algebraic torus に対する Kummer 理論と正規底問題, 例

諏訪 紀幸* (中央大学)

2013 年 3 月に開催された早稲田整数論研究集会において「algebraic torus に対する Kummer 理論と正規底問題」と題して講演し, 研究集会報告集に寄稿する機会を得たが, 本稿はその続編である.

Serre は [13, Ch.VI, 8] で, 体の有限 Galois 拡大に対する正規底の定理と群環の単数群を表現する代数群を結び付けて, Kummer 理論や Artin-Schreier-Witt 理論を記述する方法を定式化した. そこでは algebraic torus に対する Kummer 理論をも示唆している. 拙論 [15], [16] において Serre の議論を群スキームの枠組みの中で sculpture problem として捉え直し, それに embedding problem を加えて正規底をもつ不分岐 Galois 拡大の versal family について議論した.

巡回拡大を記述する algebraic torus に対する Kummer 理論は, 生成多項式とも関連して木田雅成, 小松亨, 橋本喜一朗, 陸名雄一の各氏を初めとする研究の蓄積がある ([4], [5], [6], [7], [9]). 拙稿 [17] ではこれと関連して, Weil restriction に対する Kummer 理論, norm torus に対する Kummer 理論, cyclotomic-twisted tours に対する Kummer 理論に対して sculpture problem と embedding problem について議論した. 本稿ではその例と Kummer-Artin-Schreier 理論について補足する. 第 1 節では必要な言葉と記号を定義する. 第 2 節では [17] の第 3 節から第 5 節にかけて述べた algebraic torus に対する Kummer 理論に関する結果を要約して述べる. 第 3 節では幾つかの例を示し, 第 4 節では Kummer-Artin-Schreier 理論と algebraic torus に対する Kummer 理論を組み合わせて得られた結果について述べる.

福岡数論研究集会で講演の機会が与えられたことに改めて感謝申し上げたい.

記号. 環は断らない限り可換環を意味する. R を (必ずしも可換でない) 環とする. R の可逆元のなす乗法群を $R^\times$ で表わす. また, $\mathbb{G}_{m,\mathbb{Z}} = \operatorname{Spec}\mathbb{Z}[U, 1/U]$ は乗法群スキームを表わす. したがって, R が可換環なら, $\mathbb{G}_{m,\mathbb{Z}}(R) = R^\times$.

A を環, B を A 代数とし, B が A 加群として有限型射影的であると仮定する. B スキーム X に対して, 環の拡大 B/A に対する X の Weil restriction を $\prod_{B/A} X$ で表わす.

正の整数 n に対して $\zeta_n = e^{2\pi i/n}$, $\boldsymbol{\mu}_n = \{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\}$ とおく.

1 sculpture problem と embedding problem

記号 1.1. Γ を有限群とする. $A(\Gamma) = \operatorname{Spec}\mathbb{Z}[T_\gamma\,;\,\gamma \in \Gamma]$ に加法と乗法をそれぞれ

$$T_\gamma \mapsto T_\gamma \otimes 1 + 1 \otimes T_\gamma$$

あるいは

$$T_\gamma \mapsto \sum_{\gamma'\gamma''=\gamma} T_{\gamma'} \otimes T_{\gamma''}$$

*本研究は科学研究費補助金 (No. 25·173 および 23540027) による支援を受けております.

によって定義すると, $A(\Gamma)$ は環の構造を持つ. さらに, 可換環の圏から環の圏への函手 $R \mapsto R[\Gamma]$ は $A(\Gamma)$ によって表現される. また,

$$U(\Gamma) = \operatorname{Spec}\mathbb{Z}[T_\gamma, \frac{1}{\Delta_\Gamma}\,;\gamma\in\Gamma],$$

Δ_Γ は行列 $(T_{\gamma\gamma'})_{\gamma,\gamma'\in\Gamma}$ の行列式を表わす (Dedkind の群行列式)

とおくと, $U(\Gamma)$ は $A(\Gamma)$ の乗法によって群の構造を持つ. さらに, 可換環の圏から群の圏への函手 $\Gamma \mapsto R[\Gamma]^\times$ は $U(\Gamma)$ によって表現される.

Γ によって定義される constant group scheme もまた Γ と記す. 自然な埋め込み $\Gamma \to R[\Gamma]^\times$ は群スキームの準同型 $i : \Gamma \to U(\Gamma)$ によって定義される. また, $\gamma\in\Gamma$ の $U(\Gamma)$ の上への右乗法は $T_{\gamma'} \mapsto T_{\gamma'\gamma^{-1}}$ によって定義される. さらに,

$$U(\Gamma)/\Gamma = \operatorname{Spec}\mathbb{Z}[T_\gamma, 1/\Delta_\Gamma]^\Gamma$$

が成立する.

補足 1.2. R を環とする. 環の埋め込み $i : R \to R[\Gamma]$ は乗法群の埋め込み $i : R^\times \to R[\Gamma]^\times$ を誘導する. 準同型 $i : R^\times \to R[\Gamma]^\times$ を表現する群スキームの準同型

$$i : \mathbb{G}_{m,\mathbb{Z}} = \operatorname{Spec}\mathbb{Z}[U, \frac{1}{U}] \to U(\Gamma) = \operatorname{Spec}\mathbb{Z}[T_\gamma, \frac{1}{\Delta_\Gamma}\,;\gamma\in\Gamma]$$

は

$$T_\gamma \mapsto \begin{cases} U & (\gamma = 1) \\ 0 & (\gamma \neq 0) \end{cases}$$

によって定義される.

一方,

$$\varepsilon(\sum_{\gamma\in\Gamma} a_\gamma\gamma) = \sum_{\gamma\in\Gamma} a_\gamma$$

によって R 代数の準同型 $\varepsilon : R[\Gamma] \to R$ が定義される (augmentation 写像). $\varepsilon : R[\Gamma] \to R$ から誘導される乗法群の準同型 $\varepsilon : R[\Gamma]^\times \to R^\times$ を表現する群スキームの準同型

$$\varepsilon : U(\Gamma) = \operatorname{Spec}\mathbb{Z}[T_\gamma, \frac{1}{\Delta_\Gamma}\,;\gamma\in\Gamma] \to \mathbb{G}_{m,\mathbb{Z}} = \operatorname{Spec}\mathbb{Z}[U, \frac{1}{U}]$$

は

$$U \mapsto \sum_{\gamma\in\Gamma} T_\gamma$$

によって定義される.

言葉 1.3. R を環, Γ を有限群, S を Γ による左作用をもつ R 代数とする. $\operatorname{Spec} S$ が $\operatorname{Spec} R$ の上の Γ-torsor であるとき, 言い換えれば, $\operatorname{Spec} S/\operatorname{Spec} R$ が Γ を Galois 群とする étale covering であるとき, S/R は Γ を Galois 群とする不分岐 Galois 拡大である, あるいは, S/R は不分岐 Γ 拡大であるという. 特に, Γ が位数 n の巡回群であるとき, 不分岐拡大 S/R は次数 n の巡回拡大であるという.

言葉 1.4. R を環, Γ を有限群, S/R を Γ を Galois 群とする不分岐 Galois 拡大とする. $s \in S$ が存在して $(\gamma s)_{\gamma\in\Gamma}$ が R 加群 S の基底となるとき, 不分岐 Γ 拡大 S/R は正規底を持つという.

例 1.5. $\mathbb{Z}[T_\gamma, 1/\Delta_\Gamma]/\mathbb{Z}[T_\gamma, 1/\Delta_\Gamma]^\Gamma$ は Γ を Galois 群とする不分岐 Galois 拡大となる．さらに, $\{T_\gamma\}_{\gamma\in\Gamma}$ は不分岐 Γ 拡大 $\mathbb{Z}[T_\gamma, 1/\Delta_\Gamma]/\mathbb{Z}[T_\gamma, 1/\Delta_\Gamma]^\Gamma$ の正規底となる．

これから次が従う．

系 1.6. R を環, Γ を有限群, S/R を不分岐 Γ 拡大とする．このとき, 不分岐 Γ 拡大 S/R が正規底をもつ $\Leftrightarrow$ 射 $\mathrm{Spec}\, S \to U(\Gamma)$ および $\mathrm{Spec}\, R \to U(\Gamma)/\Gamma$ が存在して図式

$$\begin{array}{ccc} \mathrm{Spec}\, S & \longrightarrow & U(\Gamma) \\ \big\downarrow & & \big\downarrow \\ \mathrm{Spec}\, R & \longrightarrow & U(\Gamma)/\Gamma \end{array}$$

が cartesian となる．

Serre が [13, Ch.VI, 8] で議論しているように, Γ が巡回群である場合, 正規底を持つ不分岐 Γ 拡大の versal family $U(\Gamma) \to U(\Gamma)/\Gamma$ を彫琢することによって Kummer 理論や Artin-Schreier-Witt 理論が導き出される．この議論を一般化さらに補完して次の sculpture problem や embedding problem が考えられる．

問題 1.7. Γ を有限群, R を環とし, $i : \Gamma \to G$ を R の上の群スキームの埋め込みとする．
(a) (sculpture problem) 可換図式

$$\begin{array}{ccc} \Gamma & \longrightarrow & U(\Gamma)_R \\ \big\downarrow\wr & & \big\downarrow \\ \Gamma & \xrightarrow{\ i\ } & G \end{array}$$

が存在するか．
(b) (embedding problem) 可換図式

$$\begin{array}{ccc} \Gamma & \xrightarrow{\ i\ } & G \\ \big\downarrow\wr & & \big\downarrow \\ \Gamma & \longrightarrow & U(\Gamma)_R \end{array}$$

が存在するか．

sculpture problem が正しければ次の結論を得る．S/R を不分岐 Γ 拡大とする．Galois 拡大 S/R が正規底を持つなら, cartesian 図式

$$\begin{array}{ccc} \mathrm{Spec}\, S & \longrightarrow & G \\ \big\downarrow & & \big\downarrow \\ \mathrm{Spec}\, R & \longrightarrow & G/\Gamma \end{array}$$

が存在する．
一方, embedding problem が正しければ次の結論を得る．S/R を cartesian 図式

$$\begin{array}{ccc} \mathrm{Spec}\, S & \longrightarrow & G \\ \big\downarrow & & \big\downarrow \\ \mathrm{Spec}\, R & \longrightarrow & G/\Gamma \end{array}$$

によって定義される不分岐 Γ 拡大とする．このとき, Galois 拡大 S/R は正規底を持つ．

2 algebraic tours に対する Kummer 理論

Γ を位数 n の巡回群, γ を Γ の生成元とし, $\zeta = \zeta_n = e^{2\pi i/n}$ とおく. R を可換環とする. n の正の約数 d に対して

$$\chi_d : \sum_{k=0}^{n-1} a_k \gamma^k \mapsto \sum_{k=0}^{n-1} a_k \otimes \zeta_d^k$$

によって環の準同型 $\chi_d : R[\Gamma] \to R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_d]$ が, さらに, 群の準同型 $\chi_d : (R[\Gamma])^\times \to (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_d])^\times$ が定義される. 準同型 $\chi_d : (R[\Gamma])^\times \to (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_d])^\times$ は群スキームの準同型

$$\chi_d : U(\Gamma) \to \prod_{\mathbb{Z}[\zeta_d]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta_d]}$$

によって表現される.

$$\chi = (\chi_d)_{d|n} : U(\Gamma) \to \prod_{d|n} \prod_{\mathbb{Z}[\zeta_d]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta_d]}$$

とおく. 群スキームの準同型 χ は $\mathbb{Z}[1/n]$ の上で同型. 実際, 逆射は

$$(\alpha_d)_{d|n} \mapsto \frac{1}{n} \sum_{j=0}^{n-1} \Big\{ \sum_{d|n} \mathrm{Tr}_{R\otimes_Z \mathbb{Z}[\zeta_d]/R}(1 \otimes \zeta_d^{-j}) \alpha_d \Big\} \gamma^j$$

によって与えられる.

補足 2.1. $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ とおく. このとき, Weil restriction $\big(\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}\big) \otimes_{\mathbb{Z}} \mathbb{Z}[1/n]$ は $\mathbb{Z}[G]$ を指標群にもつ $\mathbb{Z}[1/n]$ の上の algebraic torus.

さらに, 各 $d|n$ に対して $G_d = \mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})$ とおく. このとき, G_d は G の剰余群なので, 係数の制限によって $\mathbb{Z}[G_d]$ は $\mathbb{Z}[G]$ 加群とみなせる. また, $\big(\prod_{\mathbb{Z}[\zeta_d]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta_d]}\big) \otimes_{\mathbb{Z}} \mathbb{Z}[1/n]$ は $\mathbb{Z}[G_d]$ を指標群にもつ $\mathbb{Z}[1/n]$ の上の algebraic torus. したがって, $U(\Gamma)_{\mathbb{Z}[1/n]}$ は $\bigoplus_{d|n} \mathbb{Z}[G_d]$ を指標群にもつ $\mathbb{Z}[1/n]$ の上の algebraic torus.

観察 2.2. R を環とする. このとき, 対応 $\gamma \mapsto 1 \otimes \zeta$ によって群の準同型 $\Gamma \to (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])^\times$ が定義される. 群の準同型 $\Gamma \to (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])^\times$ は群スキームの準同型 $\Gamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ によって表現される.

(a) n が奇数なら, $\Gamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ は群スキームの埋め込み. さらに, 図式

$$\begin{tikzcd} \Gamma \arrow[r] \arrow[d, equal] & U(\Gamma) \arrow[d, "\chi_n"] \\ \Gamma \arrow[r] & \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} \end{tikzcd}$$

は可換. したがって, 埋め込み $\Gamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ に対して sculpture problem は肯定的.

(b) n が偶数なら, $\Gamma \to \big(\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}\big) \otimes_{\mathbb{Z}} \mathbb{Z}[1/2]$ は群スキームの埋め込み. さらに, 図式

$$\begin{tikzcd} \Gamma \arrow[r] \arrow[d, equal] & U(\Gamma)_{\mathbb{Z}[1/2]} \arrow[d, "\chi_n"] \\ \Gamma \arrow[r] & \big(\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}\big) \otimes_{\mathbb{Z}} \mathbb{Z}[1/2] \end{tikzcd}$$

は可換. したがって, 埋め込み $\Gamma \to \big(\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}\big) \otimes_{\mathbb{Z}} \mathbb{Z}[1/2]$ に対して sculpture problem は肯定的.

観察 2.3. 各 $g \in G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ に対して $g(\zeta) = \zeta^{i(g)}$ となるような $i(g) \in (\mathbb{Z}/n\mathbb{Z})^\times$ が唯一つ存在する．このとき, 対応 $g \mapsto i(g)$ は群の同型 $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$ を与える．さらに, $(g, l) \mapsto i(g)l$ によって定義される G による左作用をもつ左 $\mathbb{Z}[G]$ 加群 $\mathbb{Z}/n\mathbb{Z}$ を $\mathbb{Z}/n\mathbb{Z}(1)$ と記す．$\varGamma$ によって定義される $\mathbb{Z}[1/n]$ の上の constant group scheme は $\mathbb{Z}/n\mathbb{Z}(1)$ を指標群とする乗法型群スキーム．乗法型群スキームの埋め込み $i : \varGamma \to \left(\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}\right) \otimes_{\mathbb{Z}} \mathbb{Z}[1/n]$ に対応する指標群の準同型 $\eta_n : \mathbb{Z}[G] \to \mathbb{Z}/n\mathbb{Z}(1)$ は

$$1 \mapsto 1 \bmod n$$

によって与えられる．

さらに, $1 \mapsto n/d \bmod n$ によって $Z[G]$ 加群の準同型 $\eta_d : \mathbb{Z}[G_d] \to \mathbb{Z}/n\mathbb{Z}(1)$ が定義される．$\mathbb{Z}[1/n]$ の上の群スキームの埋め込み $i : \varGamma \to U(\varGamma)_{\mathbb{Z}[1/n]}$ に対応する指標群の準同型は

$$\eta = \sum_{d|n} \eta_d : \bigoplus_{d|n} \mathbb{Z}[G_d] \to \mathbb{Z}/n\mathbb{Z}(1)$$

によって与えられる．

命題 2.4 ([17, 命題 3.4])**.** n を整数 ≥ 2 とする．このとき, 次の条件は同値.
(a) 埋め込み $\varGamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ に対して embedding problem が $\mathbb{Z}[1/n]$ の上で肯定的.
(b) 埋め込み $\varGamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ に対して embedding problem が $\mathbb{Q}$ の上で肯定的.
(c) 各 $d|n$ に対して $\mathrm{Nr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_d)}$ は $\boldsymbol{\mu}_n$ から $\boldsymbol{\mu}_d$ の上への全射を誘導する.

系 2.5. n が偶数 ≥ 4 なら, 埋め込み $\varGamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ に対する embedding problem は $\mathbb{Z}[1/n]$ の上で否定的.

系 2.6. p を素数 > 2 とし, $n = p^r$ とする．このとき, 埋め込み $\varGamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ に対する embedding problem は $\mathbb{Z}[1/p]$ の上で肯定的.

記号 2.7. R を環とする．$\mathrm{Nr} : \mathbb{Z}[\zeta] \to \mathbb{Z}$ は乗法群の準同型 $\mathrm{Nr} : (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])^\times \to R^\times$ を誘導する．群の準同型 $\mathrm{Nr} : (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])^\times \to R^\times$ は群スキームの準同型

$$\mathrm{Nr} : \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} \to \mathbb{G}_{m,\mathbb{Z}}$$

によって表現される．さらに,

$$\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}}^{(1)} \mathbb{G}_{m,\mathbb{Z}[\zeta]} = \mathrm{Ker}[\mathrm{Nr} : \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} \to \mathbb{G}_{m,\mathbb{Z}}]$$

と定義する．このとき, 群スキームの準同型 $\varGamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ は

$$\varGamma \longrightarrow \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}}^{(1)} \mathbb{G}_{m,\mathbb{Z}[\zeta]} \longrightarrow \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$$

と分解される．

補足 2.8. $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ とおく．$1 \mapsto \sum_{g \in G} g$ によって $\mathbb{Z}[G]$ 加群の準同型 $\nu : \mathbb{Z} \to \mathbb{Z}[G]$ が定義される．$J_G = \mathrm{Coker}[\nu : \mathbb{Z} \to \mathbb{Z}[G]]$ とおけば, $\left(\prod^{(1)}_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}\right) \otimes_{\mathbb{Z}} \mathbb{Z}[1/n]$ は J_G を指標群にもつ $\mathbb{Z}[1/n]$ の上の algebraic torus.

命題 2.9 ([17, 命題 4.3, 4.4, 4.5])**.** n を整数 ≥ 3 とする．
(1) n が奇数なら, 群スキームの埋め込み $\varGamma \to \prod^{(1)}_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ に対して sculpture problem は $\mathbb{Z}[1/n]$ の上で肯定的.
(2) n が偶数なら, 群スキームの埋め込み $\varGamma \to \prod^{(1)}_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ に対して sculpture problem は $\mathbb{Q}$ の上で否定的.
(3) 埋め込み $\varGamma \to \prod^{(1)}_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ に対して embedding problem が $\mathbb{Z}[1/n]$ の上で肯定的 $\Leftrightarrow$ 埋め込み $\varGamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ に対して embedding problem が $\mathbb{Z}[1/n]$ の上で肯定的.

記号 2.10. K を円分拡大 $\mathbb{Q}(\zeta)/\mathbb{Q}$ の部分拡大, $\mathcal{O}_K$ を K の整数環とする．R を環とすれば, 写像 $\mathrm{Nr}_{\mathbb{Q}(\zeta)/K} : \mathbb{Z}[\zeta] \to \mathcal{O}_K$ は乗法群の準同型 $\mathrm{Nr}_K : (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])^\times \to (R \otimes_{\mathbb{Z}} \mathcal{O}_K)^\times$ を誘導する．準同型 $\mathrm{Nr}_K : (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])^\times \to (R \otimes_{\mathbb{Z}} \mathcal{O}_K)^\times$ は群スキームの準同型

$$\mathrm{Nr}_K : \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} \to \prod_{\mathcal{O}_K/\mathbb{Z}} \mathbb{G}_{m,\mathcal{O}_K}$$

によって表現される．
n が素数 $p > 2$ であると仮定し,

$$\boldsymbol{G}_p = \bigcap_{\substack{\mathbb{Q}\subset K\subset\mathbb{Q}(\zeta)\\ K\neq\mathbb{Q}(\zeta)}} \mathrm{Ker}\big[\mathrm{Nr}_K : \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} \to \prod_{\mathcal{O}_K/\mathbb{Z}} \mathbb{G}_{m,\mathcal{O}_K}\big]$$

とおく．このとき, 群スキームの埋め込み $\varGamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ は

$$\varGamma \longrightarrow \boldsymbol{G}_p \longrightarrow \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$$

と分解される．

命題 2.11 ([17, 命題 5.2])**.** p を素数 > 2 とする．
(1) 群スキームの埋め込み $\varGamma \to \boldsymbol{G}_p$ に対して sculpture problem は肯定的.
(2) $\mathbb{Z}[1/p]$ の上の群スキームの埋め込み $\varGamma \to \boldsymbol{G}_p \otimes_{\mathbb{Z}} \mathbb{Z}[1/p]$ に対して embedding problem は肯定的.

補足 2.12. p を素数 > 2 とし, $\zeta = e^{2\pi i/p}$ とおく．$G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ とおき, g を G の生成元とする．指標 $\rho : G \to \mathbb{C}^\times$ を $\rho(g) = e^{2\pi i/(p-1)}$ によって定義する．このとき, $\mathrm{Im}[\rho : \mathbb{Z}[G] \to \mathbb{C}] = \mathbb{Z}[\zeta]$. ρ によって $\mathbb{Z}[\zeta]$ は $\mathbb{Z}[G]$ 加群と見なせる．さらに, $\boldsymbol{G}_p \otimes_{\mathbb{Z}} \mathbb{Z}[1/p]$ は $\mathbb{Z}[\zeta]$ を指標群とする $\mathbb{Z}[1/p]$ の上の algebriac torus $\mathbb{G}_m(\rho)$ に同型 (Mazur-Rubin-Silverberg [8, Remark 5.11]).

3　例

指標群によって記述した algebraic torus の座標環を記述することは不変式を求める問題に帰着するが, どのように円分体の整数環の整数底をとるかによって記述が異なって来る．ここでは, 巡回群 $\varGamma$ の位数が素数 $p > 2$ である場合に第 2 節で現れた群スキームの準同型を具体的に記述する．
p を素数 > 2 とし, $\zeta = e^{2\pi i/p}$ とおく．このとき, $\{\zeta, \zeta^2, \ldots, \zeta^{p-1}\}$ は $\mathbb{Z}[\zeta]$ の $\mathbb{Z}$ の上の基底. したがって, R を環とすれば, $R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta]$ の元は

$$a_1 \otimes \zeta + a_2 \otimes \zeta^2 + \cdots + a_{p-1} \otimes \zeta^{p-1} \quad (a_1, a_2, \ldots, a_{p-1} \in R)$$

の形に一意的に表わせる．ここで，

$$N_p(X_1, X_2, \dots, X_{p-1}) = \prod_{j=1}^{p-1}(\zeta^j X_1 + \zeta^{2j} X_2 + \cdots + \zeta^{(p-1)j} X_{p-1})$$

とおけば，$N_p(X_1, X_2, \dots, X_{p-1}) \in \mathbb{Z}[X_1, X_2, \dots, X_{p-1}]$．さらに，

$$a_1 \otimes \zeta + a_2 \otimes \zeta^2 + \cdots + a_{p-1} \otimes \zeta^{p-1} \in (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])^\times \ \Leftrightarrow\ N_p(a_1, a_2, \dots, a_{p-1}) \in R^\times.$$

したがって，

$$\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} = \operatorname{Spec} \mathbb{Z}[X_1, X_2, \dots, X_{p-1}, \frac{1}{N_p(X_1, X_2, \dots, X_{p-1})}].$$

また，乗法は

$$X_i \mapsto -\sum_{\substack{j+k\equiv 0 \\ \bmod p}} X_j \otimes X_k + \sum_{\substack{j+k\equiv i \\ \bmod p}} X_j \otimes X_k \quad (1 \le i \le p-1)$$

によって定義される．

さらに，群スキームの準同型

$$\mathrm{Nr} : \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} = \operatorname{Spec} \mathbb{Z}[X_1, X_2, \dots, X_{p-1}, \frac{1}{N_p(X_1, X_2, \dots, X_{p-1})}]$$
$$\to \mathbb{G}_{m,\mathbb{Z}} = \operatorname{Spec} \mathbb{Z}[U, \frac{1}{U}]$$

は

$$U \mapsto N_p(X_1, X_2, \dots, X_{p-1})$$

によって定義される．したがって，

$$\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}}{}^{(1)} \mathbb{G}_{m,\mathbb{Z}[\zeta]} = \operatorname{Spec} \mathbb{Z}[X_1, X_2, \dots, X_{p-1}]/(N_p(X_1, X_2, \dots, X_{p-1}) - 1).$$

$\varGamma = \{1, \gamma, \dots, \gamma^{p-1}\}$ を位数 p の巡回群とする．また，

$$\varDelta_p(T_0, T_1, \dots, T_{p-1}) = \varDelta_\varGamma(T_0, T_1, \dots, T_{p-1}) = \begin{vmatrix} T_0 & T_1 & \dots & T_{p-1} \\ T_1 & T_2 & \dots & T_0 \\ \vdots & \vdots & \ddots & \vdots \\ T_{p-1} & T_0 & \dots & T_{p-2} \end{vmatrix}$$

とおく．このとき，

$$\varDelta_p(T_0, T_1, \dots, T_{p-1}) = (-1)^{(p-1)/2} \prod_{j=0}^{p-1}(T_0 + \zeta^j T_1 + \zeta^{2j} T_2 + \cdots + \zeta^{(p-1)j} T_{p-1}).$$

さらに，

$$U(\varGamma) = \operatorname{Spec} \mathbb{Z}[T_0, T_1, \dots, T_{p-1}, \frac{1}{\varDelta_p(T_0, T_1, \dots, T_{p-1})}]$$

で, 乗法は

$$T_i \mapsto \sum_{\substack{j+k\equiv i \\ \bmod p}} T_j \otimes T_k \quad (1 \leq i \leq p-1)$$

によって定義される.

また, 群スキームの準同型

$$\begin{aligned}\chi_p : U(\varGamma) = \operatorname{Spec} \mathbb{Z}\bigl[T_0, T_1, \ldots, T_{p-1}, \frac{1}{\varDelta_p(T_0, T_1, \ldots, T_{p-1})}\bigr] \\ \longrightarrow \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} = \operatorname{Spec} \mathbb{Z}[X_1, X_2, \ldots, X_{p-1}, \frac{1}{N_p(X_1, X_2, \ldots, X_{p-1})}]\end{aligned}$$

は

$$X_i \mapsto T_i - T_0 \quad (1 \leq i \leq p-1)$$

によって定義される.

一方, $\mathbb{Z}[1/p]$ の上の群スキームの準同型

$$\begin{aligned}\sigma : \Bigl(\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}\Bigr) \otimes_{\mathbb{Z}} \mathbb{Z}[1/p] = \operatorname{Spec} \mathbb{Z}[\frac{1}{p}][X_1, X_2, \ldots, X_{p-1}, \frac{1}{N_p(X_1, X_2, \ldots, X_{p-1})}] \\ \longrightarrow U(\varGamma)_{\mathbb{Z}[1/p]} = \operatorname{Spec} \mathbb{Z}[\frac{1}{p}]\bigl[T_0, T_1, \ldots, T_{p-1}, \frac{1}{\varDelta_p(T_0, T_1, \ldots, T_{p-1})}\bigr]\end{aligned}$$

を

$$T_i \mapsto \begin{cases} \dfrac{1}{p}(1 - X_1 - X_2 - \cdots - X_{p-1}) & (i = 0) \\ X_j - \dfrac{1}{p}(1 - X_1 - X_2 - \cdots - X_{p-1}) & (i > 0) \end{cases}$$

によって定義すれば, 群スキームの可換図式

$$\begin{array}{ccc} \varGamma & \longrightarrow & \Bigl(\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}\Bigr) \otimes_{\mathbb{Z}} \mathbb{Z}[1/p] \\ \Big\| & & \Big\downarrow \sigma \\ \varGamma & \longrightarrow & U(\varGamma)_{\mathbb{Z}[1/p]} \end{array}$$

を得る.

$G = \operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ とおき, g を G の生成元とする. また,

$$\theta = \sum_{k=0}^{p-2} n_k g^k \in \mathbb{Z}[G]$$

とする. このとき, R を環とすれば,

$$\theta(r \otimes \alpha) = \prod_{k=0}^{p-2} \bigl(r \otimes g^k(\alpha)\bigr)^{n_k}$$

によって乗法群の準同型 $\theta : (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])^\times \to (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])^\times$ が定義される. 準同型 θ は群スキームの準同型 $\theta : \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ によって表現される.

例えば,

$$\sigma = g - 1 \in \mathbb{Z}[G]$$

とおく．このとき, 群スキームの準同型 $\sigma : \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ から群スキームの準同型 $\sigma : \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} \to \prod^{(1)}_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ が誘導される．さらに, 図式

$$\begin{array}{ccc} \mathit{\Gamma} & \longrightarrow & \displaystyle\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} \\ \big\downarrow \wr & & \big\downarrow \sigma \\ \mathit{\Gamma} & \longrightarrow & \displaystyle\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}}{}^{(1)} \mathbb{G}_{m,\mathbb{Z}[\zeta]} \end{array}$$

は可換．これからさらに, 可換図式

$$\begin{array}{ccc} \mathit{\Gamma} & \longrightarrow & U(\mathit{\Gamma}) \\ \big\downarrow \wr & & \big\downarrow \sigma \\ \mathit{\Gamma} & \longrightarrow & \displaystyle\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}}{}^{(1)} \mathbb{G}_{m,\mathbb{Z}[\zeta]} \end{array}$$

を得る．

さらに,

$$\tilde{\sigma} = \prod_{\substack{d|(p-1) \\ d \neq p-1}} \mathit{\Phi}_d(g)$$

とおけば, $\tilde{\sigma} : \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ から群スキームの準同型 $\tilde{\sigma} : \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} \to \boldsymbol{G}_p$ が誘導される．さらに, 図式

$$\begin{array}{ccc} \mathit{\Gamma} & \longrightarrow & \displaystyle\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} \\ \big\downarrow \wr & & \big\downarrow \tilde{\sigma} \\ \mathit{\Gamma} & \longrightarrow & \boldsymbol{G}_p \end{array}$$

は可換．これからさらに, 可換図式

$$\begin{array}{ccc} \mathit{\Gamma} & \longrightarrow & U(\mathit{\Gamma}) \\ \big\downarrow \wr & & \big\downarrow \\ \mathit{\Gamma} & \longrightarrow & \boldsymbol{G}_p \end{array}$$

を得る．

例 3.1. $p = 3$ とし, $\zeta = e^{2\pi i/3}$ とおく．このとき,

$$N_3(U, V) = U^2 - UV + V^2.$$

また,

$$\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} = \operatorname{Spec} \mathbb{Z}[U, V, \frac{1}{U^2 - UV + V^2}],$$

$$\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}}{}^{(1)} \mathbb{G}_{m,\mathbb{Z}[\zeta]} = \operatorname{Spec} \mathbb{Z}[U, V]/(U^2 - UV + V^2 - 1)$$

で, いずれも乗法は

$$U \mapsto -U \otimes V - V \otimes U + V \otimes V,\ V \mapsto -U \otimes V - V \otimes U + U \otimes U$$

によって与えられる.

$g(\zeta) = \zeta^2$ によって $g \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ を定義すれば, $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{I, g\}$. 群スキーム $\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ の自己同型 g は

$$U \mapsto V,\ V \mapsto U$$

によって定義される. さらに, 群スキームの準同型

$$\begin{aligned}\sigma : \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} = \mathrm{Spec}\,\mathbb{Z}[U, V, \frac{1}{U^2 - UV + V^2}] \\ \longrightarrow \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}}{}^{(1)}\mathbb{G}_{m,\mathbb{Z}[\zeta]} = \mathrm{Spec}\,\mathbb{Z}[U, V]/(U^2 - UV + V^2 - 1)\end{aligned}$$

は

$$U \mapsto \frac{U^2 - 2UV}{U^2 - UV + V^2},\ V \mapsto \frac{V^2 - 2UV}{U^2 - UV + V^2}$$

によって定義される.

さらに, 完全系列の可換図式

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathit{\Gamma} & \longrightarrow & \Big(\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}\Big) \otimes_{\mathbb{Z}} \mathbb{Z}[1/p] & \xrightarrow{g+2} & \Big(\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}\Big) \otimes_{\mathbb{Z}} \mathbb{Z}[1/p] & \longrightarrow & 0 \\
 & & \downarrow\wr & & \downarrow\sigma & & \downarrow\sigma & & \\
0 & \longrightarrow & \mathit{\Gamma} & \longrightarrow & \Big(\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}}{}^{(1)}\mathbb{G}_{m,\mathbb{Z}[\zeta]}\Big) \otimes_{\mathbb{Z}} \mathbb{Z}[1/p] & \xrightarrow{3} & \Big(\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}}{}^{(1)}\mathbb{G}_{m,\mathbb{Z}[\zeta]}\Big) \otimes_{\mathbb{Z}} \mathbb{Z}[1/p] & \longrightarrow & 0
\end{array}$$

を得る.

系 3.2. R を $\mathbb{Z}[1/3]$ 代数, $a, b \in R$ とし, $a^2 - ab + b^2 = 1$ と仮定する. このとき,

$$S = R[U, V]/(U^2 - UV + V^2 - 1, 3U^2V - U^3 - V^3 - a, 3UV^2 - U^3 - V^3 - b)$$

とおけば, S/R は不分岐 3 次巡回拡大. α, β をそれぞれ U, V の S における像とすれば, $\mathrm{Gal}(S/R)$ は $(\alpha, \beta) \mapsto (-\beta, \alpha - \beta)$ によって生成される. さらに, $\{(1 - \alpha - \beta)/3, (1 - \alpha + 2\beta)/3, (1 + 2\alpha - \beta)/3\}$ は不分岐拡大 S/R の正規底.

補註 3.3. $T = (1 + U)/V$ とおけば, 3 次巡回拡大の生成多項式 $T^3 + 3cT^2 - 3(1 + c)T + 1$ を得る ([9],[14, Cor.3.12]). $T^3 + 3cT^2 - 3(1 + c)T + 1$ の判別式は $81(c^2 + c + 1)^2$.

R を $\mathbb{Z}[1/3]$ 代数, $c \in R$ とし, $c^2 + c + 1 \in R^\times$ と仮定する. このとき,

$$S = R[T]/(T^3 + 3cT^2 - 3(1 + c)T + 1)$$

とおけば, S/R は不分岐巡回 3 次拡大. α を T の S における像とすれば, $\mathrm{Gal}(S/R)$ は $\alpha \mapsto (\alpha - 1)/\alpha$ によって生成される. さらに,

$$\frac{1}{3}\Big(\frac{\alpha + \zeta^{-1}}{\alpha + \zeta} + 1 + \frac{\alpha + \zeta^{-1}}{\alpha + \zeta^{-1}}\Big) = \frac{\alpha^2 - \alpha}{\alpha^2 - \alpha + 1}$$

は S/R の正規底を生成する.

4 Kummer-Artin-Schreier 理論との関係

A を環, $\lambda \in A$ とする.

$$\mathcal{G}^{(\lambda)} = \operatorname{Spec} A\big[T, \frac{1}{1+\lambda T}\big]$$

とする.

$$T \mapsto T \otimes 1 + 1 \otimes T + \lambda T \otimes T$$

によって乗法を定義すれば, $\mathcal{G}^{(\lambda)}$ は可換群スキームとなる. さらに, 群スキームの準同型

$$\alpha^{(\lambda)} : \mathcal{G}^{(\lambda)} = \operatorname{Spec} A\big[T, \frac{1}{1+\lambda T}\big] \to \mathbb{G}_{m,A} = \operatorname{Spec} A\big[U, \frac{1}{U}\big]$$

を

$$U \mapsto 1 + \lambda T$$

によって定義する. λ が A において可逆なら, $\alpha^{(\lambda)}$ は同型. 一方, λ が A で可逆でないとき, $A_0 = A/(\lambda)$ とすれば, $\mathcal{G}^{(\lambda)} \otimes_A A_0$ は $\mathbb{G}_{a,A_0}$ に他ならない.

以下, p を素数とし, $\zeta = e^{2\pi i/p}$, $\lambda = \zeta - 1$ とおく. このとき,

$$\frac{(1+\lambda T)^p - 1}{\lambda^p} \in \mathbb{Z}[\zeta][T]$$

で

$$\frac{(1+\lambda T)^p - 1}{\lambda^p} \equiv T^p - T \bmod \lambda.$$

群スキームの準同型 $\Psi : \mathcal{G}^{(\lambda)} \to \mathcal{G}^{(\lambda^p)}$ を

$$T \mapsto \frac{(1+\lambda T)^p - 1}{\lambda^p}$$

によって定義する. $\operatorname{Ker}[\Psi : \mathcal{G}^{(\lambda)} \to \mathcal{G}^{(\lambda^p)}]$ は $\mathbb{Z}/p\mathbb{Z}$ に同型. さらに, 完全列の可換図式

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \mathcal{G}^{(\lambda)} & \xrightarrow{\Psi} & \mathcal{G}^{(\lambda^p)} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \alpha^{(\lambda)}} & & \downarrow{\scriptstyle \alpha^{(\lambda^p)}} & & \\
0 & \longrightarrow & \boldsymbol{\mu}_{p,\mathbb{Z}[\zeta]} & \longrightarrow & \mathbb{G}_{m,\mathbb{Z}[\zeta]} & \xrightarrow[p]{} & \mathbb{G}_{m,\mathbb{Z}[\zeta]} & \longrightarrow & 0
\end{array}$$

を得る. したがって,

$$[0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathcal{G}^{(\lambda)} \xrightarrow{\Psi} \mathcal{G}^{(\lambda^p)} \longrightarrow 0] \otimes_{\mathbb{Z}[\zeta]} \mathbb{Q}(\zeta)$$

は Kummer sequence

$$0 \longrightarrow \boldsymbol{\mu}_{p,\mathbb{Q}(\zeta)} \longrightarrow \mathbb{G}_{m,\mathbb{Q}(\zeta)} \xrightarrow{p} \mathbb{G}_{m,\mathbb{Q}(\zeta)} \to 0$$

に同型. また, $\mathbb{F}_p = \mathbb{Z}[\zeta]/(\lambda)$ で

$$[0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathcal{G}^{(\lambda)} \xrightarrow{\Psi} \mathcal{G}^{(\lambda^p)} \longrightarrow 0] \otimes_{\mathbb{Z}[\zeta]} \mathbb{F}_p$$

は Artin-Schreier sequence

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{G}_{a,\mathbb{F}_p} \xrightarrow{F-1} \mathbb{G}_{a,\mathbb{F}_p} \longrightarrow 0$$

に他ならない.

補註 4.1. 完全列 (#) は Waterhouse[18] と [12] によって独立に発見された. 方程式

$$\frac{(1+\lambda t)^p - 1}{\lambda^p} = a$$

は Furtwängler の仕事 [2], [3] に遡る.

$\{1, 1+\zeta, \dots, 1+\zeta+\cdots+\zeta^{p-2}\}$ は $\mathbb{Z}[\zeta]$ の $\mathbb{Z}$ の上の基底. したがって, R を環とすれば, $R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta]$ の元は

$$\begin{aligned} &a_1 \otimes 1 + a_2 \otimes (1+\zeta) + \cdots + a_{p-1} \otimes (1+\zeta+\cdots+\zeta^{p-2}) \\ &\qquad = a_1 \otimes \frac{\zeta-1}{\zeta-1} + a_2 \otimes \frac{\zeta^2-1}{\zeta-1} + \cdots + a_{p-1} \otimes \frac{\zeta^{p-1}-1}{\zeta-1} \quad (a_1, a_2, \dots, a_{p-1} \in R) \end{aligned}$$

の形に一意的に表わせる. ここで,

$$1\otimes 1 + (1\otimes\lambda)\Big\{\sum_{i=1}^{p-1} a_i \otimes \frac{\zeta^i - 1}{\zeta - 1}\Big\} = 1\otimes 1 + \sum_{i=1}^{p-1} a_i \otimes (\zeta^i - 1) = \sum_{i=1}^{p-1} (-1 + a_1 + \cdots + 2a_i + \cdots + a_{p-1}) \otimes \zeta^i.$$

さらに,

$$\begin{aligned} &N_p(-1+2X_1+X_2+\cdots+X_{p-1}, -1+X_1+2X_2+\cdots+X_{p-1}, \dots, -1+X_1+X_2+\cdots+2X_{p-1}) \\ &\qquad = 1 + p\tilde{N}_p(X_1, X_2, \dots, X_{p-1}) \end{aligned}$$

とおけば, $\tilde{N}(X_1, X_2, \dots, X_{p-1}) \in \mathbb{Z}[X_1, X_2, \dots, X_{p-1}]$. したがって,

$$\begin{aligned} &1 \otimes 1 + (1 \otimes \lambda)\big\{a_1 \otimes 1 + a_2 \otimes (1+\zeta) + \cdots + a_{p-1} \otimes (1+\zeta+\cdots+\zeta^{p-2})\big\} \in (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])^\times \\ &\qquad \Leftrightarrow \ 1 + p\tilde{N}_p(a_1, a_2, \dots, a_{p-1}) \in R^\times. \end{aligned}$$

これから,

$$\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} = \operatorname{Spec} \mathbb{Z}[X_1, X_2, \dots, X_{p-1}, \frac{1}{1 + p\tilde{N}_p(X_1, X_2, \dots, X_{p-1})}].$$

また, 乗法は

$$\begin{aligned} X_i \mapsto\ & X_i \otimes (1 - X_1 - X_2 - \cdots - X_{p-1}) \\ &+ (1 - X_1 - X_2 - \cdots - X_{p-1}) \otimes X_i + \sum_{\substack{j+k \equiv i \\ \mathrm{mod}\ p}} X_j \otimes X_k \quad (1 \le i \le p-1) \end{aligned}$$

によって定義される.

また, 群スキームの準同型

$$\begin{aligned} \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \alpha^{(\lambda)} : \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} &= \operatorname{Spec} \mathbb{Z}[X_1, X_2, \dots, X_{p-1}, \frac{1}{1 + p\tilde{N}_p(X_1, X_2, \dots, X_{p-1})}] \\ &\longrightarrow \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} = \operatorname{Spec} \mathbb{Z}[X_1, X_2, \dots, X_{p-1}, \frac{1}{N_p(X_1, X_2, \dots, X_{p-1})}] \end{aligned}$$

は

$$X_i \mapsto -1 + X_1 + \cdots + 2X_i + \cdots + X_{p-1} \quad (1 \leq i \leq p-1)$$

によって定義される. $\displaystyle\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \alpha^{(\lambda)}$ は $\mathbb{Z}[1/p]$ の上で同型で, 逆射は

$$X_i \mapsto X_i + \frac{1}{p}(1 - X_1 - \cdots - X_{p-1}) \quad (1 \leq i \leq p-1)$$

によって与えられる.

R を環とする. このとき, 対応

$$\begin{aligned} &a_1 \otimes 1 + a_2 \otimes (1+\zeta) + \cdots + a_{p-1} \otimes (1 + \zeta + \cdots + \zeta^{p-2}) \\ &\qquad\qquad \mapsto (1 - a_1 - a_2 - \cdots - a_{p-1}) + a_1\gamma + a_2\gamma^2 + \cdots + a_{p-1}\gamma^{p-1} \end{aligned}$$

によって群の準同型

$$\tilde{\iota} : \Big(\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)}\Big)(R) = \mathcal{G}^{(\lambda)}(R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta]) \to R[\varGamma]^{\times}$$

が定義される. 準同型 $\tilde{\iota}$ を表現する群スキームの準同型

$$\begin{aligned} \tilde{\iota} : \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} = \operatorname{Spec} \mathbb{Z}[X_1, X_2, \ldots, X_{p-1}, \frac{1}{1 + p\tilde{N}_p(X_1, X_2, \ldots, X_{p-1})}] \to \\ U(\varGamma) = \operatorname{Spec} \mathbb{Z}\big[T_0, T_1, \ldots, T_{p-1}, \frac{1}{\varDelta_p(T_0, T_1, \ldots, T_{p-1})}\big] \end{aligned}$$

は対応

$$T_j \mapsto \begin{cases} 1 - X_1 - \ldots - X_{p-1} & (j = 0) \\ X_j & (j > 0) \end{cases}$$

によって定義される. 群スキームの列

$$0 \longrightarrow \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \xrightarrow{\tilde{\iota}} U(\varGamma) \xrightarrow{\varepsilon} \mathbb{G}_{m,\mathbb{Z}} \longrightarrow 0$$

は完全. また,

$$1 \mapsto 0,\ \gamma \mapsto 1,\ \gamma^2 \mapsto 1 + \zeta, \ldots,\ \gamma^{p-1} \mapsto 1 + \zeta + \cdots + \zeta^{p-2}$$

によって群スキームの埋め込み

$$\varGamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)}$$

が定義される. さらに, 群スキームの図式

$$\begin{array}{ccc} \varGamma & \longrightarrow & \displaystyle\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \\ \| & & \downarrow{\scriptstyle \tilde{\iota}} \\ \varGamma & \longrightarrow & U(\varGamma) \end{array}$$

は可換.

一方, 群スキームの埋め込み $\tilde{\iota}: \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \to U(\Gamma)$ の切断

$$\begin{aligned}\tilde{\chi}: U(\Gamma) = \operatorname{Spec}\mathbb{Z}\big[T_0, T_1, \ldots, T_{p-1}, \frac{1}{\Delta_p(T_0, T_1, \ldots, T_{p-1})}\big] \\ \longrightarrow \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} = \operatorname{Spec}\mathbb{Z}[X_1, X_2, \ldots, X_{p-1}, \frac{1}{1 + p\tilde{N}_p(X_1, X_2, \ldots, X_{p-1})}]\end{aligned}$$

が

$$X_j \mapsto \frac{T_j}{T_0 + T_1 + \cdots + T_{p-1}}$$

によって定義される. このとき, 群スキームの図式

$$\begin{array}{ccc} \Gamma & \longrightarrow & U(\Gamma) \\ \| & & \big\downarrow \tilde{\chi} \\ \Gamma & \longrightarrow & \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \end{array}$$

は可換. また, 群スキームの図式

$$\begin{array}{ccc} \Gamma & \longrightarrow & \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \\ \| & & \big\downarrow \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \alpha^{(\lambda)} \\ \Gamma & \longrightarrow & \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} \end{array}$$

は可換.

$G = \operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ とおき, $\theta \in \mathbb{Z}[G]$ とする. このとき, R を環とすれば, 乗法群の準同型 $\theta: (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])^\times \to (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])^\times$ は群の準同型 $\theta: \mathcal{G}^{(\lambda)}(R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta]) \to \mathcal{G}^{(\lambda)}(R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])$ を誘導する. 準同型 θ は群スキームの準同型 $\theta: \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)}$ によって表現される.

g を G の生成元とし,

$$\nu = 1 + g + \cdots + g^{p-1} \in \mathbb{Z}[G]$$

とおく.

$${\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}}}^{(1)} \mathcal{G}^{(\lambda)} = \operatorname{Ker}\Big[\nu: \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)}\Big]$$

と定義する. このとき, 群スキームの可換図式

$$\begin{array}{ccc} {\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}}}^{(1)} \mathcal{G}^{(\lambda)} & \longrightarrow & \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \\ \big\downarrow & & \big\downarrow \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \alpha^{(\lambda)} \\ {\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}}}^{(1)} \mathbb{G}_{m,\mathbb{Z}[\zeta]} & \longrightarrow & \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} \end{array}$$

を得る.

さらに,

$$\sigma = g - 1 \in \mathbb{Z}[G]$$

とおけば, 群スキームの準同型 $\sigma : \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)}$ から群スキームの準同型 $\sigma : \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \to \prod^{(1)}_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)}$ が誘導される. さらに, 図式

$$\begin{array}{ccc} \mathit{\Gamma} & \longrightarrow & \prod\limits_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \\ \big\downarrow \wr & & \big\downarrow \sigma \\ \mathit{\Gamma} & \longrightarrow & \prod\limits_{\mathbb{Z}[\zeta]/\mathbb{Z}}{}^{(1)} \mathcal{G}^{(\lambda)} \end{array}$$

は可換. これからさらに, 可換図式

$$\begin{array}{ccc} \mathit{\Gamma} & \longrightarrow & U(\mathit{\Gamma}) \\ \big\downarrow \wr & & \big\downarrow \sigma \\ \mathit{\Gamma} & \longrightarrow & \prod\limits_{\mathbb{Z}[\zeta]/\mathbb{Z}}{}^{(1)} \mathcal{G}^{(\lambda)} \end{array}$$

を得る.

同様の議論によって, $\boldsymbol{G}_p$ の Kummer-Artin-Schreier version $\tilde{\boldsymbol{G}}_p$ が定義され, 群スキームの埋め込み $\mathit{\Gamma} \to \tilde{\boldsymbol{G}}_p$ に対しても sculpture problem と embedding problem がともに肯定的であることを示せる.

例 4.2. $p = 3$ とし, $\zeta = e^{2\pi i/3}$ とおく. このとき,

$$\tilde{N}_3(U, V) = -U - V + U^2 + UV + V^2.$$

したがって,

$$\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} = \operatorname{Spec} \mathbb{Z}[U, V, \frac{1}{1 + 3(-U - V + U^2 + UV + V^2)}],$$
$$\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}}{}^{(1)} \mathcal{G}^{(\lambda)} = \operatorname{Spec} \mathbb{Z}[U, V]/(-U - V + U^2 + UV + V^2)$$

で, いずれも乗法は

$$U \mapsto U \otimes (1 - U - V) + (1 - U - V) \otimes U + V \otimes V,$$
$$V \mapsto V \otimes (1 - U - V) + (1 - U - V) \otimes V + U \otimes U$$

によって与えられる.

補註 4.3. $T = (1 + U)/V$ とおけば, 3 次巡回拡大の生成多項式 $T^3 + (1 - c)T^2 - (4 - c)T + 1$ を得る ([7], [14]). $T^3 + (1 - c)T^2 - (4 - c)T + 1$ の判別式は $(c^2 - 5c + 13)^2$.

R を環, $c \in R$ とし, $c^2 - 5c + 13 \in R^\times$ と仮定する. このとき,

$$S = R[T]/(T^3 + (1 - c)T^2 - (4 - c)T + 1)$$

とおけば, S/R は不分岐巡回 3 次拡大. α を T の S における像とすれば, $\mathrm{Gal}(S/R)$ は $\alpha \mapsto (\alpha - 1)/\alpha$ によって生成される. さらに, $(\alpha^2 - \alpha)/(\alpha^2 - \alpha + 1)$ は S/R の正規底を生成する.

参考文献

[1] M. Demazure and P. Gabriel, Groupes algébriques, Tome I, Masson, Paris and North-Holland Publishing, Amsterdam, 1970.

[2] P. Furtwängler, Über die Reziprozitätsgesetze der ℓ-ten Potenzreste in algebraischen Zahl-körpern, wenn ℓ eine ungerade Primzahl bedeutet, Math. Ann. **58** (1904), 1–50.

[3] P. Furtwängler, Allgemeiner Existenzbeweis für den Klassenkörper eines bebliegen Zahlkörpers, Math. Ann. **63** (1907), 1–37.

[4] K. Hashimoto and Y. Rikuna, On generic families of cyclic polynomials with even degree, Manuscripta Math. **107** (2002), 283–288.

[5] M. Kida, Kummer theory for norm algebraic tori, J. Algebra **293** (2005), 427–447.

[6] M. Kida, Descent Kummer theory via Weil restriction of multiplicative groups, J. Number Theory **130** (2010), 639–659.

[7] T. Komatsu, Arithmetic of Rikuna's generic cyclic polynomial and generalization of Kummer theory, Manuscripta Math. **114** (2004), 265–279.

[8] B. Mazur, K. Rubin and A. Silverberg, Twisting commutative algebraic groups, J. Algebra **314** (2007), 419–438.

[9] Y. Rikuna, On simple families of cyclic polynomials, Proc. Amer. Math. Soc. **130** (2002), 2215–2218.

[10] T. Sekiguchi and N. Suwa, Théorie de Kummer-Artin-Schreier, C. R. Acad. Sci. Paris Sér. I Math. **312** (1991), 418–420.

[11] T. Sekiguchi and N. Suwa, On the structure of the group scheme $\mathbb{Z}[\mathbb{Z}/p^n]^\times$, Compos. Math. **97** (1995), 253–271.

[12] T. Sekiguchi, F. Oort and N. Suwa, On the deformation of Artin-Schreier to Kummer, Ann. Sci. École Norm. Sup. (4) **22** (1989), 345–375.

[13] J.-P. Serre, Groupes algébriques et corps de classes, Publications de l'institut de mathématique de l'université de Nancago, Hermann, Paris, 1959.

[14] N. Suwa, Twisted Kummer and Kummer-Artin-Schreier theories, Tohoku Math. J. (2) **60** (2008), 183–218.

[15] N. Suwa, Around Kummer theories, In: Algebraic number theory and related topics 2007, 115–148, RIMS Kokyuroku Bessatsu, B12, Res. Inst. Math. Sci., Kyoto, 2009.

[16] N. Suwa, Artin-Schreier-Witt extensions and normal bases, Hiroshima Math. J. **44** (2012), 325–354.

[17] N. Suwa, algebraic torus に対する Kummer 理論と正規底問題, 早稲田大学整数論研究集会 2013 報告集, 掲載予定.

[18] W. C. Waterhouse, A unified Kummer-Artin-Schreier sequence, Math. Ann. **277** (1987), 447–451.