式, 類数を, それぞれ $\mathrm{reg}(K)$, $\mathrm{disc}(K)$, $h(K)$ で表す.

与えられた二つの有理数体上の有限次ガロア拡大が一致する十分条件は, 昔から研究がなされている. たとえば, 有理数体上の二つの有限次ガロア拡大体のゼータ関数が一致するならば, この二つの体は一致してしまうという事実は, とてもよく知られている. 他にも, 参考文献 [11] において, 有理数体上の二つの有限次ガロア拡大体の絶対ガロア群が同型となるならば, この二つの体が一致するという事実が証明されている.

このような十分条件で直ちに思いつく例として, 二つの実二次体の単数基準が一致するならば, その二つの実二次体は一致してしまう, という事実が挙げられる. なぜなら, この状況下で単数基準が一致すると, log の単射性により, ただ一つの基本単数が一致してしまうからである.

すると, 任意の ℓ について, 有理数体上の二つの ℓ 次ガロア拡大体の単数基準が一致するならば, この二つの体は一致するのか, という疑問が生じる. ここでは詳細は述べないが, さらに類数と判別式の一致を仮定し, 次の予想が正しければ, この二つの ℓ 次ガロア拡大体は一致することがわかる.

予想 1.1. ℓ を奇素数, K_1 と K_2 を有理数体上の任意の ℓ 次ガロア拡大とし,

$$S_i(x) = \{p < x \mid p \text{ は } K_i/\mathbb{Q} \text{ で完全分解する }\}$$

とおく. このとき

$$\prod_{p \in S_1(x)} \frac{p^\ell - 1}{(p-1)^\ell} \sim \prod_{q \in S_2(x)} \frac{q^\ell - 1}{(q-1)^\ell} \quad (x \to \infty)$$

が成立しているならば, $K_1 = K_2$ となる.

有理数体上の ℓ 次ガロア拡大体は, 常に総実代数体であることに注意する. では, 有理数体上の虚のガロア拡大体について, 単数基準, 判別式, 類数が一致する二つの体は一致するであろうか？答えは「いいえ」で, 有理数体上の虚の 4 次拡大で反例を構成することが出来る (例 4.3 を参照).

本稿の目的は, このような反例を構成するために, 次の定理を示すことである:

定理 1.2. 同じ判別式と単数基準をもつ異なる虚の巡回 4 次体のペアが無限に多く存在する.

本稿では証明は行わないが, 双 2 次体でも同様な結果が得られる:

定理 1.3. 同じ判別式と単数基準をもつ異なる虚の双 2 次体のペアが無限に多く存在する.

[1] 本研究は学習院大学の飯塚義睦氏との共同研究である.

2　巡回 4 次体のペアの構成

0 でない $s, t \in \mathbb{Q}$ に対し, $\mathbb{Q}$ 係数の 4 次多項式

$$f(s,t,X) = X^4 - 2s(t^2+1)X^2 + s^2t^2(t^2+1)$$

を考える. $f(s,t,X)$ の $\mathbb{C}$ における 4 つの根は

$$\pm\sqrt{s(t^2+1) \pm s\sqrt{t^2+1}} \quad (\text{複号任意})$$

である. $f(s,t,X)$ の $\mathbb{Q}$ 上の最小分解体を $K_{s,t}$ で表す.

$K_{s,t}/\mathbb{Q}$ が Galois 拡大の場合, $K_{s,t}$ の $\mathbb{Q}$ 上の共役体がすべて一致するので,

$$K_{s,t} = \mathbb{Q}\left(\sqrt{s(t^2+1) + s\sqrt{t^2+1}}\right)$$

が成り立つ. また, $s > 0$ のとき総実であり, $s < 0$ のとき総虚である.

定理 2.1. $f(X) = X^4 + aX^2 + b \in \mathbb{Q}[X]$ とし, $f(X)$ は $\mathbb{Q}$ 上既約であると仮定する. もし $b \notin (\mathbb{Q}^\times)^2$ かつ $b(a^2-4b) \in (\mathbb{Q}^\times)^2$ ならば, 多項式 f の根によって $\mathbb{Q}$ 上生成される体は巡回 4 次体である.

証明. Jensen, Ledet and Yui [6], Corollary 2.2.4 を参照. □

補題 2.2. s, t を 0 でない有理数とし, $t^2+1 \notin \mathbb{Q}^2$ を満たすと仮定する. このとき, $f(s,t,X)$ は $\mathbb{Q}$ 上の既約多項式であり, $K_{s,t}$ は巡回 4 次体である. さらに, 2 次体 $\mathbb{Q}(\sqrt{t^2+1})$ は $K_{s,t}$ の部分体である.

証明. $K_{s,t}$ が巡回 4 次体であることは, $f(s,t,X)$ について定理 2.1 の条件を確認すればよい.

$f(s,t,X)$ の根の形に着目すると, $t^2+1 \notin \mathbb{Q}^2$ より, $f(s,t,X)$ は 4 次未満の有理数係数多項式に分解しないことが直ちに確かめられる. したがって, $f(s,t,X)$ は $\mathbb{Q}$ 上既約である.

再び $t^2+1 \notin \mathbb{Q}^2$ より, $\mathbb{Q}(\sqrt{t^2+1})$ は 2 次体である. $\theta = \sqrt{s(t^2+1) + s\sqrt{t^2+1}}$ とおくと, $K_{s,t} = \mathbb{Q}(\theta)$ かつ $\mathbb{Q}(\sqrt{t^2+1}) = \mathbb{Q}(\theta^2)$ である. ゆえに, $\mathbb{Q}(\sqrt{t^2+1})$ は $K_{s,t}$ の部分体である. □

補題 2.3. t を整数とするとき, t^2+1 が平方数ならば $t = 0$ である.

証明. t^2+1 が平方数であると仮定する. ある整数 u が存在して, $t^2+1 = u^2$ である. よって,

$$(u-t)(u+t) = u^2 - t^2 = 1.$$

$u-t$ と $u+t$ はともに整数だから,

$$(u-t, u+t) = (1,1) \;\text{ or }\; (-1,-1).$$

いずれにせよ, $u-t = u+t$ である. これより, $t = 0$ を得る. □

命題 2.4. s, t を 0 でない整数とする. このとき, $f(s,t,X)$ は $\mathbb{Q}$ 上既約であり, $K_{s,t}$ は巡回 4 次体である.

証明. 補題 2.2 と補題 2.3 より $f(s,t,X)$ は $\mathbb{Q}$ 上既約であり, したがって $K_{s,t}$ は巡回 4 次体である. $\square$

補題 2.5. s, s', t を 0 でない有理数とし, $ss' \notin \mathbb{Q}^2$ を満たすとする. このとき, $K_{s,t} = K_{s',t}$ であるためには $t^2+1 \in ss'\mathbb{Q}^2$ が必要十分である.

証明. まず,

$$K_{s,t} = \mathbb{Q}\left(\sqrt{s(t^2+1)+s\sqrt{t^2+1}}\right),$$
$$K_{s',t} = \mathbb{Q}\left(\sqrt{s'(t^2+1)+s'\sqrt{t^2+1}}\right)$$

が成り立つことを注意しておく.

$K_{s,t} = K_{s',t}$ と仮定する. このとき, $\sqrt{s'(t^2+1)+s'\sqrt{t^2+1}} \in K_{s,t}$ であるから,

$$\frac{\sqrt{ss'}}{s} = \frac{\sqrt{s'}}{\sqrt{s}} = \frac{\sqrt{s'(t^2+1)+s'\sqrt{t^2+1}}}{\sqrt{s(t^2+1)+s\sqrt{t^2+1}}} \in K_{s,t}.$$

ゆえに, $\mathbb{Q}(\sqrt{ss'})$ は $K_{s,t}$ の部分体である. また, 補題の仮定 $ss' \notin \mathbb{Q}^2$ より, $\mathbb{Q}(\sqrt{ss'})$ は 2 次体である. 一方, 補題 2.2 によれば, $K_{s,t}$ は $\mathbb{Q}(\sqrt{t^2+1})$ を含む. $K_{s,t}$ は巡回体であるから, 部分体となるような 2 次体は 1 つしかない. よって, $\mathbb{Q}(\sqrt{ss'}) = \mathbb{Q}(\sqrt{t^2+1})$ が成り立つ. これは $t^2+1 \in ss'\mathbb{Q}^2$ と同値である.

$t^2+1 \in ss'\mathbb{Q}^2$ と仮定する. このとき, $\mathbb{Q}(\sqrt{ss'}) = \mathbb{Q}(\sqrt{t^2+1})$ が成り立つ. $ss' \notin \mathbb{Q}^2$ より $t^2+1 \notin \mathbb{Q}^2$ であるから, 補題 2.2 より $\sqrt{ss'} \in K_{s,t}$. よって, $K_{s',t} \subseteq K_{s,t}$. 逆の包含関係も同様にして示せる. $\square$

注意 2.6. $s = s'$ の場合, $K_{s,t} = K_{s',t}$ であるが, 条件 $ss' \notin \mathbb{Q}^2$ は成り立たない.

さて, 命題 2.4 より, $K_{s,t}$, $K_{2s,t}$ は巡回 4 次体である. 補題 2.2 より, ともに 2 次体 $\mathbb{Q}(\sqrt{t^2+1})$ を含む.

補題 2.7. t を整数とし, $t \equiv 3 \text{ or } 5 \pmod 8$ を満たすとする. このとき, $t^2+1 \notin 2\mathbb{Q}^2$.

証明. t を $t \equiv 3 \text{ or } 5 \pmod 8$ を満たす整数とする. $t^2+1 \in 2\mathbb{Q}^2$ と仮定する. ある $q \in \mathbb{Q}$ が存在して, $t^2+1 = 2q^2$ と表せる. また, q は既約分数によって以下のように表せる:

$$q = \frac{m}{n}, \quad \gcd(m,n) = 1, \quad n > 0.$$

すると,

$$t^2+1 = 2\cdot\left(\frac{m}{n}\right)^2$$

となる. 両辺を n^2 倍し, さらに 2 で割ると,

$$\frac{t^2+1}{2}\cdot n^2 = m^2.$$

t は奇数であるから, 左辺の $(t^2+1)/2$ は整数である. $\gcd(m,n) = 1$ なので, n に素因数 p があれば $p^2 \mid m^2$ となり $p \mid m$ となって矛盾が生じる. よって $n = \pm 1$ であるが, q の既約分数による表し方から $n = 1$ である. したがって,

$$\frac{t^2+1}{2} = m^2.$$

一方, $t \equiv 3$ or $5 \pmod 8$ であるから, $t^2 \equiv 9 \pmod{16}$. よって,

$$\frac{t^2+1}{2} \equiv \frac{10}{2} \equiv 5 \pmod 8.$$

ゆえに,

$$m^2 \equiv 5 \pmod 8.$$

ところが, 整数を 2 乗したものが法 8 でとりうる値は 0, 1, 4 だけである. これは矛盾である. したがって, $t^2+1 \notin 2\mathbb{Q}^2$ でなければならない. $\square$

命題 2.8. s, t を整数とし, $t \equiv 3$ or $5 \pmod 8$ を満たすとする. このとき, $K_{s,t} \neq K_{2s,t}$.

証明. $s' = 2s$ とおくと, $ss'\mathbb{Q}^2 = 2s^2\mathbb{Q}^2 = 2\mathbb{Q}^2$. 補題 2.7 より, $t^2+1 \notin ss'\mathbb{Q}^2$. 補題 2.5 より, 求める結果が得られる. $\square$

3 巡回 4 次体の判別式の一致

巡回 4 次体の判別式に関する次の結果は, Huard, Spearman and Williams [5], Corollary 4 から抜粋したものである:

定理 3.1. a, b, c を整数とし, c と $\gcd(a,b)$ は square-free と仮定する. また, 次の条件 (a), (b) のどちらかを満たすと仮定する:

(a) $a \equiv 4 \pmod 8$, $b \equiv 2 \pmod 4$, $c \equiv 2 \pmod 8$,

(b) $a \equiv 2 \pmod 4$, $b \equiv 1 \pmod 2$, $c \equiv 2 \pmod 8$.

もし $\mathbb{Q}(\sqrt{a+b\sqrt{c}})$ が巡回 4 次体ならば, その判別式は

$$2^8 \cdot \frac{\gcd(a,b)^2 \cdot c^3}{\gcd(a,b,c)^2}.$$

命題 3.2. t を整数とし, $t \equiv 1 \pmod 2$ を満たすとする. s を整数とし, square-free かつ $\gcd(s, t^2+1) = 1$ を満たすとする.

このとき, $K_{s,t}$, $K_{2s,t}$, $K_{-s,t}$, $K_{-2s,t}$ は同じ判別式をもつ. さらに, 以下が成り立つ:

(i) 判別式の 2-指数は 11 である.

(ii) 任意の奇素数 p に対して, $p \mid s$ ならば, 判別式の p-指数は 2 である.

(iii) 任意の奇素数 q に対して, $q \nmid s$ かつ $q \nmid t^2+1$ ならば, 判別式の q-指数は 0 である.

証明. $K_{s,t}$, $K_{2s,t}$ についてのみ証明するが, $K_{-s,t}$, $K_{-2s,t}$ についても全く同様である. まず,

$$K_{s,t} = \mathbb{Q}\left(\sqrt{s(t^2+1)+s\sqrt{t^2+1}}\right),$$
$$K_{2s,t} = \mathbb{Q}\left(\sqrt{2s(t^2+1)+2s\sqrt{t^2+1}}\right)$$

である. また, ある正の整数 y, m が存在して,

$$t^2+1 = y^2 m, \quad m \text{ は square-free.}$$

さらに, ある正の整数 x, n が存在して,

$$y = x^2 n, \quad n \text{ は square-free}$$

と書ける. ゆえに,

$$t^2 + 1 = x^4 n^2 m$$

が成り立つ. したがって,

$$\begin{aligned}\sqrt{s(t^2+1) + s\sqrt{t^2+1}} &= x\sqrt{sx^2n^2m + sn\sqrt{m}},\\ \sqrt{2s(t^2+1) + 2s\sqrt{t^2+1}} &= x\sqrt{2sx^2n^2m + 2sn\sqrt{m}}.\end{aligned}$$

すなわち,

$$\begin{aligned}K_{s,t} &= \mathbb{Q}\left(\sqrt{sx^2n^2m + sn\sqrt{m}}\right),\\ K_{2s,t} &= \mathbb{Q}\left(\sqrt{2sx^2n^2m + 2sn\sqrt{m}}\right).\end{aligned}$$

$t \equiv 1 \pmod 2$ より $t^2 + 1 \equiv 2 \pmod 8$ であるから, t^2+1 の 2-指数は 1 である. よって,

$$x^4n^2 = y^2 \equiv 1, \quad m \equiv 2 \pmod 8.$$

したがって, x, n は奇数, m は偶数である.
　さて, $a = sx^2n^2m$, $b = sn$, $c = m$ とおくと,

$$\begin{aligned}\gcd(a,b) &= sn,\\ \gcd(a,b,c) &= \gcd(\gcd(a,b),c) = \gcd(m,sn).\end{aligned}$$

s に関する仮定により, $\gcd(a,b)$ は square-free であり, $\gcd(m,sn) = \gcd(m,n)$ である. 定理 3.1 より $K_{s,t}$ の判別式は $2^8s^2n^2m^3/\gcd(m,n)^2$ である.
　次に, $a = 2sx^2n^2m$, $b = 2sn$, $c = m$ とおくと,

$$\begin{aligned}\gcd(a,b) &= 2sn,\\ \gcd(a,b,c) &= \gcd(\gcd(a,b),c) = \gcd(m,2sn).\end{aligned}$$

s に関する仮定により, $\gcd(a,b)$ は square-free である. また, m の 2-指数は 1 であり, s, n は奇数であるから,

$$\gcd(m,2sn) = 2\cdot\gcd(m/2,sn) = 2\cdot\gcd(m,sn) = 2\cdot\gcd(m,n).$$

定理 3.1 より $K_{2s,t}$ の判別式もまた $2^8s^2n^2m^3/\gcd(m,n)^2$ である.
　条件 (i), (ii), (iii) は, 判別式の具体的な形から明らかである. 特に, 条件 (iii) について, もし素数 p が $n^2m^3/\gcd(m,n)^2$ を割れば p は t^2+1 を割ることに注意せよ. □

系 3.3. 同じ判別式をもつ異なる実の巡回 4 次体のペアが無限に多く存在する. 虚の場合も同様.

証明. $t \equiv 3$ or $t \equiv 5 \pmod 8$ を満たす整数 t を 1 つとって固定する. p を t^2+1 より大きい奇素数とする. $K_{p,t}$, $K_{2p,t}$ は, 定義から明らかに実である. 命題 2.8 より, $K_{p,t} \neq K_{2p,t}$ である. p は square-free かつ $\gcd(p, t^2+1) = 1$ が成り立つ. 命題 3.2 より, $K_{p,t}$, $K_{2p,t}$ は同じ判別式をもつ. p が異なれば判別式が異なるから, ペアの重複は起こらない.

虚の巡回 4 次体のペア $K_{-p,t}$, $K_{-2p,t}$ についても同様である. □

注意 3.4. $t \equiv 1 \pmod 2$ を満たす t を 1 つとって固定し, t^2+1 より大きい奇素数 p に対して $K_{p,t}$, $K_{-p,t}$ を考えれば, 同じ判別式をもつ実と虚の巡回 4 次体のペアが無限に多く存在することは明らかである.

4 CM 体の単数基準と主結果の証明

この節では, K を CM 体, K^+ を K の最大実部分体とする. $E(K)$ は部分群 $W(K)E(K^+)$ をもつ. Q を $E(K)$ における $W(K)E(K^+)$ の指数とする. n を K の $\mathbb{Q}$ 上の拡大次数, r を K の単数群の自由部分の階数とする. K は総虚だから,

$$r = \frac{n}{2} - 1$$

が成り立つ. Washington [17], Proposition 4.16 によれば, CM 体とその最大実部分体の単数基準の比について, 等式

$$Q \cdot \mathrm{reg}(K) = 2^r \cdot \mathrm{reg}(K^+)$$

が成り立つ. さらに, Washington [17], Theorem 4.12 によれば, $Q = 1$ or 2 である. Remak [14], §3 によれば, 最大実部分体 K^+ が与えられたとき, $Q = 2$ を満たす CM 体 K は有限個しかない. 以下の定理は, $Q = 1$ になるための十分条件を与える:

定理 4.1 (Nakamura [10], §2.4, Lemma 1)**.** もし $\mathrm{disc}(K)/\mathrm{disc}(K^+)^2$ が 2^n を割り切らないならば, $Q = 1$.

この定理を用いて, 主結果の証明を述べる.

定理 1.2 の証明. $K_{-p,t}$, $K_{-2p,t}$ は, 命題 2.4 より巡回 4 次体であり, 定義から明らかに虚である. 命題 2.8 より, $K_{-p,t} \neq K_{-2p,t}$ である. p は square-free かつ $\gcd(p, t^2+1) = 1$ が成り立つ. 命題 3.2 より, $K_{-p,t}$, $K_{-2p,t}$ は同じ判別式をもつ. 補題 2.2 より, それらは同じ最大実部分体をもつ. それらは CM 体であるから, 定理 4.1 より, それらは同じ単数基準をもつ. これで証明が完了した. □

最後に, 判別式, 単数基準, 類数がすべて一致する, 虚の巡回 4 次体のペアの例を挙げる. 基本単数の計算は次の補題 4.2 を用いる. 類数の計算は Magma [1] を用いる.

補題 4.2. t を t^2+1 が square-free であるような奇数とする. このとき, $t + \sqrt{t^2+1}$ は 2 次体 $\mathbb{Q}(\sqrt{t^2+1})$ の基本単数である.

証明. t を t^2+1 が square-free であるような奇数とする. Pell 方程式 $X^2 - (t^2+1)Y^2 = -1$ の最小正整数解は $(X, Y) = (t, 1)$ であり, かつ $t^2+1 \equiv 2 \pmod 4$. ゆえに, $t + \sqrt{t^2+1}$ は 2 次体 $\mathbb{Q}(\sqrt{t^2+1})$ の基本単数である. □

例 4.3. 巡回 4 次体のペア $K_{-3,35}$, $K_{-6,35}$ を考える．これらは共通の最大実部分体 $\mathbb{Q}(\sqrt{2\cdot 613})$ をもつ．その基本単数は $\varepsilon = 35+\sqrt{2\cdot 613}$ である．

判別式はともに $2^{11}\cdot 3^2\cdot 613^3$ である．単数基準はともに $2\cdot\log|\varepsilon| = 8.4973985\cdots$ である．類数はともに $2^3\cdot 5^2\cdot 97$ である．

本報告集では詳細を触れていないが, 虚の双 2 次体のペアで, 判別式, 単数基準, 類数がすべて一致する例もあげることが出来る:

例 4.4. 双 2 次体のペア $B_{-21,10}$, $B_{-42,10}$ を考える．これらは共通の最大実部分体 $\mathbb{Q}(\sqrt{10})$ をもつ．その基本単数は $\varepsilon = 3+\sqrt{10}$ である．判別式はともに $2^8\cdot 3^2\cdot 5^2\cdot 7^2$ である．単数基準はともに $2\cdot\log|\varepsilon| = 3.6368929\cdots$ である．類数はともに 32 である．

謝辞

講演の機会を与えて下さった世話人の方々に感謝を申し上げます.

参考文献

[1] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265.

[2] L. Carlitz, A characterization of algebraic number fields with class number two, Proc. Amer. Math. Soc. **11** (1960), 391–392.

[3] S. T. Chapman and W. W. Smith, On a characterization of algebraic number fields with class number less than three, J. Algebra **135** (1990), no. 2, 381–387.

[4] F. Gassmann, Bemerkungen zur vorstehenden Arbeit von Hurwitz, Math. Z. **25** (1926), 665–675.

[5] J. S. Huard, B. K. Spearman and K. S. Williams, Integral bases for quartic fields with quadratic subfields, J. Number Theory **51** (1995), no. 1, 87–102.

[6] C. U. Jensen, A. Ledet and N. Yui, Generic polynomials. Constructive aspects of the inverse Galois problem, Math. Sci. Res. Inst. Publ., 45, Cambridge University Press, Cambridge, 2002.

[7] K. Komatsu, On the adele rings and zeta-functions of algebraic number fields, Kodai Math. J. **1** (1978), no. 3, 394–400.

[8] U. Krause, A characterization of algebraic number fields with cyclic class group of prime power order, Math. Z. **186** (1984), 143–148.

[9] T. Nagell, Zur Arithmetik der Polynome, Abh. Math. Sem. Hamburg **1** (1922), 178–193.

[10] K. Nakamura, Certain quartic fields with small regulators, J. Number Theory **57** (1996), no. 1, 1–21.

[11] J. Neukirch, Kennzeichnung der endlich-algebraischen Zahlkörper durch die Galoisgruppe der maximal auflösbaren Erweiterungen, J. Reine Angew. Math. **238** (1969), 135–147.

[12] R. Perlis, On the equation $\zeta_K(s) = \zeta_{K'}(s)$, J. Number Theory **9** (1977), 342–360.

[13] R. Perlis, On the class numbers of arithmetically equivalent fields, J. Number Theory **10** (1978), 489–509.

[14] R. Remak, Über algebraische Zahlkörper mit schwachem Einheitsdefekt, Compos. Math. **12** (1954), 35–80.

[15] D. E. Rush, An arithmetic characterization of algebraic number fields with a given class group, Math. Proc. Cambridge Philos. Soc. **94** (1983), 23–28.

[16] K. Uchida, Isomorphisms of Galois groups, J. Math. Soc. Japan **28** (1976), 617–620.

[17] L. C. Washington, Introduction to Cyclotomic Fields, 2nd ed., Graduate Texts in Mathematics, 83, Springer-Verlag, New York, 1996.