

3 次体の 3 次不分岐巡回拡大の構成

都立大・理 尾台 喜孝 (Yoshitaka Odaj)

良く知られているように、2 次体の 2 次不分岐拡大は Gauss の genus theory によって容易に構成される。そこでここでは 3 次体の 3 次不分岐巡回拡大の構成について考察する。2 次体の場合は 2 次不分岐拡大はすべて genus field に含まれるので話が簡単に済んだ。3 次体の場合でも genus field に含まれる 3 次不分岐巡回拡大は構成方法が知られている。([2]) しかし genus field に含まれないものが存在するので、それらの構成が問題になる。この問題に対して、elementary な方法である程度の結果を得たので以下に報告する。なお純 3 次体の場合については既に [4] に発表した。

記号

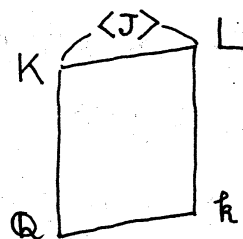
K : 実 3 次体

$$k = \mathbb{Q}(\zeta), \quad \zeta = \exp(2\pi i/3)$$

$$L = K\bar{k}$$

$$\text{Gal}(L/K) = \langle J \rangle$$

J : complex conjugate mapping



§1. 3次体一般

Lemma A: K の 3 次不分岐巡回拡大すべての集合.

B : L の 3 次不分岐巡回拡大で K 上 abel なものすべての集合.

B の元は Kummer 理論より. $L(\sqrt[3]{\alpha})$, $\alpha \in L^\times$ と書けるが、このとき写像

$$\rho: B \ni L(\sqrt[3]{\alpha}) \longrightarrow K(\text{Re } \sqrt[3]{\alpha}) \quad \text{Re } *: * \text{ の実部}$$

は B から A の上への全単射になる。

Proof. $L(\sqrt[3]{\alpha})$ に $L(\sqrt[3]{\alpha})/K$ の 3 次中間体を対応させる写像が B から A の上への全単射になることはすぐわかる。従って、 $[K(\text{Re } \sqrt[3]{\alpha}):K] = 3$ を示せばよい。

$L(\sqrt[3]{\alpha})/K$ abel $\Rightarrow \alpha^{1+J} \in (L^\times)^3 \Rightarrow (\sqrt[3]{\alpha})^{1+J} \in L \cap \bar{L} = K$
 よって、 $\sqrt[3]{\alpha} + \sqrt[3]{\alpha}^J = 2 \text{Re } \sqrt[3]{\alpha}$ に注意すれば、 $\sqrt[3]{\alpha}$ は $K(\text{Re } \sqrt[3]{\alpha})$ 上 2 次。これより $[K(\text{Re } \sqrt[3]{\alpha}):K] = 3$ が従う。

Theorem 1 K の 3 次不分岐巡回拡大は K に $\text{Re } \sqrt[3]{\alpha}$ を添加

して得られる。但し α は次の条件を満たす L^x の元：

$$0. \alpha \notin (L^x)^3$$

I. (i) α はイデアルとして立方

(ii) α は $\text{mod } (1-\zeta)^3$ で立方剰余

$$\text{II. } \alpha^{1+j} \in (L^x)^3$$

Proof. Lemma より B を求めればよい。 B の元の条件を Kummer 拡大の理論で書き直せば条件 0~II になる。

これで K の 3 次不分岐巡回拡大を構成することは、 L^x の元で条件 0~II を満たすものを捜すことに帰着された。

Remark 1 α は $L^x / (L^x)^3$ の元と思ってよい。

$$\odot \alpha' = \alpha \beta^3 \Rightarrow L(\sqrt[3]{\alpha}) = L(\sqrt[3]{\alpha'}) \Rightarrow K(\text{Re } \sqrt[3]{\alpha}) = K(\text{Re } \sqrt[3]{\alpha'}) .$$

Remark 2 $H = \{ \mathfrak{h} : L \text{ のイデアル類} \mid \mathfrak{h}^3 = 1 \}$

明らかに、 α が I(i) を満たす $\Leftrightarrow (\alpha) = \alpha^3, \alpha \in \mathfrak{h} \in H$

これより H と L の単数群 E_L がわかれば I(i) を満たす α がわかる。しかも H と E_L / E_L^3 は有限ゆえ、そういう α は有限個。

Remark 3 $H^- = \{ \mathfrak{h} \in H \mid \mathfrak{h}^j = \mathfrak{h}^{-1} \}$

すると、 α が I(i), II を満たす $\Rightarrow (\alpha) = \alpha^3, \alpha \in \mathfrak{h} \in H^-$

$$\odot \alpha^{1+j} \in (L^x)^3 \Rightarrow \alpha^{1+j} \text{ が単項} \Rightarrow \mathfrak{h}^{1+j} = 1 .$$

§2. 巡回3次体及び純3次体の場合

まず純3次体の定義:

$$K \text{ が純3次体} \iff K = \mathbb{Q}(\sqrt[3]{m}), \exists m \in \mathbb{Z}$$

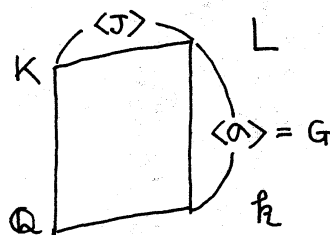
3次体に関して次の事実は良く知られている:

$$L/\mathbb{Q} \text{ が巡回拡大} \iff K \text{ が巡回3次体又は純3次体}$$

以下この§では, K は 巡回3次体又は純3次体 と仮定する。

$$G = \text{Gal}(L/\mathbb{Q})$$

の: G の生成元



Theorem 2 M : K の genus field (i.e. K の絶対類体の最大絶対アーベル部分体と K との合成体)

K の3次不分岐巡回拡大 $K(\sqrt[3]{\Delta})$ が M に含まれないための必要十分条件は.

$$\text{III. } \alpha^{\alpha-1} \notin (L^\times)^3$$

Proof. genus field の定義とガロア群の群論的考察により.

$$K(\sqrt[3]{\Delta}) \subset M \iff L(\sqrt[3]{\Delta})/\mathbb{Q} \text{ abel}$$

$$\text{Kummer 拡大の理論より, } L(\sqrt[3]{\Delta})/\mathbb{Q} \text{ abel} \iff \alpha^{\alpha-1} \in (L^\times)^3$$

さて、§1のRemark 2で注意したように

$$H = \{ \mathfrak{h} : L \text{ のイデアル類} \mid \mathfrak{h}^3 = 1 \}$$

が問題になる。 $\mathcal{H}$ を L のイデアル類群の 3-Sylow subgroup とする。 $\mathcal{H}$ は $\mathbb{Z}[G]$ -module ゆえ

$$\mathcal{H}_i := \{ \mathfrak{h} \in \mathcal{H} \mid \mathfrak{h}^{(\sigma-1)^i} = 1 \} \quad i \in \mathbb{N} \cup \{0\}$$

が定義できる。 $\mathfrak{h}$ の類数が 1 であることより

$$\mathcal{H}_2 = H$$

$$\cup$$

$\mathcal{H}_1$: $\mathfrak{h}$ に関する特異類群

$$\cup$$

$$\mathcal{H}_0 = \{1\}$$

が証明される。

さらに $i = 0, 1, 2$ に対して

F_i : K の 3 次不分岐巡回拡大で、 $\mathcal{H}_i$ からつくられるものすべての合成体。

但し、“ $\mathcal{H}_i$ からつくられる” とは、Th1 の α が

$(\alpha) = \sigma^3$, $\sigma \in \mathfrak{h} \in \mathcal{H}_i$ なるときにいう。

と定義する。すると、§1のRemark 2より

F_2 : K の 3 次不分岐巡回拡大すべての合成体

$$\cup$$

F_1

$$\cup$$

F_0 : $\alpha \in E_L$ なるものすべての合成体

となる。

また、 L の $\mathfrak{f}$ に関する特異イデアルを含む類のなす群を $\mathcal{H}_i^0$ と書き、 F_i^0 を F_i と同様に定義する。

$$\mathcal{H}_0 \subset \mathcal{H}_i^0 \subset \mathcal{H}_1, \quad F_0 \subset F_i^0 \subset F_1.$$

Gras により $\mathcal{H}_2$ を求めるアルゴリズムが得られている。([1])
しかし、実行するには途中の Norm 方程式の部分はかなり大変である。そこで、ここでは F_2 はあきらめて、 F_0, F_i^0, F_1 について考察する。

Proposition 3 $M: K$ の genus field

$$F_i^0 = F_0 M$$

さらに、-part を § 1. Remark 3 のように定義すれば、

$$\mathcal{H}_1^- = \mathcal{H}_i^0^- \Rightarrow F_1 = F_0 M$$

Proof. (概略)

$p_1, \dots, p_s, q_1, \dots, q_t: K$ で分岐する有理素数, $p_i \equiv 1, q_i \equiv -1 \pmod{3}$

$$p_i = \pi_i^{1+2j} \quad \pi_i: \mathfrak{f} \text{ の素元}, \equiv 1 \pmod{3}$$

$\pi := \sqrt{-3}$ if $L/\mathfrak{f}$ で $(\sqrt{-3})$ が分岐

すると、 π_i, π_i^j, q_i, π が $L/\mathfrak{f}$ で分岐する $\mathfrak{f}$ の prime 全部。

1st step. $M = K \left(\mathfrak{f}_0 \sqrt[3]{\pi_i^{1+2j}} \mid i=1, \dots, s \right)$ を証明する。

2nd step. $\mathcal{H}_i^0$ が L の $\mathfrak{f}$ 上分岐する素イデアルを含む類のなす群と一致することを証明する。

3rd step § 1. Remark 3 より F_i^0 を求めるには

$$(\alpha) = \alpha^3, \alpha \in \mathfrak{h} \in \mathcal{H}_i^-$$

なることを考えればよい。(よって、 $\mathcal{H}_i^- = \mathcal{H}_i^0 \Rightarrow F_i = F_i^0$)

すると 2nd step の結果より

$$\alpha = \varepsilon \prod \pi_i^{a_i + b_i J} \cdot \prod q_j^{c_j} \cdot \pi^d, \quad \varepsilon \in E_L, a_i, b_i, c_j, d \in \mathbb{Z}/3\mathbb{Z}$$

さらに条件 II を満たすためには、 $b_i = 2a_i, c_j = d = 0$ 。

$$\therefore \alpha = \varepsilon \prod (\pi_i^{1+2J})^{a_i}$$

1st step の結果と比べて Prop. を得る。

Corollary K が巡回 3 次体のとき、導手を m とする。

m が (1) または (2) を満たせば $F_i = F_0 M$

$$(1) \exists p: \text{prime s.t. } p|m, p \neq 3, p \not\equiv 1 \pmod{9}$$

$$(2) m = 9$$

K が純 3 次体のときは常に $F_i = F_0 M$

Proof. $A = \mathcal{H}_1 / \mathcal{H}_i^0, B = (E_K \cap \text{Nul}_K L^\times) / \text{Nul}_K E_L$

$A^\pm = \{ \mathfrak{h} \in A \mid \mathfrak{h}^J = \mathfrak{h}^{\pm 1} \}$, $B^\pm$ も同様に定義。(複号同順)

$A \ni \mathfrak{h}$ に対し、 $\mathfrak{h} \ni \alpha, \alpha^{\sigma^{-1}} = (\alpha), \text{Nul}_K \alpha = \varepsilon$ で決まる ε を

対応させることにより $A \cong B$ となる。 K が巡回のときは σJ

$= J$ のゆえ $A^- \cong B^-$ 。よって、 $A^- = \{1\} \Leftrightarrow B^- = \{1\} \Leftrightarrow 3 \notin \text{Nul}_K L^\times$

$\Leftrightarrow m$ が (1) または (2) を満たす。 K が純のときは $\sigma J = J \sigma^2$ のゆえ

$A \cong B^+$ 。よって、 $A^- = \{1\} \Leftrightarrow B^+ = \{1\}$ 。これは常に 0, K ..

従って Prop. 3 より Cor. が証明される。

Remark 講演では K が巡回3次体のときも含めて常に $F_1 = F_0 M$ であると述べたが、それは言い過ぎだった。現在証明できているのは Cor. まで。

Prop. 3 より、 F_0 、特に F_0 のうち M に含まれない部分が問題になる。すなわち E_L の元で条件 0 ~ III (Th2) を満たすものが問題になる。巡回3次体と純3次体に分けて考察する。

E_* : $*$ の単数群, W_* : $*$ の 1 の根の群

巡回3次体 L は虚巡回体ゆえ

$$E_L = E_K W_L = E_K W_K \quad \text{if } K \text{ の導手} \neq 9$$

$W_i^{1+j} = W_i^{a-1} = 1$ に注意すれば、 E_L の元で II と III を同時に満たすものが存在しないことがわかる。

$$\therefore F_0 \subset M \quad (K \text{ の導手が } 9 \text{ のときも } K = F_0 = M)$$

純3次体 ([4]) e : K の基本単数で norm が 1 のもの。

$x^{1-a} = e$ が E_L 内で解を持たないときを Case 1, 持つときを Case 2, そのときの解の 1 つを ε とする。

Case 1. L の基本単数系として $\{e, e^a\}$ がとれる。

従って、 $\sum a e^{b+ca}$ ($a, b, c \in \mathbb{Z}/3\mathbb{Z}$) について条件をみればよい。 $\sum a = a^2 \sum$, $e^3 = e$, $e^{a^2} = e^{-1-a}$ に注意して計算してみると、II と III を同時に満たすものは存在しない。

$$\therefore F_0 \subset M$$

Case 2. L の基本単数系として $\{\varepsilon, \varepsilon^\alpha\}$ がとれる。

$\varepsilon^{1-\alpha} = e$ より $\varepsilon^J = \pm \varepsilon^{-\alpha}$ がわかるので、これと $\varepsilon^{\alpha^2} = \varepsilon^{-1-\alpha} \eta$ ($\eta \in W_E$) に注意して計算してみると、 $\zeta^a \varepsilon^{1+\alpha}$ だけが II と III を同時に満たす。(もちろん 0, I(i) も満たす。) I(ii) の判定は局所体の中での素元による展開を用いて容易にできる。特に $\zeta^a \varepsilon^{1+\alpha}$ を満たさないので、 $\zeta^a \varepsilon^{1+\alpha}$ のうち I(ii) を満たすのはせいぜい 1 個

以上まとめて：

Theorem 4 K が巡回 3 次体： $F_0 = M$

導手 m が Cor. の条件を満たせば、 $F_1 = M$

K が純 3 次体：Case 1, 2, ε を上と同じとする。

Case 1. $F_1 = M$

Case 2. $U := \{ \zeta^a \varepsilon^{1+\alpha} (a=0,1,2) \text{ のうち I(ii) を満たすもの } \}$

$$\# U \leq 1, \quad \begin{cases} U = \emptyset \Rightarrow F_1 = M \\ U = \{\varepsilon_0\} \Rightarrow F_1 = M(\mathbb{R} \sqrt[3]{\varepsilon_0}) \neq M \end{cases}$$

例

$K = \mathbb{Q}(\sqrt[3]{m}) \quad m \in \mathbb{Z}, > 0, \text{ cube free}$

$$(*) \quad m = D^3 + d, \quad D, d \in \mathbb{Z}, D > 0, d \mid 3D^2$$

$$(D, d) \neq (1, 1), (2, 1), (1, 3), (2, -6), (5, -25), (2, -4)$$

とすると、

$$\begin{cases} d = \pm 1 \Rightarrow \text{Case 1} \\ d \neq \pm 1 \Rightarrow \text{Case 2, } \varepsilon = (\sqrt[3]{m} - D)^{1-\alpha^2} \end{cases}$$

I(ii)の判定を行なって次のProp.を得る:

Proposition 5 ([4]) K が純3次体で(*)を満たしていて、さらに $d \neq \pm 1$ とする。 $\varepsilon = (\sqrt[3]{m} - D)^{1-\alpha^2}$ とおく。このとき Th.4のUは次のようになる:

	$3 \nmid m$	$3 \parallel m$	$3^2 \parallel m$
$3 \nmid D$	$\begin{smallmatrix} * \\ (1) \end{smallmatrix}$	$\emptyset$	$\begin{smallmatrix} * \\ (2) \end{smallmatrix}$
$3 \parallel D$	$\{\zeta \varepsilon^{1+\alpha}\}$	$\begin{smallmatrix} * \\ (3) \end{smallmatrix}$	$\emptyset$
$3^2 \mid D$	$\{\zeta \varepsilon^{1+\alpha}\}$		

(1)	$m \backslash$	$3 \nmid d$	$3 \mid d$
	$\pm 1 \bmod 3^2$	$\emptyset$	$\emptyset$
	$\pm 2 \text{ "}$	$\{\varepsilon^{1+\alpha}\}$	
	$\pm 4 \text{ "}$	$\{\zeta \varepsilon^{1+\alpha}\}$	

$$(2) \begin{cases} m/3^2 \equiv D \bmod 3 \Rightarrow \{\zeta^2 \varepsilon^{1+\alpha}\} \\ m/3^2 \equiv -D \bmod 3 \Rightarrow \{\zeta \varepsilon^{1+\alpha}\} \end{cases}$$

$$(3) \begin{cases} m/3 \equiv D/3 \bmod 3 \Rightarrow \{\zeta^2 \varepsilon^{1+\alpha}\} \\ m/3 \equiv -D/3 \bmod 3 \Rightarrow \{\varepsilon^{1+\alpha}\} \end{cases}$$

Remark このProp.より、genus fieldに含まれない3次不分岐巡回拡大を構成できる3次体の例が無限個得られる。

数値例 (1) Prop. 5 に属する例。 $U \neq \emptyset$ なるもの:

m	30	68	130	204	210
D	3	4	5	6	6
d	3	4	5	-12	-6
U	$\{\zeta^2 \varepsilon^{140}\}$	$\{\zeta \varepsilon^{140}\}$	$\{\zeta \varepsilon^{140}\}$	$\{\zeta^2 \varepsilon^{140}\}$	$\{\varepsilon^{140}\}$

(2) Prop. 5 に属さない例.

$$m = 34 \quad \varepsilon = 305 + 94\sqrt[3]{34} + 29\sqrt[3]{34}^2 - 52\zeta - 16\sqrt[3]{34}\zeta - 5\sqrt[3]{34}^2\zeta$$

$$U = \{\varepsilon^{140}\}$$

§3. 巡回3次体でも純3次体でもない場合

最後に、講演では触れることができなかったが、 K が 巡回3次体でも純3次体でもない場合 について述べる。この場合 §2 の最初で述べたように、 $L/\mathbb{Q}$ は Galois 拡大にならず、§2 の議論は成り立たない。ここでは小規模な変更で対応する結果が得られる部分について報告する。証明方法は主張を見ればだいたい想像がつくと思うので省略する。

まず、Th. 2 に対応する結果:

Theorem 2' D_K : K の判別式, $\hat{L} = L(\sqrt[3]{D_K})$, $\hat{\mathbb{Q}} = \mathbb{Q}(\sqrt[3]{D_K})$,

の: $\text{Gal}(\tilde{L}/\tilde{K})$ の生成元。 K の 3 次不分岐巡回拡大 $K(\sqrt[3]{\alpha})$ が genus field M に含まれないための必要十分条件は,

$$\text{III}'. \alpha^{n-1} \notin (\tilde{L}^\times)^3$$

$\mathcal{H}_i, \mathcal{H}_i^0, F_i, F_i^0$ は §2 のように定義することはできないが、 $\mathcal{H}_0 := \{1\}$ と定義すれば F_0 は定義できる。

Theorem 4' K が総実: $F_0 \subset M$

K が非総実: $\{u \in E_L \mid N_{L/K}(u) = \pm 1\} = W_L \cdot \langle \varepsilon \rangle$ なる ε が存在する。 ε が条件 III' を満たさないときを Case 1, 満たすときを Case 2 とする。

Case 1. $F_0 \subset M$

Case 2. $U = \{ \zeta^a \varepsilon \ (a=0,1,2) \text{ のうち } I(\text{ii}) \text{ を満たすもの} \}$

$$\begin{cases} U = \emptyset & \Rightarrow F_0 \subset M \\ U \ni \varepsilon_0 & \Rightarrow F_0 \not\subset M, F_0 \subset M(\sqrt[3]{\alpha}) \end{cases}$$

Remark ε を求め, 同時に ε が III' を満たすかどうかの判定をするアルゴリズムが得られている。([3])

例 Prop. 5 のような系列例は得られていないが, [3] のアルゴリズムを, コンピューターを用いて実行することによっ

て次の例が得られた。

$K = \mathbb{Q}(\theta)$ $\theta : X^3 - 6X^2 + 24X - 12 = 0$ の実根.

$\varepsilon : X^3 - 3(-27+55\sqrt{5})X^2 + 3(-82-55\sqrt{5})X - 1 = 0$ の絶対値 1 の根.

$$\zeta^2 \varepsilon \in U$$

参考文献

- [1] G. Gras, Sur les l -classes d'ideaux dans les extensions cycliques relatives de degré premier l , Ann. Inst. Fourier 23, 3, (1973), 1-48, 23, 4, (1973), 1-44.
- [2] M. Ishida, The genus fields of algebraic number fields, Lecture Notes in Math., 555, Springer, Berlin-Heidelberg-New York, 1976.
- [3] K. Nakamura, Class number calculation of a sextic field from the elliptic unit, Acta Arith. XLV (1985), 229-247.
- [4] Y. Odaï, Some unramified cyclic cubic extensions of pure cubic fields, Tokyo J. Math. 7, (1984), 391-398.