冪根を含まない体のクンマー理論について*

木田雅成

概 要

第 27 回サマースクールでの講演の報告である．代数的トーラスを使って，冪根のない体にクンマー理論を拡張することを解説した．

1　理論的な枠組み

k を体とする．$\bar{k}$ を k の分離閉包とし，一つ固定する．m を k の標数と互いに素な 2 以上の整数とする．$k^\times$ が 1 の m 乗根の群 μ_m を含むと仮定する．完全系列

$$1 \longrightarrow \mu_m \longrightarrow \bar{k}^\times \overset{m\text{ 乗写像}}{\longrightarrow} \bar{k}^\times \longrightarrow 1$$

から，ガロア・コホモロジーをとることによって，

$$\begin{array}{ccccc} 1 & \longrightarrow & k^\times/(k^\times)^m & \longrightarrow & \mathrm{H}^1(k,\mu_m) \\ & & & & \| \\ & & & & \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\bar{k}/k),\mu_m) \end{array} \longrightarrow \begin{array}{c} \mathrm{H}^1(k,\bar{k}^\times) \\ \| \\ 1 \end{array}$$

がヒルベルトの定理 90 によって得られ，

$$k^\times/(k^\times)^m \cong \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\bar{k}/k),\mu_m)$$

というクンマー双対が得られるというのが古典的なクンマー理論である．これから k の任意の m 次巡回拡大がある $a \in k^\times$ を使って，$k(\sqrt[m]{a})$ と書けることが導かれる．このクンマー理論が代数学，数論に多くの応用を持つことは周知の通りである．

この古典的な場合を乗法群 $\mathbb{G}_{m,k}$ のクンマー理論だと考えて，それを次のような枠組みで一般化することを考えよう．k を体として G/k を可換な代数群とする．まず

(P1)　m 次巡回自己同種写像 $\lambda/k : G \longrightarrow G$ が存在する

*この研究は文部科学省科学研究費補助金基盤研究 (C) (No.15K04798) の援助をうけて行われています．

ことを仮定すると，完全系列

$$1 \longrightarrow \ker(\lambda) \longrightarrow G \xrightarrow{\lambda} G \longrightarrow 1$$

が得られる．ガロア・コホモロジーをとると，

$$1 \longrightarrow G(k)/\lambda G(k) \longrightarrow \mathrm{H}^1(k, \ker(\lambda)(\bar{k})) \longrightarrow \mathrm{H}^1(k, G(\bar{k}))[\lambda]$$

が導かれる．ここで $\mathrm{H}^1(k, G(\bar{k}))[\lambda]$ は λ が $\mathrm{H}^1(k, G(\bar{k}))$ に引き起こす自己準同型の核である．ここでさらに

$$\text{(P2)} \quad \ker(\lambda)(\bar{k}) = \ker(\lambda)(k)$$

ならば

$$\mathrm{H}^1(k, \ker(\lambda)(\bar{k})) \cong \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\bar{k}/k), \ker(\lambda)(\bar{k}))$$

となる．さらに

$$\text{(P3) 弱ヒルベルト 90} \quad \mathrm{H}^1(k, G(\bar{k}))[\lambda] = 1$$

が成り立てば，最終的にクンマー双対

$$G(k)/\lambda G(k) \cong \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\bar{k}/k), \ker(\lambda)(\bar{k}))$$

を得ることができる．この同型はコホモロジーの連結準同型から誘導されるものであり，具体的には次のように与えられる．$P \in G(k)$ に対し，$\lambda(Q) = P$ をみたす $Q \in G(\bar{k})$ を選び，P に対応する指標 $\chi_P \in \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\bar{k}/k), \ker(\lambda)(\bar{k}))$ を $\tau \in \mathrm{Gal}(\bar{k}/k)$ に対し，$\chi_P(\tau) = Q^{\tau-1}$ とする．これから，古典的な場合と同様に，k の任意の m 次巡回拡大は $k(Q) = k(\lambda^{-1}(P))$ の形に書けることがわかる．もし体 k が冪根を含まないようにとれれば，冪根を含まない体についてもクンマー理論が成り立つことになる．

これまで，中心的に研究されてきたのは代数群 G が代数的トーラスの場合で，次の場合に，拡大体 K/k をうまく選ぶと，上記の (P1),(P2),(P3) が成り立つことがわかっている．

(i) ([10]). 乗法群の Weil 制限 $R_{K/k}\mathbb{G}_m$.

(ii) ([13]). M を K/k の中間体とするとき，相対ノルム $N_{K/M} : K^\times \longrightarrow M^\times$ が誘導する写像の核

$$\ker(N_{K/M} : R_{K/k}\mathbb{G}_m \longrightarrow R_{M/k}\mathbb{G}_m).$$

(ii) で $M = k$ とするとき，上のトーラスは $R^{(1)}_{K/k}\mathbb{G}_m$ になり，この場合が [5] で研究された場合である．また，K/k が 2 次拡大で，このトーラスが 1 次元の場合が小松 [15] あるいは小川 [20] で調べられ，一連の研究の発端となった場合である．これらの先行研究については最後の節でまとめて述べることにする．

2　クンマー理論

この節では，前節で述べた条件 (P1), (P2), (P3) がみたされるような状況をどのようにして作り出すかを解説する．(P1), (P2) をみたす λ を作るのが問題である．(P3) に関してはこれが成り立つような代数的トーラスをとるということで解決する．

一般に T を体 k 上定義された代数的トーラスとし，k のガロア拡大体 K で分解するとする．すなわち，$T \times K \cong \mathbb{G}_{m,K}^{\dim T}$. このとき，$T$ の指標加群 $\widehat{T} = \mathrm{Hom}_{K\text{-gr}}(T \times_k K, \mathbb{G}_{m,K})$ は，階数 $\dim T$ の自由 $\mathbb{Z}$ 加群で $G = \mathrm{Gal}(K/k)$ が作用する．T の自己同種写像 λ を見つけたければ，その双対である $\widehat{T}$ の G 自己準同型でその余核が有限になるものを見つければよい．したがって，$\widehat{T}$ を計算して，その G 自己準同型を計算しなければならない．この部分はどのような T をとるかに関わらず必要な計算である．

以下では T として，$R^{(1)}_{K/k}\mathbb{G}_m$ をとり，[13] にしたがって，冪根の含まれない体のクンマー理論の定理を紹介し，(P1), (P2), (P3) をどのように示すかの概要を示そう．

整数 n に対して $R(n)$ で n の 1 以外の約数全体をあらわす．

定理 2.1. m を 1 より大きい整数とし，n を m と互いに素な $\varphi(m)$ の約数とする．

次数が $n-2$ 次以下の整係数多項式

$$\mathscr{P}(t) = c_1 + c_2 t + \cdots + c_{n-s-1}t^{n-2} \in \mathbb{Z}[t] \tag{2.1}$$

と，$R(n)$ の部分集合 R と，R の元を添字にもつ，2 つごとに互いに素な整数 $m_r\,(r \in R)$ が存在して以下の条件をみたすとする．

(i) $n = \mathrm{lcm}\{r \mid r \in R\}$;

(ii) $\displaystyle\prod_{r\in R} m_r = m$;

(iii) $r \in R$ なら，同型

$$\mathbb{Z}[\zeta_r]/(\mathscr{P}(\zeta_r)) \cong \mathbb{Z}/m_r\mathbb{Z} \tag{2.2}$$

が成り立つ．

(iv) $r \in R(n)\backslash R$ なら

$$\mathscr{P}(\zeta_r) \in \mathbb{Z}[\zeta_r]^\times \tag{2.3}$$

が成り立つ．

k を標数が m と互いに素な体で，環準同型 (2.2) が群同型

$$\nu_k \,:\, \mathrm{Gal}(k(\zeta_m)/k) \xrightarrow{\sim} \langle \zeta_r \bmod \ \mathscr{P}(\zeta_r) \mid r \in R\rangle \tag{2.4}$$

を誘導するようなものとする．$K = k(\zeta_m)$ とし，$T = R^{(1)}_{K/k}\mathbb{G}_m$ とする．

これらの条件のもとで，T の次数 m の巡回自己同種写像 λ で，条件 $\ker\lambda(\bar{k}) = \ker\lambda(k)$ をみたすものが存在し，λ に付随する完全系列

$$1 \longrightarrow \ker\lambda \longrightarrow T \xrightarrow{\lambda} T \longrightarrow 1$$

はクンマー双対

$$\kappa_k \ : \ T(k)/\lambda T(k) \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\bar{k}/k), \ker\lambda(\bar{k})). \tag{2.5}$$

を誘導する．

証明の概要. 拡大 K/k はあとで具体的にその定め方をみることにして，まず一般に K/k が巡回拡大のときに $T = R^{(1)}_{K/k}\mathbb{G}_m$ の指標加群 $\widehat{T}$ の自己同型環を計算する．$G = \mathrm{Gal}(k/k) = \langle\tau\rangle$ とする．$\widehat{T} = \mathrm{Hom}(\ker\varepsilon, \mathbb{Z})$ であることが知られている．ここで $\varepsilon : \mathbb{Z}[G] \longrightarrow \mathbb{Z}$ は augumentaion map である．$\ker\varepsilon$ の基底として $\tau^i - \tau^{i-1}$ $(i = 1, \ldots, n-1)$ をとると，行列の形で計算する．$[K:k]-1$ 次行列

$$S = \begin{bmatrix} -1 & -1 & \cdots\cdots & -1 \\ 1 & 0 & \cdots\cdots & \\ 0 & 1 & 0 & \cdots\cdots \\ & \cdots\cdots\cdots & & \\ 0 & 0 & \ldots & 1 \quad 0 \end{bmatrix}$$

で定義すると，$G = \mathrm{Gal}(K/k)$ として，

$$\mathrm{End}_G(\widehat{T}) \cong \mathbb{Z}[S]$$

となることがわかる．したがって，求める $\widehat{T}$ の自己同型は (2.1) の形の多項式 $\mathscr{P}(t)$ を使って，$\Lambda = \mathscr{P}(S)$ とかける．Λ の余核を計算すると，

$$\mathrm{Coker}\Lambda \cong \bigoplus_{r\in R(n)} \mathbb{Z}[\zeta_r]/(\mathscr{P}(\zeta_r)) \tag{2.6}$$

となることがわかる．定理の条件 (iii), (iv) により，余核は $\oplus_{r\in R}\mathbb{Z}/m_r\mathbb{Z}$ に同型であり，(ii) と m_r たちが互いに素であることから，この群は位数 m の巡回群になる．λ を Λ に対応する $\mathrm{End}(T)$ の元とすると，λ は k 上定義された次数 m の巡回同種写像となり (P1) がみたされる．

ここで基礎体 k を次のように決める．標数が m と素な体 k_0 をとり，$K_0 = k_0(\zeta_m)$ とおく．$\mathrm{Gal}(K_0/k_0)$ を $(\mathbb{Z}/m\mathbb{Z})^\times$ の部分群と同一視する．このとき，この部分群が十分大きくなるように k_0 をとっておく．(2.2) の同型での ζ_r の像を σ_r とする．σ_r $(r \in R)$ が $\oplus_{r\in R}(\mathbb{Z}/m_r\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times$ において生成する部分群を H とする．すべての r が n の約数であることに注意すると，(i) から，H の位数は n になる．$k = K_0^H$ とし，$K = k(\zeta_m)$ とすれば，(2.4) をみたす拡大体 K/k がとれたことになる．$n = [K:k]$ であって $n \mid \varphi(m)$ をみたしている．

λ が (P2) をみたすことを示すために，(2.6) を使って，Λ の余核を具体的に計算する．法 m での座標がわかるので，それから λ の核の具体的な表示がえられる．これから (P2) が成り立つ．

(P3) は次のように示される．完全系列

$$1 \longrightarrow \ker\lambda \longrightarrow T \xrightarrow{\lambda} T \longrightarrow 1$$

のガロア・コホモロジーをとると，

$$T(k) \xrightarrow{\lambda} T(k) \longrightarrow \mathrm{H}^1(k, \ker\lambda) \longrightarrow \ker\Big(\lambda : \mathrm{H}^1(k,T) \longrightarrow \mathrm{H}^1(k,T)\Big).$$

一方，完全系列

$$1 \longrightarrow T \longrightarrow R_{K/k}\mathbb{G}_m \xrightarrow{N_{K/k}} \mathbb{G}_{m,k} \longrightarrow 1$$

から，

$$R_{K/k}\mathbb{G}_m(k) \xrightarrow{N_{K/k}} \mathbb{G}_{m,k}(k) \longrightarrow \mathrm{H}^1(k,T) \longrightarrow \mathrm{H}^1(k, R_{K/k}\mathbb{G}_m) \text{ (完全)}.$$

Shapiro の補題とヒルベルトの定理 90 から，

$$\mathrm{H}^1(k, R_{K/k}\mathbb{G}_m) \cong \mathrm{H}^1(K, \mathbb{G}_{m,K}) = 1.$$

標準的な同型 $R_{K/k}\mathbb{G}_m(k) \cong K^\times$ のもとで，

$$\mathrm{H}^1(k,T) \cong k^\times / N_{K/k}K^\times.$$

右辺は $[K : k]$ 乗で消える群である．一方 $m = \deg\lambda$ は n と互いに素だから，$\mathrm{H}^1(k,T)[\lambda] = 1$ をえる． □

補注 2.2. 条件 (2.2) から，$\mathscr{P}(\zeta_r)$ の生成する単項イデアルは剰余標数が相異なる次数 1 の素イデアルの積にならなくてはいけない．特に m_r および m は平方因子を持たない．

補注 2.3. この定理をスキーム理論を使って述べたものが [26] にある．特に核の決定に関しては同論文 Remark 3.5 が明快な記述を与えているようである．

この定理から，同型 (2.5) が成り立つような $[k(\zeta_m) : k] = n$ をみたす体 k 上の m 次巡回拡大が全てクンマー拡大としてえられることになる．それらは $T(k)$ の元でパラメータづけされていると考えると，$T(k) \cong \ker(N_{K/k} : K^\times \longrightarrow k^\times)$ だから k 上の n 個のパラメータ（そのパラメータには 1 つの関係式がはいる）を含む多項式で定義されることになる．これからわかるように，代数的トーラスの次元が小さいほど，パラメータの個数は少なくなる．その方向に議論をすすめると，相対ノルムのトーラスを使った [13] になる．

いろいろな都合があって，論文 [13] にしたがって，定理を述べたが，$R_{K/k}\mathbb{G}_m$ を使った [10] が一番定式化が素直で，証明も簡明である．

3 いくつかの例

この節では定理 2.1 が成立するような例をいくつかあげる．

例 3.1 (2 次降下 [5, Example 6.1]). m を平方因子を持たない正の奇数とする．$n = 2$ とする．$R(2) = R = \{2\}$ とする．$\mathscr{P}(t) = \dfrac{m+1}{2} + \dfrac{1-m}{2}t \in \mathbb{Z}[t]$ とすると，$\mathscr{P}(-1) = m$ であるから (2.2) は

$$\mathbb{Z}[-1]/\mathscr{P}(-1)\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z}$$

となる．$K = \mathbb{Q}(\zeta_m)$ とし，$H = \langle -1 \bmod m \rangle$ の固定体 $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ を k ととって，$T = R^{(1)}_{K/k}\mathbb{G}_m$ とする．T は 1 次元トーラスになる．$\mathscr{P}(S) = m$ であるから，λ は T の m 乗写像である．よってこのトーラス T に関してクンマー双対が成立する．これが小松 [15]，小川 [20] で扱われた場合である．最大実部分体上で generic 巡回多項式を簡単な形で書いた [22] もこの文脈で理解される．

$1, \sqrt{d} = (\zeta_m^2 - \zeta_m^{-2})$ を基底にとって，T 上の m 乗写像を計算すると，本質的にチェエビシェフ多項式が座標に現れる．

例えば $m = 3$ とすると，$k = \mathbb{Q}$ となり，クンマー拡大を定義する多項式が $(u_1 : u_2) \in \mathbb{P}^1(\mathbb{Q})$ をパラメータとして

$$4x^3 - 3x = \frac{u_1^2 - 3u_2^2}{u_1^2 + 3u_2^2}$$

と求められる．(詳細については [5, Example 6.1] を見よ)．パラメータ u_1, u_2 に $\mathbb{Q}$ の元を代入すれば $\mathbb{Q}$ 上の巡回 3 次拡大が得られ，逆に任意の $\mathbb{Q}$ 上の巡回 3 次拡大はこの形で得られる．

例 3.2 (基礎体として有理数体が取れる場合). 例 3.1 の $m = 3$ の場合以外にも，次の場合には基礎体として $\mathbb{Q}$ が取れることがわかる．すべて，$R = \{m-1\}$ ととればよい．

$\mathscr{P}(t)$	m
$2t+1$	5
$t+2$	7
$2t^3 - t^2 + t$	11

例 3.3 ($|R| \geq 2$ の場合 [13, Example 4.4]). $n = 6$ とする．$R(6) \supset R = \{3, 6\}$ をとる．多項式 $\mathscr{P}(t) = t^4 + t^3 + 2t^2 + 3t + 2$ は

$$\mathscr{P}(-1) = 1, \quad \mathscr{P}(\zeta_3) = 2\zeta_3 + 1, \quad \mathscr{P}(\zeta_6) = 4\zeta_6 - 1$$

をみたすから，

$$\mathbb{Z}[\zeta_3]/(2\zeta_3 + 1) \cong \mathbb{Z}/3\mathbb{Z}, \qquad \zeta_3 \mapsto 1,$$

$$\mathbb{Z}[\zeta_6]/(4\zeta_6 - 1) \cong \mathbb{Z}/13\mathbb{Z}, \qquad \zeta_6 \mapsto 10.$$

となり定理 2.1 の諸条件がみたされる．k を $\mathbb{Q}(\zeta_{39})$ の部分体で $\zeta_{39} \mapsto \zeta_{39}^{10}$ で固定されるものとする．計算により $x^4 + x^3 - 11x^2 + 9x + 3$ が k の定義多項式であることがわかる．$\mathscr{P}(t)$ できまる $T = R^{(1)}_{\mathbb{Q}(\zeta_{39})/k}\mathbb{G}_m$ の同種写像の逆像により，4 次体 k を含む体上の 39 次巡回拡大がすべてえられる．

このようなクンマー拡大では，体の生成元 $Q = \lambda^{-1}(P)$ へのガロア群の作用は Q に $\ker\lambda$ の元をかけることで得られる．これを利用すると，Q の座標を根に持つような多項式を具体的に計算することができる．詳細は [7] をみよ．

4　クンマー拡大の数論

古典的なクンマー拡大は単純な生成元をもち，そのガロア作用も 1 の冪根のかけ算という形でよくわかる．このことから，特に基礎体が代数体である場合に，その数論的な性質が詳しく調べられ，クンマー拡大は代数拡大体の構成において基本的なツールになっている．これらが，われわれのクンマー理論の場合にどのように一般化されるかをみるのがこの節の目的である．

4.1　分岐の記述

k を代数体とする．クンマー拡大 $k(\sqrt[n]{a})/k$ で n または a をわる k の素イデアル以外は不分岐であることはよく知られている．n が素数の場合は Hecke の理論として知られる詳細な分岐理論がある（例えば [1, Theorem 10.2.9] を見よ）．

トーラスを使ったクンマー拡大の場合も，$P \in T(k)$ に対応するクンマー拡大 $k(\lambda^{-1}(P))$ においては，標準的な同一視で $P \in K^\times$ とみたときに，P または m をわる k の素イデアルしか分岐しないことが示されている ([10, Proposition 6.3])．

Hecke の理論に対応する分岐理論は 1 次元のノルムトーラスの場合に小松 [15] で研究が行われた．一般の場合は，小野 [21] のアイディアに基づいて，局所体上のトーラスの指標加群にフィルター付けを行い，それを使って，局所体の巡回拡大の導手の付値を求めることができる．詳細は島倉 [23] を見ていただきたい．

4.2　Artin map

ふたたび k を代数体とする．クンマー拡大 $k(\sqrt[n]{a})/k$ の Artin 写像は具体的に計算することができる ([1, Proposition 5.4.1])．

$\mathbb{Q}$ 上の巡回 3 次拡大を 1 次元のノルムトーラスからくるクンマー拡大とみて，Artin map を計算したのが，小松 [16] である．

4.3 Equivariant Kummer theory

k_0 を通常の m 次のクンマー理論が成り立つ体とする．このとき k_0 の任意の拡大体 k でクンマー理論が成り立つ．k/k_0 がガロア拡大であれば $\mathrm{Gal}(k/k_0)$ が $k^\times/(k^\times)^m$ に作用し，この作用で不変な部分空間に対応するクンマー拡大は k_0 上のガロア拡大になる．これが節題の equivariant Kummer theory である ([2, Theorem 1.26]).

k/k_0 をその次数が m と素なアーベル拡大にとると，$\mathrm{Gal}(k/k_0)$ の指標で $k^\times/(k^\times)^m$ を固有空間に分解できる．この場合に，上の定理の特別な場合が [1, Theorem 5.3.5 (1)] にのっている．この定理の一般化を使って $\mathbb{Q}$ 上のいろいろな metacyclic 拡大を構成したのが [19] である．ここで群 G が metacyclic であるとは，G が巡回群の巡回群による拡大になること，すなわち，ある $u, v \in \mathbb{N}$ に対して完全系列

$$1 \longrightarrow C_u \longrightarrow G \longrightarrow C_v \longrightarrow 1$$

が存在することである．上記の論文 [19] では，クンマー理論で構成した体を冪根を含まない体に落とす際に，トレイスが使われている．これは [1, Theorem 5.3.5 (2)] を素直にならった構成だが，トレイスを使うとクンマー生成元のもつ乗法的な情報が欠落してしまう．

そこで，トーラスを使ったクンマー理論を使って metacyclic 拡大を構成する試みを行ったのが [12] である．(2.5) にあらわれる，$T(k)/\lambda T(k)$ を上と同様にアーベル群の作用で不変部分空間にわける．適用範囲が狭くなるものの，metacyclic 拡大が Kummer 拡大として得られ，しかもその部分体の情報を含んだ形で得られる．とくに $\mathbb{Q}$ 上のクンマー理論が存在する $m = 3, 5, 7, 11$ に対して，二面体群 D_m やフロベニウス群 $F_{m(m-1)}$ などの群をガロア群にもつ拡大体がクンマー拡大で実現される．日韓シンポジウムの報告集に掲載された [11] にこの方法で計算した S_3 クンマー多項式の例がある．

4.4 代数的トーラスを楕円曲線に取り替える

代数的トーラス T を他の代数群に取り替えることは容易に思いつくアイディアであろう．たとえば楕円曲線に取り替えると，自己同種写像だけを考えていても，虚数乗法を持たない場合は巡回拡大がえられない．一般の同種写像を考えて，クンマー拡大を作ることは例えば [14] や [9] で行われている．[18] はその先駆的仕事である．[14] では次のような形の単射準同型が得られている．

$$E_{a,b}(\mathbb{Q})/\phi^*(E^*_{a,b}(\mathbb{Q})) \hookrightarrow \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\bar{k}/k), \ker \lambda^*(\mathbb{Q})).$$

くわしい説明はしないが，$E_{a,b}, E^*_{a,b}$ はパラメータ a, b をもつ楕円曲線，λ^*, ϕ^* はある同種写像である．この単射の左辺は弱モーデル・ヴェイユの定理から有限群で，右辺の群のほんの一部の情報しかもっていない．同論文では，パラメータ a, b を動かすことにより，右辺の群の情報を回復している．

[18] や [9] では，楕円曲線を使った metacyclic 拡大の構成についても述べられている．

5 いくつかの課題

以上の節で，現在までの研究を振り返ったので，これをふまえて，いくつか今後の課題を述べよう．

5.1 クンマー生成元を求める

通常のクンマー拡大では， Lagrange resolvent を使って，$K = k(\sqrt[m]{a})$ となる $a \in k^\times$ が求められる ([1, Theorem 5.3.5 (4)])．それでは，巡回拡大 K/k が巡回同種写像 λ に関するクンマー拡大であることがわかっているとき，$K = k(\lambda^{-1}(P))$ をみたす $P \in T(k)$ を求めるにはどうすればよいか．

Artin map が一般の場合にも計算できれば，[1, Section 5.4] で説明されている方法が使えるかもしれない．

5.2 イデアル類群の鏡映定理

イデアル類群の鏡映定理というのは Scholz によって証明された，$\mathbb{Q}(\sqrt{d})$ と $\mathbb{Q}(\sqrt{-3d})$ のイデアル類群の 3-rank の関係を与える定理である ([27, Theorem 10.10])．その証明にはクンマー理論，ガロア理論，類体論が三位一体で使われる．この場合には $\mathbb{Q}(\sqrt{-3})$ が円分体であるから，クンマー理論が使えるわけだが，ここで前節までで説明したクンマー理論を使ったらどうなるだろう．別の体の組であったり，3-rank ではなく 5-rank であったりというふうに拡張できるだろうか．[4] の拡張や簡単な証明が得られたりするだろうか．

[20] の第 4 節にも同様の問題がのっている．この節にはいろいろな課題がのっているがどれも手付かずであろうと推測される．

5.3 代数群を取りかえる

まず，これまで研究されてきた代数的トーラス以外の代数的トーラスをとると，クンマー理論の適用範囲は広がるだろうか．$R^{(1)}_{K/k}\mathbb{G}_m$ と $R_{K/k}\mathbb{G}_m$ では適用範囲が変わらないことが [10, Section 6] で示されている．[17] にリストのある 2 次元や 3 次元の代数的トーラスに限って具体的に調べてみてもよいかもしれない．また自己同種写像だけでなく，一般の同種写像についても調べる価値があるかもしれない．

4.4 節で述べたように代数群をアーベル多様体に取りかえるのも一つのアイディアである．楕円曲線だけを考えていると，大きい核を持つ同種写像が得られない

ので，高次元のものも考える必要があろう．その場合でも弱モーデル・ヴェイユの定理があるので，なんらかの族を考える必要がある．ただし，実際に巡回多項式を計算することなどは容易ではないであろう．

究極には可換代数群だけではなく，非可換代数群も考えてはどうだろうか．クンマー双対の定式化をどうすればよいのか，私にはよくわからないが，非可換なガロア群をもつ拡大が，クンマー拡大として得られれば，とてもおもしろいのではないだろうか．

6　先行研究に関する覚書

昔から，クンマー理論を冪根のない体に拡張しようとする試みはいろいろあるようだが，それらをすべて調べ上げ，解説するのは私の手に余る．ここでは第2節で解説した研究に直接つながるものだけを覚書風に書いておくことにとどめる．

まずあげなければいけないのは小松 [15] である．橋本・三宅 [3] の仕事をうけて，最大実部分体上で簡明な形の generic 巡回方程式を作った陸名 [22] の仕事を「2次降下」クンマー理論として定式化したのがこの小松さんの仕事である．私は，そのころ活発に研究されていた generic 多項式に関するいろいろな結果の素晴らしさは別にして，証明の中で使われる巧妙な式変形，華麗な変数変換に，かなり近寄りがたい印象を受けていた．小松さんの仕事を知ったとき（それは確か立命館大学での小規模な研究集会の時であったと記憶する），「こういう風にやる方法もあるのか」と蒙を啓かれる思いだった．小松さん自身は巡回多項式への興味が強かったと思うが，私は初めから体の理論としてのクンマー理論の一般化を考える方に興味があった．そのような意識を共有していたのが，阪大の小川さんだったように思われる．残念ながら彼のこの方面の論文は [20] しかない．以上が2002年の出来事である．

その後，私は2003年10月から2004年7月にかけて文部科学省長期在外研究員として，ローマに滞在した．ホストの Schoof さんのもとで非常に楽しい滞在であったが，その間，小松さんの仕事を高次元に拡張することを考えた．高次元の代数群に関する知識はほとんどないに等しかったので，小野先生の [21] などを読みながら，手探りで拡張を探った．はじめは，小松さんのやり方を踏襲して，冪乗写像を使っていて，巡回同種写像が必要なことがすぐには気づかなかった．同種写像を双対である指標加群に構成することができると，あとはいろいろな計算が，自分でも驚くほど順調に進み，その結果としてできあがったのが [5] である．帰国後2004年の数理研の研究集会での講演の記録が [6] である．

小川さんや小松さんの定式化を群スキームの枠組みで拡張したのが，諏訪さんの [24] で，2004年の上記の数理研の研究集会でも，その内容を講演している．その後，諏訪さんは，今回紹介した定理を含めて，それらを環上に一般化した理論を群スキームの洗練された言葉で書いたものを論文にしている ([25], [26] など)．幾

何の達者な方には私の論文よりも諏訪さんの論文の方が読みやすいであろう．

謝辞 このサマースクールで講演の機会をいただけたことに対し，世話人の皆様に深く感謝します．2015 年には完成稿ができていたにもかかわらず，諸事情からお蔵入りになりかけていた [13] を出版するきっかけにもなったことを記しておきます．

参考文献

[1] H. Cohen, *Advanced topics in computational number theory*, Springer-Verlag, New York, 2000.

[2] P. Guillot, *A gentle course in local class field theory*, Cambridge University Press, Cambridge, 2018.

[3] K.-I. Hashimoto and K. Miyake, *Inverse Galois problem for dihedral groups*, Number theory and its applications (Kyoto, 1997), Dev. Math., vol. 2, Kluwer Acad. Publ., Dordrecht, 1999, pp. 165–181.

[4] M. Imaoka and Y. Kishi, *On dihedral extensions and Frobenius extensions*, Galois theory and modular forms, Dev. Math., vol. 11, Kluwer Acad. Publ., Boston, MA, 2004, pp. 195–220.

[5] M. Kida, *Kummer theory for norm algebraic tori*, J. Algebra **293** (2005), no. 2, 427–447.

[6] ———, **ノルム・トーラスのクンマー理論**, 数理解析研究所講究録 (2005), no. 1451, 237–242, Algebraic number theory and related topics (Japanese) (Kyoto, 2004).

[7] ———, *Cyclic polynomials arising from Kummer theory of norm algebraic tori*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 102–113.

[8] ———, **冪根を含まない体のクンマー理論について**, 第 5 回北陸数論研究集会報告集, 2006, pp. 87–94.

[9] ———, D_5 **拡大のクンマー理論**, 早稲田大学整数論研究集会 2008 報告集, 2008, pp. 51–62.

[10] ———, *Descent Kummer theory via Weil restriction of multiplicative groups*, J. Number Theory **130** (2010), no. 3, 639–659.

[11] ———, *A Kummer theoretic construction of an S_3-polynomial with given quadratic subfield*, Interdiscip. Inform. Sci. **16** (2010), no. 1, 17–20.

[12] ———, *On metacyclic extensions*, J. Théor. Nombres Bordeaux **24** (2012), no. 2, 339–353.

[13] ———, *Algebraic extensions attached to algebraic tori of relative norm*, to appear in SUT Journal of Math. (2019).

[14] M. Kida, Y. Rikuna, and A. Sato, *Classifying Brumer's quintic polynomials by weak Mordell-Weil groups*, Int. J. Number Theory **6** (2010), no. 3, 691–704.

[15] T. Komatsu, *Arithmetic of Rikuna's generic cyclic polynomial and generalization of Kummer theory*, Manuscripta Math. **114** (2004), no. 3, 265–279.

[16] ———, *Cyclic cubic field with explicit Artin symbols*, Tokyo J. Math. **30** (2007), no. 1, 169–178.

[17] B. Kunyavskiĭ and J.-J. Sansuc, *Réduction des groupes algébriques commutatifs*, J. Math. Soc. Japan **53** (2001), no. 2, 457–483.

[18] O. Lecacheux, *Constructions de polynômes génériques à groupe de Galois résoluble*, Acta Arith. **86** (1998), no. 3, 207–216.

[19] S. Nakano and M. Sase, *A note on the construction of metacyclic extensions*, Tokyo J. Math. **25** (2002), no. 1, 197–203.

[20] H. Ogawa, *Quadratic reduction of multiplicative group and its applications*, 数理解析研究所講究録 (2003), no. 1324, 217–224, Algebraic number theory and related topics (Japanese) (Kyoto, 2002).

[21] T. Ono, *Arithmetic of algebraic tori*, Ann. of Math. (2) **74** (1961), 101–139.

[22] Y. Rikuna, *On simple families of cyclic polynomials*, Proc. Amer. Math. Soc. **130** (2002), no. 8, 2215–2218 (electronic).

[23] M. Shimakura, *Ramification in Kummer extensions arising from algebraic tori*, Bull. Aust. Math. Soc. **96** (2017), no. 2, 196–204.

[24] N. Suwa, *Twisted Kummer and Kummer-Artin-Schreier theorems*, Tohoku Math. J. (2) **60** (2008), no. 2, 183–218.

[25] ———, *Around Kummer theories*, Algebraic number theory and related topics 2007, RIMS Kôkyûroku Bessatsu, B12, Res. Inst. Math. Sci. (RIMS), Kyoto, 2009, pp. 115–148.

[26] ———, *Kummer theories for algebraic tori and normal basis problem*, Tokyo J. Math. **39** (2017), no. 3, 827–862.

[27] L. C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.

木田雅成
東京理科大学理学部第一部数学科
〒 162-8601 新宿区神楽坂 1-3
E-mail: kida@rs.tus.ac.jp
(2019 年 9 月 7 日講演)