Tokyo J. Math.
Vol. 39, No. 3, 2017

Kummer Theories for Algebraic Tori and Normal Basis Problem

Dedicated to Professor Ken-ichi SHINODA with gratitude

Noriyuki SUWA

Chuo University

Abstract. We discuss the inverse Galois problem with normal basis, concerning Kummer theories for algebraic tori, in the framework of group schemes. The unit group scheme of a group algebra plays an important role in this article, as was pointed out by Serre [8]. We develop our argument not only over a field but also over a ring, considering integral models of Kummer theories for algebraic tori.

Introduction

The inverse Galois problem is nowadays a very attractive topic and there is a vast accumulation of results concerning the problem. We can divide the problem into two parts:
(A) Given a field k and a finite group Γ, examine the existence of Galois extensions of k with Galois group Γ;
(B) Given a field k and a finite group Γ, construct Galois extensions of k with Galois group Γ.

The Kummer theory is the simplest example of affirmative solution for the inverse Galois problem. It provides us with an explicit way to construct the cyclic extensions of degree n when n is invertible in k and k contains all the n-th roots of unity. We have several manners to establish the Kummer theory, and it would be the most elementary to verify the Kummer theory by Lagrange resolvents. In [8, Ch.VI, 8] Serre formulated this method, combining the normal basis theorem and the unit group scheme of a group algebra.

In the previous articles [10] and [11], we examined several theories of Kummer type, including Kummer, Artin-Schreier, Artin-Schreier-Witt and Kummer-Artin-Schreier theories, formulating Serre's method as the sculpture problem and adding the embedding problem. Now we explain briefly a point of our argument.

Let Γ be a finite group, and let $U(\Gamma)$ denote the unit group scheme of the group algebra of Γ. (For the definition of $U(\Gamma)$, see Section 1.) It is the starting point of our argument that

Received April 1, 2015; revised March 5, 2016
2010 *Mathematics Subject Classification*: 13B05 (Primary), 14L15, 12G05 (Secondary)
Partially supported by Grant-in-Aid for Scientific Research No.23540027 and No.26400024.

the morphism $U(\varGamma) \to U(\varGamma)/\varGamma$ is a versal family of unramified $\varGamma$-extensions with normal basis. That is to say, we have the following assertion:
(A) Let R be a ring, $\varGamma$ a finite group and S/R an unramified Galois extension with Galois group $\varGamma$. Then the Galois extension S/R has a normal basis if and only if there exist morphisms $\operatorname{Spec} S \to U(\varGamma)$ and $\operatorname{Spec} R \to U(\varGamma)/\varGamma$ such that the diagram

$$\begin{array}{ccc} \operatorname{Spec} S & \longrightarrow & U(\varGamma) \\ \downarrow & & \downarrow \\ \operatorname{Spec} R & \longrightarrow & U(\varGamma)/\varGamma \end{array}$$

is cartesian.

In [8, Ch.VI, 8] Serre established this assertion over a field, however, it is not difficult to paraphrase his argument over a ring. Furthermore, it would be interesting to propose the problem whether the following assertions hold true:
(Sculpture problem) Let $\varGamma$ be a finite group and R a ring. Given an affine group R-scheme G and an embedding $i : \varGamma \to G$, there exists a commutative diagram

$$\begin{array}{ccc} \varGamma & \longrightarrow & U(\varGamma)_R \\ \downarrow\wr & & \downarrow \\ \varGamma & \xrightarrow{i} & G\,. \end{array}$$

(Embedding problem) Let $\varGamma$ be a finite group and R a ring. Given an affine group R-scheme G and an embedding $i : \varGamma \to G$, there exists a commutative diagram

$$\begin{array}{ccc} \varGamma & \xrightarrow{i} & G \\ \downarrow\wr & & \downarrow \\ \varGamma & \longrightarrow & U(\varGamma)_R\,. \end{array}$$

If both the sculpture and embedding problems are affirmatively solved for $i : \varGamma \to G$, then the morphism $G \to G/\varGamma$ is a versal family over R of unramified $\varGamma$-extensions with normal basis. In other words, we study the inverse Galois problem with normal basis in the framework of group schemes, extracting the sculpture and embedding problems from the inverse Galois problem.

In the previous works, we treated the sculpture and embedding problems concerning
(1) the Kummer theory ([10, Corollary 2.3]);
(2) the Kummer-Artin-Schreier theory ([10, Corollary 2.7]);
(3) the Artin-Schreier theory ([10, Corollary 2.10]);
(4) the quadratic-twisted Kummer theory of odd degree ([10, Corollary 3.6]);
(5) the quadratic-twisted Kummer theory of even degree ([10, Corollary 3.12]);
(6) the quadratic-twisted Kummer-Artin-Schreier theory ([10, Corollary 4.4]);

(7) the Artin-Schreier-Witt theory ([11, Theorem 2.5]).

In this article, we study the sculpture and embedding problems concerning Kummer theories for algebraic tori, on which Kida developed his arguments in [2] and [3] generalizing the classical Kummer theory to describe the cyclic extensions of degree n of a field without n-th roots of unity. We proceed our argument not only over a field but also over a ring, considering integral models of Kummer theories for algebraic tori, while the base field is restricted to be the rational number field $\mathbb{Q}$. The following list shows which proposition replies to which problem:

(1) Proposition 3.4: the sculpture problem concerning the Kummer theory for Weil restrictions;

(2) Theorem 3.6: the embedding problem concerning the Kummer theory for Weil restrictions;

(3) Propositions 4.3 and 4.4: the sculpture problem concerning the Kummer theory for norm tori;

(4) Theorem 4.5: the embedding problem concerning the Kummer theory for norm tori;

(5) Proposition 6.4: the sculpture and embedding problems concerning integral models of the Kummer theory for Weil restrictions;

(6) Proposition 6.11: the sculpture and embedding problems concerning integral models of the Kummer theory for norm tori;

(7) Theorem 6.14: the sculpture and embedding problems concerning integral models of the cyclotomic-twisted Kummer theory.

Now we explain the organization of this article briefly. In Section 1 we recall the sculpture and embedding problems. In Section 2 we recall needed facts on algebraic tori and on group algebras. In fact, Remark 2.10 is the key to Theorem 3.6, Remark 2.7 to Proposition 4.4, and Remark 2.12 to Theorem 4.5. It is crucial that there exists an anti-equivalence between algebraic tori and integral representations of the Galois group. This enables us to translate freely many problems on algebraic tori into the language of rings and modules.

We treat the Kummer theory for Weil restrictions in Section 3, and the Kummer theory for norm tori in Section 4. It would be worthwhile to remark that Proposition 3.4 and Proposition 4.4 reveal an evident difference between the Kummer theories for Weil restrictions and for norm tori.

In Section 5 we mention the isogeny problem concerning Kummer theories for algebraic tori, which is the main subject of Kida [2], [3]. We conclude the article, by discussing the sculpture and embedding problems for analogues of norm tori in the Kummer-Artin-Schreier theory in Section 6.

The author thanks the referees for their careful reading the manuscript.

Notation

For a ring R (not necessarily commutative), $R^\times$ denotes the multiplicative group of invertible elements of R. A ring is assumed to be commutative unless otherwise mentioned.

For an A-algebra B, which is projective of finite type as A-module, $\prod_{B/A}$ denotes the Weil restriction functor with respect to the ring extension B/A.

We use the following notation.

$\mathbb{G}_{a,A}$: the additive group scheme over A
$\mathbb{G}_{m,A}$: the multiplicative group scheme over A
$U(\Gamma)$: recalled in 1.3
$\prod_{B/A}^{(1)} \mathbb{G}_{m,B}$: defined in 2.6
$\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}}^{(1)} \mathcal{G}^{(\lambda)}$: defined in 6.7
$\chi_d : U(\Gamma) \to \prod_{\mathbb{Z}[\zeta_d]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta_d]}$: defined in 2.1
$\mathcal{G}^{(\lambda)}$: recalled in 6.1
$\alpha^{(\lambda)} : \mathcal{G}^{(\lambda)} \to \mathbb{G}_{m,A}$: recalled in 6.1
$\tilde{\chi}$: $\mathrm{Ker}[\varepsilon : U(\Gamma) \to \mathbb{G}_{m,\mathbb{Z}}] \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)}$: defined in 6.3
$s : U(\Gamma) \to \mathrm{Ker}[\varepsilon : U(\Gamma) \to \mathbb{G}_{m,\mathbb{Z}}]$: defined in 6.3

1. Sculpture problem and embedding problem

In this section we recall the sculpture and embedding problems, referring to the previous articles [10] and [11] for details. We refer to [1] or [13] on formalisms of affine group schemes and Hopf algebras.

1.1. As usual we denote by $\mathbb{G}_m = \mathrm{Spec}\,\mathbb{Z}[U, 1/U]$ the multiplicative group scheme and by $\mathbb{G}_a = \mathrm{Spec}\,\mathbb{Z}[T]$ the additive group scheme, respectively. The multiplication is defined by $U \mapsto U \otimes U$, and the addition is defined by $T \mapsto T \otimes 1 + 1 \otimes T$.

1.2. Let Γ be a finite group. The functor $R \mapsto R[\Gamma]$ is represented by the ring scheme $A(\Gamma)$ defined by

$$A(\Gamma) = \mathrm{Spec}\,\mathbb{Z}[T_\gamma\,;\ \gamma \in \Gamma]$$

with

(a) the addition: $T_\gamma \mapsto T_\gamma \otimes 1 + 1 \otimes T_\gamma$;
(b) the multiplication: $T_\gamma \mapsto \sum_{\gamma'\gamma''=\gamma} T_{\gamma'} \otimes T_{\gamma''}$.

Put now

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

where $\Delta_\Gamma = \det(T_{\gamma\gamma'})$ denotes the determinant of the matrix $(T_{\gamma\gamma'})_{\gamma,\gamma'\in\Gamma}$ (the group determinant of Γ). Then $U(\Gamma)$ is an open subscheme of $A(\Gamma)$, and the functor $R \mapsto R[\Gamma]^\times$ is represented by the group scheme $U(\Gamma)$.

We also denote by Γ, for the abbreviation, the constant group scheme defined by Γ. More precisely, $\Gamma = \operatorname{Spec}\mathbb{Z}^\Gamma$ and the law of multiplication is defined by $e_\gamma \mapsto \sum_{\gamma'\gamma''=\gamma} e_{\gamma'} \otimes e_{\gamma''}$. Here $\mathbb{Z}^\Gamma$ denotes the functions from Γ to $\mathbb{Z}$, and $(e_\gamma)_{\gamma\in\Gamma}$ is a basis of $\mathbb{Z}^\Gamma$ over $\mathbb{Z}$ defined by

$$e_\gamma(\gamma') = \begin{cases} 1 & (\gamma' = \gamma) \\ 0 & (\gamma' \neq \gamma)\,. \end{cases}$$

The canonical injection $\Gamma \to R[\Gamma]^\times$ is represented by the homomorphism of group schemes $i : \Gamma \to U(\Gamma)$ defined by

$$T_\gamma \mapsto e_\gamma : \mathbb{Z}\left[T_\gamma, \frac{1}{\Delta_\Gamma}\right] \to \mathbb{Z}^\Gamma\,.$$

It is readily seen that $\Gamma \to U(\Gamma)$ is a closed immersion. Moreover, the right multiplication by $\gamma \in \Gamma$ on $U(\Gamma)$ is defined by the automorphism $\gamma : T_{\gamma'} \mapsto T_{\gamma'\gamma^{-1}}$ of $\mathbb{Z}[T_\gamma, 1/\Delta_\Gamma]$.

If $\Gamma = \{1\}$, then $U(\Gamma)$ is nothing but the multiplicative group scheme $\mathbb{G}_{m,\mathbb{Z}} = \operatorname{Spec}\mathbb{Z}[U, 1/U]$.

DEFINITION 1.3. Let R be a ring, Γ a finite group and S an R-algebra. We shall say that:
(1) S/R is an *unramified Galois extension with Galois group* Γ if Spec S has a structure of right Γ-torsor over Spec R;
(2) an unramified Galois extension S/R with Galois group Γ has a *normal basis* if there exists $s \in S$ such that $(\gamma s)_{\gamma\in\Gamma}$ is a basis of R-module S.

In particular, an unramified Galois extension S/R with Galois group Γ is called an *unramified cyclic extension of degree n* if Γ is a cyclic group of order n.

EXAMPLE 1.4. Let $S = \mathbb{Z}[T_\gamma, 1/\Delta_\Gamma\,;\ \gamma \in \Gamma]$, and let $R = S^\Gamma$ denote the invariants in S under the action of Γ. Then S/R is an unramified Galois extension with Galois group Γ, and $(T_{\gamma^{-1}})_{\gamma\in\Gamma}$ is a normal basis of the Galois extension S/R.

1.5. The morphism $U(\Gamma) \to U(\Gamma)/\Gamma$ is a versal family of unramified Γ-extension with normal basis. That is to say, the following assertion holds true:
(A) Let R be a ring, Γ a finite group and S/R an unramified Galois extension with Galois group Γ. Then the Galois extension S/R has a normal basis if and only if there exist mor-

phisms Spec $S \to U(\Gamma)$ and Spec $R \to U(\Gamma)/\Gamma$ such that the diagram

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

is cartesian.

The assertion (A) implies the following assertions:

(B) Let R be a ring, G an affine group scheme and Γ a constant finite subgroup scheme of G.

(1) Let S/R be an unramified Galois extension with Galois group Γ. Assume that there exists a commutative diagram

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

Then, if the Galois extension S/R has a normal basis, there exist morphisms Spec $S \to G$ and Spec $R \to G/\Gamma$ such that the diagram

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

is cartesian.

(2) Let S/R be the unramified Galois extension with Galois group Γ defined by a cartesian diagram

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

Assume that there exists a commutative diagram

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

Then the Galois extension S/R has a normal basis.

It is now interesting to propose the problem whether the following assertions hold true:

(1) Let Γ be a finite group and R a ring. Given an affine group R-scheme G and an embedding $i : \Gamma \to G$, there exists a commutative diagram

$$\begin{tikzcd} \Gamma \arrow[r] \arrow[d, "\wr"] & U(\Gamma)_R \arrow[d] \\ \Gamma \arrow[r, "i"] & G\,. \end{tikzcd}$$

(2) Let Γ be a finite group and R a ring. Given an affine group R-scheme G and an embedding $i : \Gamma \to G$, there exists a commutative diagram

$$\begin{tikzcd} \Gamma \arrow[r, "i"] \arrow[d, "\wr"] & G \arrow[d] \\ \Gamma \arrow[r] & U(\Gamma)_R\,. \end{tikzcd}$$

The problems shall be called respectively *sculpture problem* and *embedding problem* for the embedding of group schemes $i : \Gamma \to G$.

If both the sculpture and embedding problems are affirmatively solved for $i : \Gamma \to G$, then the morphism $G \to G/\Gamma$ is a versal family over R of unramified Γ-extension with normal basis.

2. Algebraic tori

In this section we recall needed facts on algebraic tori and group algebras. We refer to Demazure-Gabriel [1, Ch.IV, 1] concerning generalities on algebraic tori.

DEFINITION 2.1. Let A be a ring and Γ a finitely generated commutative group. Then the group algebra $A[\Gamma]$ is a Hopf A-algebra equipped with the comultiplication $\gamma \mapsto \gamma \otimes \gamma$. Moreover, $D(\Gamma)_A = \operatorname{Spec} A[\Gamma]$ is a commutative group A-scheme. For example, if $\Gamma = \mathbb{Z}$, then $D(\Gamma)_A = \mathbb{G}_{m,A}$.

DEFINITION 2.2. Let A be a ring and V a group A-scheme of finite type. We say that V is diagonalizable if there exists a finitely generated commutative group Γ such that $D(\Gamma)_A$ is isomorphic to V. Furthermore, we say that V is *of multiplicative type* if there exists an unramified Galois extension B/A such that $V \otimes_R B$ is a diagonalizable group B-scheme. Then $\operatorname{Hom}_{B-\mathrm{gr}}(V_B, \mathbb{G}_{m,B})$ has a left action by $\operatorname{Gal}(B/A)$.

Let V be a group A-scheme of multiplicative type. Assume that $\operatorname{Spec} A$ is connected, and let Π denote the fundamental group. Then $Hom_{A-\mathrm{gr}}(V, \mathbb{G}_{m,A})$ has a continuous left action of Π. The correspondence $V \mapsto Hom_{A-\mathrm{gr}}(V, \mathbb{G}_{m,A})$ gives rise to an anti-equivalence between the category of group A-schemes of multiplicative type and the category of discrete left Π-modules, finitely generated as $\mathbb{Z}$-module. We call the left Π-module $Hom_{A-\mathrm{gr}}(V, \mathbb{G}_{m,A})$ the *character group* of the group A-scheme V of multiplicative type. In particular, V is called an *algebraic torus* if the character group of V is a free $\mathbb{Z}$-module.

EXAMPLE 2.3. Let A be a ring, B/A an unramified Galois extension and $G = \mathrm{Gal}(B/A)$. Then the Weil restriction $\prod_{B/A} \mathbb{G}_{m,B}$ is an algebraic torus with character group $\mathbb{Z}[G]$ (for example, see [13, Theorem 7.5]). Therefore, if $\mathrm{Spec}\, A$ is connected, we have

$$\mathrm{End}_{A-\mathrm{gr}}\Bigl(\prod_{B/A} \mathbb{G}_{m,B}\Bigr) = (\mathrm{End}_{\mathbb{Z}[G]}\mathbb{Z}[G])^{\circ} = \mathbb{Z}[G]\,.$$

Furthermore, let H be a subgroup of G, and put $A' = B^H$. Then the Weil restriction $\prod_{A'/A} \mathbb{G}_{m,A'}$ is an algebraic torus with character group $\mathbb{Z}[G/H]$.

NOTATION 2.4. Let G be a finite group. We define a homomorphism of left $\mathbb{Z}[G]$-modules $\varepsilon_G : \mathbb{Z}[G] \to \mathbb{Z}$ by

$$\sum_{g\in G} a_g g \mapsto \sum_{g \in G} a_g .$$

We put

$$I_G = \mathrm{Ker}\bigl[\varepsilon_G : \mathbb{Z}[G] \to \mathbb{Z}\bigr]\,.$$

Furthermore, let H be a subgroup of G. Then, tensoring $\mathbb{Z}[G]\otimes_{\mathbb{Z}[H]}$ with the exact sequence of left $\mathbb{Z}[H]$-modules

$$0 \longrightarrow I_H \longrightarrow \mathbb{Z}[H] \xrightarrow{\varepsilon_H} \mathbb{Z} \longrightarrow 0\,,$$

we obtain an exact sequence of left $\mathbb{Z}[G]$-modules

$$0 \longrightarrow \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} I_H \longrightarrow \mathbb{Z}[G] \xrightarrow{\mathrm{id}_G \otimes \varepsilon_H} \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} \mathbb{Z} \longrightarrow 0\,.$$

(Here id_G stands for the identity map of $\mathbb{Z}[G]$.) The correspondence $g \otimes 1 \mapsto [g]$ gives rise to an isomorphism of left $\mathbb{Z}[G]$-modules

$$\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} \mathbb{Z} \xrightarrow{\sim} \mathbb{Z}[G/H]\,.$$

Under the identification $\mathbb{Z}[G]\otimes_{\mathbb{Z}[H]}\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}[G/H]$, the map $\mathrm{id}_G \otimes \varepsilon_H : \mathbb{Z}[G] \to \mathbb{Z}[G]\otimes_{\mathbb{Z}[H]} \mathbb{Z}$ is identified with the homomorphism of left $\mathbb{Z}[G]$-modules $\mathbb{Z}[G] \to \mathbb{Z}[G/H]$ defined by

$$\sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g[g]\,.$$

Now define a homomorphism of left $\mathbb{Z}[G]$-modules $\varepsilon_{G/H} : \mathbb{Z}[G/H] \to \mathbb{Z}$ by

$$\sum_{\gamma\in G/H} a_\gamma \gamma \mapsto \sum_{\gamma \in G/H} a_\gamma\,.$$

Then we have $\varepsilon_G = \varepsilon_{G/H} \circ (\mathrm{id}_G \otimes \varepsilon_H)$. We put

$$I_{G/H} = \mathrm{Ker}\bigl[\varepsilon_{G/H} : \mathbb{Z}[G/H] \to \mathbb{Z}\bigr]$$

Then left $\mathbb{Z}[G]$-module $I_{G/H}$ is a free $\mathbb{Z}$-module with basis $\{\gamma - 1\ ;\ \gamma \in G/H,\ \gamma \neq 1\}$.

Now we define a homomorphism of right $\mathbb{Z}[G]$-modules $\varepsilon_{H\backslash G} : \mathbb{Z}[H\backslash G] \to \mathbb{Z}$ by

$$\sum_{\gamma \in H\backslash G} a_\gamma \gamma \mapsto \sum_{\gamma \in H\backslash G} a_\gamma \,,$$

and we put

$$I_{H\backslash G} = \mathrm{Ker}\big[\varepsilon_{H\backslash G} : \mathbb{Z}[H\backslash G] \to \mathbb{Z}\big]\,.$$

The right $\mathbb{Z}[G]$-module $I_{H\backslash G}$ is a free $\mathbb{Z}$-module with basis $\{\gamma - 1\ ;\ \gamma \in H\backslash G,\ \gamma \neq 1\}$.

DEFINITION 2.5. Let G be a finite group. We define a homomorphism of left $\mathbb{Z}[G]$-modules $\nu_G : \mathbb{Z} \to \mathbb{Z}[G]$ by

$$1 \mapsto \sum_{g \in G} g\,,$$

and we put

$$J_G = \mathrm{Coker}\big[\nu_G : \mathbb{Z} \to \mathbb{Z}[G]\big]\,.$$

The left $\mathbb{Z}[G]$-module J_G is a free $\mathbb{Z}$-module with basis $\{[g]\ ;\ g \in G,\ g \neq 1\}$.

Furthermore, let H be a subgroup of G. Then, tensoring $\mathbb{Z}[G]\otimes_{\mathbb{Z}[H]}$ with the exact sequence of left $\mathbb{Z}[H]$-modules

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\nu_H} \mathbb{Z}[H] \longrightarrow J_H \longrightarrow 0\,,$$

we obtain an exact sequence of left $\mathbb{Z}[G]$-modules

$$0 \longrightarrow \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} \mathbb{Z} \xrightarrow{\mathrm{id}_G \otimes \nu_H} \mathbb{Z}[G] \longrightarrow \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} J_H \longrightarrow 0\,.$$

Under the identification $\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} \mathbb{Z} \xrightarrow{\sim} \mathbb{Z}[G/H]$, the map $\mathrm{id}_G \otimes \nu_H : \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} \mathbb{Z} \to \mathbb{Z}[G]$ is identified with the homomorphism of left $\mathbb{Z}[G]$-modules $\mathbb{Z}[G/H] \to \mathbb{Z}[G]$ defined by

$$\sum_{\gamma \in G/H} a_\gamma \gamma \mapsto \sum_{\gamma \in G/H} a_\gamma \bigg(\sum_{g \in \gamma} g\bigg)\,.$$

Now define a homomorphism of left $\mathbb{Z}[G]$-modules $\nu_{G/H} : \mathbb{Z} \to \mathbb{Z}[G/H]$ by

$$1 \mapsto \sum_{\gamma \in G/H} \gamma\,.$$

Then we have $\nu_G = (\mathrm{id}_G \otimes \nu_H) \circ \nu_{G/H}$. We put

$$J_{G/H} = \mathrm{Coker}\big[\nu_{G/H} : \mathbb{Z} \to \mathbb{Z}[G/H]\big]\,.$$

The left $\mathbb{Z}[G]$-module $J_{G/H}$ is a free $\mathbb{Z}$-module with basis $\{[\gamma]\ ;\ \gamma \in G/H,\ \gamma \neq 1\}$.

Now we translate the statements of 2.5 into the language of algebraic tori.

DEFINITION 2.6. Let A be a ring, B/A an unramified Galois extension and $G = \mathrm{Gal}(B/A)$. The the exact sequence of left $\mathbb{Z}[G]$-modules

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\nu} \mathbb{Z}[G] \longrightarrow J_G \longrightarrow 0$$

defines an exact sequence of algebraic tori over A

$$0 \longrightarrow \prod_{B/A}{}^{(1)} \mathbb{G}_{m,B} \longrightarrow \prod_{B/A} \mathbb{G}_{m,B} \xrightarrow{\mathrm{Nr}_{B/A}} \mathbb{G}_{m,A} \longrightarrow 0\,.$$

The algebraic torus

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

is called the *norm torus* associated to the unramified Galois extension B/A. If $\mathrm{Spec}\,A$ is connected, we have

$$\mathrm{End}_{A-\mathrm{gr}}\Big(\prod_{B/A}{}^{(1)} \mathbb{G}_{m,B}\Big) = (\mathrm{End}_{\mathbb{Z}[G]} J_G)^{\circ} = J_G.$$

REMARK 2.7. Let G be a finite group and H be a subgroup of G. Then the correspondence $\varphi \mapsto \varphi(1)$ gives rise to a group isomorphism

$$\mathrm{Hom}_{\mathbb{Z}[G]}(J_G, \mathbb{Z}[G/H]) \xrightarrow{\sim} I_{G/H}\ .$$

In particular, the correspondence $\varphi \mapsto \varphi(1)$ gives rise to a group isomorphism

$$\mathrm{Hom}_{\mathbb{Z}[G]}(J_G, \mathbb{Z}[G]) \xrightarrow{\sim} I_G\ .$$

The statements of 2.7 are translated into the language of algebraic tori as follows.

REMARK 2.8. Let B be a ring, B/A an unramified Galois extension and $G = \mathrm{Gal}(B/A)$. Let H be a subgroup of G and $A' = B^H$. Then, if $\mathrm{Spec}\,A$ is connected, we obtain a group isomorphism

$$\mathrm{Hom}_{A-\mathrm{gr}}\Big(\prod_{A'/A} \mathbb{G}_{m,A'}, \prod_{B/A}{}^{(1)} \mathbb{G}_{m,B}\Big) \xrightarrow{\sim} I_{G/H}$$

since $\prod_{A'/A} \mathbb{G}_{m,A'}$ is an algebraic torus with character group $\mathbb{Z}[G/H]$. In particular, we obtain a group isomorphism

$$\mathrm{Hom}_{A-\mathrm{gr}}\Big(\prod_{B/A} \mathbb{G}_{m,B}, \prod_{B/A}{}^{(1)} \mathbb{G}_{m,B}\Big) \xrightarrow{\sim} I_G.$$

REMARK 2.9. Let G be a group, H a subgroup of G and $\varphi \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G/H], \mathbb{Z}[G])$. Then $\varphi(1)$ is expressed uniquely in the form of

$$\varphi(1) = \sum_{\gamma \in H\backslash G} a_\gamma \left(\sum_{g \in \gamma} g \right).$$

The correspondence

$$\varphi \mapsto \sum_{\gamma \in H\backslash G} a_\gamma \gamma$$

gives rise to a group isomorphism

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G/H], \mathbb{Z}[G]) \xrightarrow{\sim} \mathbb{Z}[H\backslash G].$$

In particular, $\mathrm{id}_G \otimes \nu_H \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G/H], \mathbb{Z}[G])$ corresponds to $1 \in \mathbb{Z}[H\backslash G]$.

Furthermore, if H is a normal subgroup of G, the isomorphism $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G/H], \mathbb{Z}[G]) \xrightarrow{\sim} \mathbb{Z}[G/H]$ is compatible with the right action of the group algebra $\mathbb{Z}[G/H]$. Therefore any $\mathbb{Z}[G]$-homomorphism of $\mathbb{Z}[G/H] \to \mathbb{Z}[G]$ is expressed uniquely in the form of

$$(\mathrm{id}_G \otimes \nu_H)\alpha\,, \quad \alpha \in \mathbb{Z}[G/H].$$

The statements of 2.9 are translated into the language of algebraic tori as follows.

REMARK 2.10. Let A be a ring, B/A an unramified Galois extension and $G = \mathrm{Gal}(B/A)$. Let H be a subgroup of G and $A' = B^H$. Then, if $\mathrm{Spec}\, A$ is connected, we obtain a group isomorphism

$$\mathrm{Hom}_{A-\mathrm{gr}}\left(\prod_{B/A} \mathbb{G}_{m,B}, \prod_{A'/A} \mathbb{G}_{m,A'} \right) \xrightarrow{\sim} \mathbb{Z}[H\backslash G].$$

In particular, if H is a normal subgroup, any homomorphism $\prod_{B/A} \mathbb{G}_{m,B} \to \prod_{A'/A} \mathbb{G}_{m,A'}$ are expressed uniquely in the form of

$$\alpha \circ \mathrm{Nr}_{B/A'},\ \alpha \in \mathbb{Z}[G/H] = \mathrm{End}_{A-\mathrm{gr}}\left(\prod_{A'/A} \mathbb{G}_{m,A'} \right).$$

REMARK 2.11. Let G be a finite group, H a subgroup of G and $\varphi \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G/H], J_G)$. Then $\varphi(1)$ is expressed uniquely in the form of

$$\varphi(1) = \sum_{\substack{\gamma \in H\backslash G \\ \gamma \neq H}} a_\gamma \left(\sum_{g \in \gamma} g \right).$$

The correspondence

$$\varphi \mapsto \sum_{\gamma \in H\backslash G} a_\gamma \gamma$$

gives rise to a group isomorphism

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G/H], J_G) \xrightarrow{\sim} I_{H\backslash G} = \mathrm{Ker}\big[\varepsilon_{H\backslash G} : \mathbb{Z}[H\backslash G] \to \mathbb{Z}\big].$$

In particular, if H is a normal subgroup of G, the isomorphism $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G/H], J_G) \overset{\sim}{\to} I_{G/H} = \mathrm{Ker}\big[\varepsilon_{G/H} : \mathbb{Z}[G/H] \to \mathbb{Z}\big]$ is compatible with the right action of the group algebra $\mathbb{Z}[G/H]$. Therefore any $\mathbb{Z}[G]$-homomorphism $\mathbb{Z}[G/H] \to J_G$ is expressed in the form of

$$\pi \circ (\mathrm{id}_G \otimes \nu_H)\alpha, \ \alpha \in \mathbb{Z}[G/H].$$

Here $\pi : \mathbb{Z}[G] \to J_G = \mathbb{Z}[G]/\mathbb{Z}$ denotes the canonical surjection.

Finally the statements of 2.11 are translated into the language of algebraic tori as follows.

REMARK 2.12. Let A be a ring, B/A an unramified Galois extension and $G = \mathrm{Gal}(B/A)$. Let H be a subgroup of G and $A' = B^H$. Then, if $\mathrm{Spec}\,A$ is connected, we obtain a group isomorphism

$$\mathrm{Hom}_{A-\mathrm{gr}}\Bigg(\prod_{B/A}^{(1)} \mathbb{G}_{m,B}, \prod_{A'/A} \mathbb{G}_{m,A'}\Bigg) \xrightarrow{\sim} I_{H\backslash G} = \mathrm{Ker}\big[\varepsilon_{H\backslash G} : \mathbb{Z}[H\backslash G] \to \mathbb{Z}\big].$$

In particular, if H is a normal subgroup of G, any homomorphism $\prod_{B/A}^{(1)} \mathbb{G}_{m,B} \to \prod_{A'/A} \mathbb{G}_{m,A'}$ is expressed in the form of

$$\alpha \circ \mathrm{Nr}_{B/A'}, \ \alpha \in \mathbb{Z}[G/H] = \mathrm{End}_{A-\mathrm{gr}}\Bigg(\prod_{A'/A} \mathbb{G}_{m,A'}\Bigg).$$

We conclude the section by mentioning the work of Mazur-Rubin-Silverberg [4].

NOTATION 2.13. Let A be a ring, B/A an unramified Galois extension and $G = \mathrm{Gal}(B/A)$. Let R be a ring (not necessarily commutative), and let $\pi : \mathbb{Z}[G] \to R$ be a ring homomorphism. Then by restriction of scalars all the left R-modules can be considered as left $\mathbb{Z}[G]$-module. Then a group A-scheme of multiplicative type is defined for any left R-module, finitely generated as $\mathbb{Z}$-module.

For example, let $\rho : G \to GL(n, \mathbb{Z})$ be a linear representation of G over $\mathbb{Z}$, and put $R_\rho = \mathrm{Im}[\rho : \mathbb{Z}[G] \to M(n, \mathbb{Z})]$. We denote by $\mathbb{G}_m(\rho)$ the algebraic torus over A with character group R_ρ. If $\mathrm{Spec}\,A$ is connected, then we have $\mathrm{End}_{A-\mathrm{gr}}\mathbb{G}_m(\rho) = R_\rho$.

REMARK 2.14. Let A be a ring, B/A an unramified Galois extension and $G = \mathrm{Gal}(B/A)$. Let V be a commutative group A-scheme of finite type. Then a ring homomorphism

$$\mathbb{Z}[G] = \mathrm{End}_{\mathbb{Z}[G]}\mathbb{Z}[G] \to \mathrm{End}_{A-\mathrm{gr}}\Big(\prod_{B/A} V_B\Big)$$

is defined. For an irreducible representation ρ of G, the twist V_ρ of V by ρ is defined as is described in Mazur-Rubin-Silverberg [4]. The twist of $\mathbb{G}_{m,A}$ by ρ is nothing but $\mathbb{G}_m(\rho)$.

In [4] their argument is developed for algebraic groups over a field, but it is not difficult to paraphrase the argument on a ring. For example, the assertion of [4, Remark 5.11] holds true for a ring.

THEOREM 2.15 (Mazur-Rubin-Silverberg). *Let A be a ring, B/A an unramified cyclic extension of degree m and $G = \mathrm{Gal}(B/A)$. Let V be a commutative group A-scheme of finite type. Take a generator g of G and let $\rho : G \to \mathbb{C}^\times$ denote the character of G defined by $\rho(g) = e^{2\pi i/m}$. Then we have*

$$V_\rho = \bigcap_{A\subset A'\subsetneq B} \mathrm{Ker}\Big[\mathrm{Nr}_{B/A'} : \prod_{B/A} V_B \to \prod_{A'/A} V_{A'}\Big].$$

3. Kummer theory for Weil restrictions

In this section, n denotes a positive integer, Γ a cyclic group of order n and γ a generator of Γ. We put $\zeta = \zeta_n = e^{2\pi i/n}$ and $\boldsymbol{\mu}_n = \{1, \zeta, \dots, \zeta^{n-1}\}$.

3.1. Let R be ring. For a positive divisor d of n, we define a ring homomorphism $\chi_{d,R} : R[\Gamma] \to R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_d]$ and a group homomorphism $\chi_{d,R} : R[\Gamma]^\times \to (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_d])^\times$ by

$$\chi_{d,R} : \sum_{k=0}^{n-1} a_k\gamma^k \mapsto \sum_{k=0}^{n-1} a_k \otimes \zeta_d^k .$$

The group homomorphism $\chi_{d,R} : R[\Gamma]^\times \to (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_d])^\times$ is represented by a homomorphism of group schemes

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

Put

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

Then χ is an isomorphism of group schemes over $\mathbb{Z}[1/n]$. Indeed, the inverse is given by

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

REMARK 3.2. Put $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Then, as is mentioned in 2.3, the Weil restriction $\left(\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}\right) \otimes_{\mathbb{Z}} \mathbb{Z}[1/n]$ is an algebraic torus over $\mathbb{Z}[1/n]$ with character group $\mathbb{Z}[G]$ since $\mathbb{Z}[\zeta, 1/n]$ is unramified over $\mathbb{Z}[1/n]$.

Furthermore, for each positive divisor d of n, put $G_d = \mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})$. Then $\mathbb{Z}[G_d]$ is considered as $\mathbb{Z}[G]$-module through the canonical surjection $\mathbb{Z}[G] \to \mathbb{Z}[G_d]$. The Weil restriction $\left(\prod_{\mathbb{Z}[\zeta_d]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta_d]}\right) \otimes_{\mathbb{Z}} \mathbb{Z}[1/n]$ is an algebraic torus over $\mathbb{Z}[1/n]$ with character group $\mathbb{Z}[G_d]$, and therefore $U(\Gamma)_{\mathbb{Z}[1/n]}$ is an algebraic torus over $\mathbb{Z}[1/n]$ with character group $\bigoplus_{d|n} \mathbb{Z}[G_d]$.

OBSERVATION 3.3. Let R be a ring. Then a group homomorphism $\iota_R : \Gamma \to (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])^\times$ is defined by $\gamma \mapsto 1 \otimes \zeta$. Furthermore, the homomorphism $\iota_R : \Gamma \to (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])^\times$ is represented by a homomorphism of group schemes $\iota : \Gamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$.

PROPOSITION 3.4. *Let n be a positive integer.*

(a) If n is odd, the homomorphism $\iota : \Gamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ is an embedding of group schemes. Furthermore, the diagram

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

is commutative, that is to say, the sculpture problem is affirmatively solved over $\mathbb{Z}$ for the embedding $\iota : \Gamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$.

(b) If n is even, the homomorphism $\iota : \Gamma \to \left(\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}\right) \otimes_{\mathbb{Z}} \mathbb{Z}[1/2]$ is an embedding of group schemes over $\mathbb{Z}[1/2]$. Furthermore, the diagram

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

is commutative, that is to say, the sculpture problem is affirmatively solved over $\mathbb{Z}[1/2]$ for the embedding $\iota : \Gamma \to \left(\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}\right) \otimes_{\mathbb{Z}} \mathbb{Z}[1/2]$.

PROOF. Let R be a ring, and let $i, j \in \mathbb{Z}$. Then $1 \otimes \zeta^i, 1 \otimes \zeta^j \in R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta]$ are linearly dependent over R if and only if $\zeta^i = \pm\zeta^j$. Therefore the equality $1 \otimes \zeta^i = 1 \otimes \zeta^j$ holds true if and only if $\zeta^i = \zeta^j$, or $\zeta^i = -\zeta^j$ and $2 = 0$ in R. Then $\iota_R : \Gamma \to (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])^\times$ is injective if n is odd or if n is even and $2 \neq 0$ in R. This implies the assertions of (a) and (b).

REMARK 3.5. There exists uniquely $i(g) \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $g(\zeta) = \zeta^{i(g)}$ for each $g \in G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. As is well known, the correspondence $g \mapsto i(g)$ gives rise to a group isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$. Moreover, we denote by $\mathbb{Z}/n\mathbb{Z}(1)$ the left $\mathbb{Z}[G]$-module $\mathbb{Z}/n\mathbb{Z}$ equipped with the action $(g, l) \mapsto i(g)l$. Then the constant group scheme Γ over $\mathbb{Z}[1/n]$ is a group scheme of multiplicative type with character group $\mathbb{Z}/n\mathbb{Z}(1)$. The embedding of group schemes of multiplicative type $i : \Gamma \to \left(\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}\right) \otimes_{\mathbb{Z}} \mathbb{Z}[1/n]$ induces the $\mathbb{Z}[G]$-homomorphism $\eta_n : \mathbb{Z}[G] \to \mathbb{Z}/n\mathbb{Z}(1)$, which is defined by $1 \mapsto 1 \mod n$.

As is remarked in 3.2, the group scheme $U(\Gamma)_{\mathbb{Z}[1/n]}$ is an algebraic torus over $\mathbb{Z}[1/n]$ with character group $\oplus_{d|n}\mathbb{Z}[G_d]$. Furthermore, $1 \mapsto n/d \mod n$ defines a $\mathbb{Z}[G]$-homomorphism $\eta_d : \mathbb{Z}[G_d] \to \mathbb{Z}/n\mathbb{Z}(1)$. The homomorphism of the character groups corresponding to the embedding $i : \Gamma \to U(\Gamma)_{\mathbb{Z}[1/n]}$ is defined by

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

THEOREM 3.6. *Let n be an integer ≥ 2. Then the following conditions are equivalent.*

(a) *The embedding problem is affirmatively solved over $\mathbb{Z}[1/n]$ for the embedding $\Gamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$.*

(b) *The embedding problem is affirmatively solved over $\mathbb{Q}$ for the embedding $\Gamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$.*

(c) *For each positive divisor d of n, the map $\mathrm{Nr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_d)}$ induces a surjection $\boldsymbol{\mu}_n \to \boldsymbol{\mu}_d$.*

PROOF. (a)⇒(b) Clear. (b)⇒(c) By the assumption, there exists a homomorphism of group scheme $\sigma : \prod_{\mathbb{Q}(\zeta)/\mathbb{Q}} \mathbb{G}_{m,\mathbb{Q}(\zeta)} \to U(\Gamma)_{\mathbb{Q}}$ such that the diagram

$$\begin{array}{ccc}
\Gamma & \longrightarrow & \displaystyle\prod_{\mathbb{Q}(\zeta_n)/\mathbb{Q}} \mathbb{G}_{m,\mathbb{Q}(\zeta_n)} \\
\big\downarrow{\wr} & & \big\downarrow{\sigma} \\
\Gamma & \longrightarrow & U(\Gamma)_{\mathbb{Q}}
\end{array}$$

is commutative. Now let d be a positive divisor n. Then the homomorphism of group schemes

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

induces a surjection $\Gamma \to \boldsymbol{\mu}_d$, and therefore the homomorphism

$$\chi_d \circ \sigma : \prod_{\mathbb{Q}(\zeta_n)/\mathbb{Q}} \mathbb{G}_{m,\mathbb{Q}(\zeta_n)} \to \prod_{\mathbb{Q}(\zeta_d)/\mathbb{Q}} \mathbb{G}_{m,\mathbb{Q}(\zeta_d)}$$

induces a surjection $\Gamma = \boldsymbol{\mu}_n \to \boldsymbol{\mu}_d$. As is remarked in 2.10, any homomorphism $\prod_{\mathbb{Q}(\zeta_n)/\mathbb{Q}} \mathbb{G}_{m,\mathbb{Q}(\zeta_n)} \to \prod_{\mathbb{Q}(\zeta_d)/\mathbb{Q}} \mathbb{G}_{m,\mathbb{Q}(\zeta_d)}$ is expressed uniquely in the form of

$$\alpha \circ \mathrm{Nr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_d)}, \ \alpha \in \mathrm{End}_{\mathbb{Q}-\mathrm{gr}}\Bigg(\prod_{\mathbb{Q}(\zeta_d)/\mathbb{Q}} \mathbb{G}_{m,\mathbb{Q}(\zeta_d)}\Bigg).$$

Put $\chi_d \circ \sigma = \alpha \circ \mathrm{Nr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_d)}$. Then α induces a surjection $\boldsymbol{\mu}_d \to \boldsymbol{\mu}_d$. Moreover α induces a bijection of $\boldsymbol{\mu}_d$ to $\boldsymbol{\mu}_d$ since $\boldsymbol{\mu}_d$ is a finite group. Therefore $\mathrm{Nr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_d)}$ induces a surjection of $\boldsymbol{\mu}_n$ to $\boldsymbol{\mu}_d$.

(c)$\Rightarrow$(a) By the assumption, for each positive divisor d of n, there exists an integer l_d such that $\mathrm{Nr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_d)}(\zeta_n^{l_d}) = \zeta_d$. Furthermore, putting

$$\sigma = ((\mathrm{Nr}_{\mathbb{Z}(\zeta_n)/\mathbb{Z}(\zeta_d)})^{l_d})_{d|n} : \prod_{\mathbb{Z}[\zeta_n]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta_n]} \to \prod_{d|n} \prod_{\mathbb{Z}[\zeta_d]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}(\zeta_d)},$$

we obtain a commutative diagram of group schemes over $\mathbb{Z}[1/n]$

$$\begin{array}{ccc} \Gamma & \longrightarrow & \Bigg(\prod_{\mathbb{Z}[\zeta_n]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta_n]}\Bigg) \otimes_{\mathbb{Z}} \mathbb{Z}[1/n] \\ \big\downarrow \wr & & \big\downarrow \sigma \\ \Gamma & \longrightarrow & U(\Gamma)_{\mathbb{Z}[1/n]} = \Bigg(\prod_{d|n} \prod_{\mathbb{Z}[\zeta_d]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta_d]}\Bigg) \otimes_{\mathbb{Z}} \mathbb{Z}[1/n] \end{array}.$$

EXAMPLE 3.7. If n is even ≥ 4, the embedding problem is negatively solved over $\mathbb{Q}$ for the embedding $\Gamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$.

Indeed, $\mathrm{Nr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_2)} : \boldsymbol{\mu}_n \to \boldsymbol{\mu}_2 = \{\pm 1\}$ is not surjective since $\mathrm{Nr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta) = 1$.

EXAMPLE 3.8. For $n = 15$, the embedding problem is affirmatively solved over $\mathbb{Z}[1/n]$ for the embedding $\Gamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$.

Indeed, $\mathrm{Nr}_{\mathbb{Q}(\zeta_{15})/\mathbb{Q}(\zeta_3)} : \boldsymbol{\mu}_{15} \to \boldsymbol{\mu}_3$ and $\mathrm{Nr}_{\mathbb{Q}(\zeta_{15})/\mathbb{Q}(\zeta_5)} : \boldsymbol{\mu}_{15} \to \boldsymbol{\mu}_5$ are both surjective since $\mathrm{Nr}_{\mathbb{Q}(\zeta_{15})/\mathbb{Q}(\zeta_3)}(\zeta_{15}) = \zeta_3^{-1}$ and $\mathrm{Nr}_{\mathbb{Q}(\zeta_{15})/\mathbb{Q}(\zeta_5)}(\zeta_{15}) = \zeta_5^{-1}$.

EXAMPLE 3.9. For $n = 21$, the embedding problem is negatively solved over $\mathbb{Q}$ for the embedding $\Gamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$.

Indeed, $\mathrm{Nr}_{\mathbb{Q}(\zeta_{21})/\mathbb{Q}(\zeta_3)} : \boldsymbol{\mu}_{21} \to \boldsymbol{\mu}_3$ is not surjective since $\mathrm{Nr}_{\mathbb{Q}(\zeta_{21})/\mathbb{Q}(\zeta_3)}(\zeta_{21}) = 1$.

EXAMPLE 3.10. Let p be a prime number > 2, and put $n = p^r$. Then the embedding problem is affirmatively solved over $\mathbb{Z}[1/p]$ for the embedding $\Gamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$.

Indeed, let R be a $\mathbb{Z}[1/p]$-algebra. Then the group homomorphism

$$(R\otimes_{\mathbb{Z}[1/p]}\mathbb{Z}[\zeta_{p^r},1/p])^\times \to R[\Gamma]^\times : a \mapsto \frac{1}{p^r}\sum_{j=0}^{p^r-1}\left\{\sum_{l=0}^{r}\mathrm{Tr}_{R\otimes_{\mathbb{Z}}\mathbb{Z}[\zeta_{p^l}]/R}\left(\zeta_{p^l}^{-j}\mathrm{Nr}_{R\otimes_{\mathbb{Z}}\mathbb{Z}[\zeta_{p^r}]/R\otimes_{\mathbb{Z}}\mathbb{Z}[\zeta_{p^l}]}a\right)\right\}\gamma^j$$

is represented by a homomorphism of group schemes

$$\sigma : \left(\prod_{A/\mathbb{Z}} \mathbb{G}_{m,A}\right) \otimes_{\mathbb{Z}} \mathbb{Z}[1/p] \to U(\Gamma)_{\mathbb{Z}[1/p]}\,.$$

We obtain a commutative diagram of group schemes

$$\begin{array}{ccc}
\Gamma & \longrightarrow & \left(\prod_{\mathbb{Z}[\zeta_{p^r}]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta_{p^r}]}\right) \otimes_{\mathbb{Z}} \mathbb{Z}[1/p] \\
\downarrow \wr & & \downarrow \sigma \\
\Gamma & \longrightarrow & U(\Gamma)_{\mathbb{Z}[1/p]} = \left(\prod_{l=0}^{r} \prod_{\mathbb{Z}[\zeta_{p^l}]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta_{p^l}]}\right) \otimes_{\mathbb{Z}} \mathbb{Z}[1/p]
\end{array}$$

since $\mathrm{Nr}_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}(\zeta_{p^{r-1}})}\zeta_{p^r} = \zeta_{p^{r-1}}$.

4. Kummer theory for norm tori

In this section, n denotes a positive integer, Γ a cyclic group of order n and γ a generator of Γ. We put $\zeta = \zeta_n = e^{2\pi i/n}$.

NOTATION 4.1. Let R be a ring. The map $\mathrm{Nr} : \mathbb{Z}[\zeta] \to \mathbb{Z}$ induces a homomorphism of multiplicative groups $\mathrm{Nr} : (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])^\times \to R^\times$. The homomorphism $\mathrm{Nr} : (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])^\times \to R^\times$ is represented by a homomorphism of group schemes

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

Put now

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

Then the homomorphism of group schemes $\Gamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ is factorized as

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

since $\mathrm{Nr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}\zeta = 1$.

REMARK 4.2. Put $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. As is remarked in 2.6, $\big(\prod^{(1)}_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}\big) \otimes_{\mathbb{Z}} \mathbb{Z}[1/n]$ is an algebraic torus over $\mathbb{Z}[1/n]$ with character group $J_G = \mathbb{Z}[G]/\mathbb{Z}$.

PROPOSITION 4.3. *If n is odd ≥ 3, the sculpture problem is affirmatively solved over $\mathbb{Z}[1/n]$ for the embedding $\Gamma \to \prod^{(1)}_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$.*

PROOF. There exists $g \in G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ such that $g(\zeta) = \zeta^2$ since n is odd. Defining a homomorphism of $\mathbb{Z}[G]$-modules $\xi : J_G = \mathbb{Z}[G]/\mathbb{Z} \to \mathbb{Z}[G]$ by $[1] \mapsto g - 1$, we obtain a commutative diagram of $\mathbb{Z}[G]$-modules

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z}(1) & \xleftarrow[\eta]{} & \mathbb{Z}[G] \\ \uparrow \wr & & \uparrow \xi \\ \mathbb{Z}/n\mathbb{Z}(1) & \xleftarrow[\eta]{} & J_G \end{array},$$

and therefore a commutative diagram of group schemes over $\mathbb{Z}[1/n]$

$$\begin{array}{ccc} \Gamma & \longrightarrow & \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} \\ \downarrow \wr & & \downarrow \tilde{\xi} \\ \Gamma & \longrightarrow & \prod^{(1)}_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} \end{array}.$$

We have gotten the conclusion, combining the above diagram with the commutative diagram of group schemes over $\mathbb{Z}[1/n]$

$$\begin{array}{ccc} \Gamma & \longrightarrow & U(\Gamma) \\ \downarrow \wr & & \downarrow \chi_n \\ \Gamma & \longrightarrow & \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} \end{array}.$$

PROPOSITION 4.4. *If n is even ≥ 4, the sculpture problem is negative over $\mathbb{Q}$ for the embedding problem $\Gamma \to \prod^{(1)}_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$.*

PROOF. Assume that there exists a commutative diagram of group schemes over $\mathbb{Q}$

$$\begin{array}{ccc} \Gamma & \longrightarrow & U(\Gamma)_{\mathbb{Q}} \\ \downarrow \wr & & \downarrow \tilde{\xi} \\ \Gamma & \longrightarrow & \prod^{(1)}_{\mathbb{Q}(\zeta)/\mathbb{Q}} \mathbb{G}_{m,\mathbb{Q}(\zeta)} \end{array}.$$

Then we obtain a commutative diagram of $\mathbb{Z}[G]$-modules

$$\begin{tikzcd} \mathbb{Z}/n\mathbb{Z}(1) & \bigoplus_{d|n} \mathbb{Z}[G_d] \arrow[l, "\eta"'] \\ \mathbb{Z}/n\mathbb{Z}(1) \arrow[u, "\wr"] & J_G \arrow[l, "\eta_n"] \arrow[u, "\xi"'] \end{tikzcd} .$$

Now we define $\xi_d : J_G \to \mathbb{Z}[G_d]$ by

$$\xi = (\xi_d)_{d|n} : J_G \longrightarrow \bigoplus_{d|n} \mathbb{Z}[G_d] .$$

As is remarked in 2.7, for each positive divisor d of n, we have

$$\mathrm{Im}\, \xi_d \subset I_{G_d} = \mathrm{Ker}[\varepsilon : \mathbb{Z}[G_d] \to \mathbb{Z}] .$$

Moreover, $i(g) \in \mathbb{Z}/n\mathbb{Z}$ is odd for each $g \in G$ since n is even. This implies that $(n/2)\eta_d(\xi_d(1)) = 0$ for each positive divisor d of n since I_{G_d} is generated by $g-1$ $(g \in G_d)$. Hence the homomorphism of $\mathbb{Z}[G]$-modules $\eta \circ \xi : J_G \to \bigoplus_{d|n} \mathbb{Z}[G_d] \to \mathbb{Z}/n\mathbb{Z}(1)$ is not surjective. However, this contradicts the commutativity of the above diagram.

THEOREM 4.5. *Let n be an integer ≥ 3. Then the embedding problem is affirmatively solved over $\mathbb{Z}[1/n]$ for $\Gamma \to \prod^{(1)}_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ if and only if the embedding problem is affirmatively solved over $\mathbb{Z}[1/n]$ for $\Gamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$.*

PROOF. We can verify the if-part, weaving the embedding

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

into the commutative diagram

$$\begin{tikzcd} \Gamma \arrow[r] \arrow[d, "\wr"] & \prod_{\mathbb{Z}[1/n,\zeta]/\mathbb{Z}[1/n]} \mathbb{G}_{m,\mathbb{Z}[1/n,\zeta]} \arrow[d, "\tilde{\xi}"] \\ \Gamma \arrow[r] & U(\Gamma)_{\mathbb{Z}[1/n]} \end{tikzcd} .$$

We now prove the only if-part. By the assumption, there exists a homomorphism of group schemes $\sigma : \prod^{(1)}_{\mathbb{Q}(\zeta)/\mathbb{Q}} \mathbb{G}_{m,\mathbb{Q}(\zeta)} \to U(\Gamma)_{\mathbb{Q}}$ such that the diagram

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

is commutative. Let d be a positive divisor of n. Then the homomorphism of group schemes

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

induces a surjection $\Gamma \to \boldsymbol{\mu}_d$, and therefore, the homomorphism of group schemes

$$\chi_d \circ \sigma : \prod_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}^{(1)} \mathbb{G}_{m,\mathbb{Q}(\zeta_n)} \to \prod_{\mathbb{Q}(\zeta_d)/\mathbb{Q}} \mathbb{G}_{m,\mathbb{Q}(\zeta_d)}$$

induces also a surjection $\Gamma = \boldsymbol{\mu}_n \to \boldsymbol{\mu}_d$. As is mentioned in 2.12, the homomorphism of group schemes of $\chi_d \circ \sigma : \prod_{\mathbb{Q}(\zeta_n)/\mathbb{Q}} \mathbb{G}_{m,\mathbb{Q}(\zeta_n)} \to \prod_{\mathbb{Q}(\zeta_d)/\mathbb{Q}} \mathbb{G}_{m,\mathbb{Q}(\zeta_d)}$ is expressed in the form of

$$\alpha \circ \mathrm{Nr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_d)}, \ \alpha \in \mathrm{End}_{\mathbb{Q}-\mathrm{gr}}\Bigg(\prod_{\mathbb{Q}(\zeta_d)/\mathbb{Q}} \mathbb{G}_{m,\mathbb{Q}(\zeta_d)}\Bigg).$$

Then α induces a surjection $\boldsymbol{\mu}_d \to \boldsymbol{\mu}_d$. Therefore the map $\mathrm{Nr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_d)}$ induces a surjection $\boldsymbol{\mu}_n \to \boldsymbol{\mu}_d$. It follows from Theorem 3.6 that the embedding problem is affirmatively solved over $\mathbb{Z}[1/n]$ for $\Gamma \to \prod_{\mathbb{Z}[\zeta,1/n]/\mathbb{Z}[1/n]} \mathbb{G}_{m,\mathbb{Z}[\zeta,1/n]}$.

5. Isogeny problem

5.1. Let Γ be a cyclic group of order n. It is an interesting problem to ask if the constant group scheme Γ is isomorphic over $\mathbb{Z}[1/n]$ to the kernel of an endomorphism of $\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ or $\prod^{(1)}_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$, which shall be called *isogeny problem*. Here $\zeta = e^{2\pi i/n}$.

Put now $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Then the isogeny problem for $\Gamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ or $\Gamma \to \prod^{(1)}_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ is equivalent to the question whether the kernel of the surjective $\mathbb{Z}[G]$-homomorphism $\eta : \mathbb{Z}[G] \to \mathbb{Z}/n\mathbb{Z}(1)$ or $\eta : J_G \to \mathbb{Z}/n\mathbb{Z}(1)$ is a principal ideal, respectively. Evidently, if the isogeny problem is affirmatively solved for $\Gamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$, then the isogeny problem is affirmatively solved also for $\Gamma \to \prod^{(1)}_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$.

The isogeny problem for Weil restrictions is studied in [3], and the isogeny problem for norm tori in [2]. More precisely, let k be a subfield of $\mathbb{Q}(\zeta)$ or $\mathbb{F}_p(\zeta)$ with $(n, p) = 1$, where ζ is a primitive n-th root of unity. Put $K = k(\zeta_n)$ and $G = \mathrm{Gal}(K/k)$. In [3] Kida examined, when G is cyclic, the isogeny problem for the embedding $\Gamma \to \prod_{K/k} \mathbb{G}_{m,K}$. It would be remarkable that he has gotten affirmative answers in the cases of $k = \mathbb{Q}$ and $n = 3, 5, 7, 11$. In [2] Kida examined the isogeny problem for the embedding $\Gamma \to \prod^{(1)}_{K/k} \mathbb{G}_{m,K}$ when G is cyclic and the embedding $\Gamma \to \prod_{K/k} \mathbb{G}_{m,K}$ is factorized as $\Gamma \to \prod^{(1)}_{K/k} \mathbb{G}_{m,K} \to \prod_{K/k} \mathbb{G}_{m,K}$.

It would be remarkable also that, if G is cyclic of prime order l with $(l, n) = 1$ and $\mathrm{Nr}_{K/k}\zeta = 1$, the isogeny problems are equivalent for $\Gamma \to \prod_{K/k} \mathbb{G}_{m,K}$ and for $\Gamma \to \prod^{(1)}_{K/k} \mathbb{G}_{m,K}$ (cf. [3, Proposition 4.1]).

Now we consider another kind of isogeny problem.

5.2. Let p denote a prime number > 2, Γ a cyclic group of order p, γ a generator of Γ and $\zeta = e^{2\pi i/p}$.

Put $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, and let g be a generator of G. Define a character $\rho : G \to \mathbb{C}^\times$ by $\rho(g) = e^{2\pi i/(p-1)}$. Then we have $\mathrm{Im}[\rho : \mathbb{Z}[G] \to \mathbb{C}] = \mathbb{Z}[\zeta_{p-1}]$. Let $\mathbb{G}_m(\rho)$ denote the algebraic torus over $\mathbb{Z}[1/p]$ with character group $\mathbb{Z}[\zeta_{p-1}]$. Then, by the theorem of Mazur-Rubin-Silverberg (recalled as Theorem 2.15), we have

$$\mathbb{G}_m(\rho) = \Bigg(\bigcap_{\substack{\mathbb{Q}\subset K\subset\mathbb{Q}(\zeta)\\ K\neq\mathbb{Q}(\zeta)}} \mathrm{Ker}\Big[\mathrm{Nr}_{\mathbb{Z}(\zeta)/\mathcal{O}_K} : \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} \to \prod_{\mathcal{O}_K/\mathbb{Z}} \mathbb{G}_{m,\mathcal{O}_K}\Big]\Bigg) \otimes_{\mathbb{Z}} \mathbb{Z}[1/p] .$$

Here $\mathcal{O}_K$ stands for the ring of integers in K.

The embedding $\Gamma \to (\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}) \otimes_{\mathbb{Z}} \mathbb{Z}[1/p]$ is factorized as

$$\Gamma \longrightarrow \mathbb{G}_m(\rho) \longrightarrow \Bigg(\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}\Bigg) \otimes_{\mathbb{Z}} \mathbb{Z}[1/p]$$

since $\mathrm{Nr}_{\mathbb{Q}(\zeta)/K}(\zeta) = 1$ for any subextension $K \neq \mathbb{Q}(\zeta)$ of $\mathbb{Q}(\zeta)/\mathbb{Q}$. The isogeny problem for the embedding $\Gamma \to \mathbb{G}_m(\rho)$ is equivalent to the question whether a prime ideal of $\mathbb{Z}[\zeta_{p-1}]$ over p is principal.

Swan [12] established a criterion for rationality of the function field of the homogeneous space $U(\Gamma)_{\mathbb{Q}}/\Gamma$: if a prime ideal of $\mathbb{Z}[\zeta_{p-1}]$ over p is not principal, then $U(\Gamma)_{\mathbb{Q}}/\Gamma$ is not rational as an algebraic variety over $\mathbb{Q}$. In [12] Swan showed the cases $p = 47, 113, 233$ as counterexamples for the Noether problem on rationality of invariant fields, which are also counterexamples for the isogeny problem for $\Gamma \to \mathbb{G}_m(\rho)$.

Here are a few examples. We owe Kida [3, Example 4.3 and Example 4.4] the results concerning the isogeny problem for Weil restrictions, though modifying the isogenies slightly.

EXAMPLE 5.3. $p = 5, \zeta = e^{2\pi i/5}$.

Define $g \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ by $g(\zeta) = \zeta^2$. Then $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is generated by g. Moreover, define a $\mathbb{Z}[G]$-homomorphism $\eta : \mathbb{Z}[G] \to \mathbb{Z}/5\mathbb{Z}(1)$ by $g \mapsto 2 \mod 5$. Then η

is surjective. Furthermore, a sequence of $\mathbb{Z}[G]$-modules

$$0 \longrightarrow \mathbb{Z}[G] \stackrel{1+g-g^3}{\longrightarrow} \mathbb{Z}[G] \stackrel{\eta}{\longrightarrow} \mathbb{Z}/5\mathbb{Z}(1) \longrightarrow 0$$

is exact. We obtain also exact sequences of $\mathbb{Z}[G]$-modules

$$0 \longrightarrow J_G \stackrel{2+2g+g^2}{\longrightarrow} J_G \stackrel{\eta}{\longrightarrow} \mathbb{Z}/5\mathbb{Z}(1) \longrightarrow 0$$

and

$$0 \longrightarrow \mathcal{O}_K \stackrel{1+2g}{\longrightarrow} \mathcal{O}_K \stackrel{\eta}{\longrightarrow} \mathbb{Z}/5\mathbb{Z}(1) \longrightarrow 0\,,$$

noting that $J_G = \mathbb{Z}[G]/(g^4 + g^3 + g^2 + g + 1)$ and $\mathcal{O}_K = \mathbb{Z}[G]/(g^2 + 1)$.

EXAMPLE 5.4. $p = 7, \zeta = e^{2\pi i/7}$.

Define $g \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ by $g(\zeta) = \zeta^3$. Then $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is generated by g. Moreover, define a $\mathbb{Z}[G]$-homomorphism $\eta : \mathbb{Z}[G] \to \mathbb{Z}/7\mathbb{Z}(1)$ by $g \mapsto 3 \mod 7$. Then η is surjective. Furthermore, a sequence of $\mathbb{Z}[G]$-modules

$$0 \longrightarrow \mathbb{Z}[G] \stackrel{-g+g^3+g^4}{\longrightarrow} \mathbb{Z}[G] \stackrel{\eta}{\longrightarrow} \mathbb{Z}/7\mathbb{Z}(1) \longrightarrow 0$$

is exact. We obtain also exact sequences of $\mathbb{Z}[G]$-modules

$$0 \longrightarrow J_G \stackrel{-g+g^3+g^4}{\longrightarrow} J_G \stackrel{\eta}{\longrightarrow} \mathbb{Z}/7\mathbb{Z}(1) \longrightarrow 0$$

and

$$0 \longrightarrow \mathcal{O}_K \stackrel{1-2g}{\longrightarrow} \mathcal{O}_K \stackrel{\eta}{\longrightarrow} \mathbb{Z}/7\mathbb{Z}(1) \longrightarrow 0\,,$$

noting that $J_G = \mathbb{Z}[G]/(g^6 + g^5 + g^4 + g^3 + g^2 + g + 1)$ and $\mathcal{O}_K = \mathbb{Z}[G]/(g^2 - g + 1)$.

6. Kummer-Artin-Schreier theory

In this section, p denotes a prime number and $\Gamma = \{1, \gamma, \dots, \gamma^{p-1}\}$ a cyclic group of order p. First we recall the Kummer-Artin-Schreier sequence (cf. [14], [7]).

NOTATION 6.1. Let A be a ring and $\lambda \in A$. A commutative group A-scheme $\mathcal{G}^{(\lambda)}$ is defined by

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

with multiplication

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

Furthermore, a homomorphism of group A-schemes

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

is defined by

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

If λ is invertible in A, then $\alpha^{(\lambda)}$ is an isomorphism. On the other hand, if λ is not invertible in A, then $\mathcal{G}^{(\lambda)} \otimes_A A_0$ is nothing but the additive group scheme $\mathbb{G}_{a,A_0}$. Here A_0 denotes the residue ring $A/(\lambda)$.

Hereafter we put $\zeta = e^{2\pi i/p}$, $\lambda = \zeta - 1$ and $A = \mathbb{Z}[\zeta]$.

6.2. A homomorphism of group $\mathbb{Z}[\zeta]$-scheme

$$\Psi : \mathcal{G}^{(\lambda)} = \operatorname{Spec} A\left[T, \frac{1}{1+\lambda T}\right] \to \mathcal{G}^{(\lambda^p)} = \operatorname{Spec} A\left[T, \frac{1}{1+\lambda^p T}\right]$$

is defined by

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

It is readily seen that $\operatorname{Ker}[\Psi : \mathcal{G}^{(\lambda)} \to \mathcal{G}^{(\lambda^p)}]$ is isomorphic to the constant group scheme $\mathbb{Z}/p\mathbb{Z}$. Moreover, the diagram of group A-schemes with exact raws

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}/p\mathbb{Z} \arrow[r] \arrow[d] & \mathcal{G}^{(\lambda)} \arrow[r, "\Psi"] \arrow[d, "\alpha^{(\lambda)}"] & \mathcal{G}^{(\lambda^p)} \arrow[r] \arrow[d, "\alpha^{(\lambda^p)}"] & 0 \\
0 \arrow[r] & \boldsymbol{\mu}_{p,\mathbb{Z}[\zeta]} \arrow[r] & \mathbb{G}_{m,\mathbb{Z}[\zeta]} \arrow[r, "p"'] & \mathbb{G}_{m,\mathbb{Z}[\zeta]} \arrow[r] & 0
\end{tikzcd}$$

is commutative. Hence the sequence

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

is isomorphic to the Kummer sequence

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

On the other hand, we have $\mathbb{F}_p = \mathbb{Z}[\zeta]/(\lambda)$. Moreover, the sequence

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

is nothing but the Artin-Schreier sequence

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

since $\{(1+\lambda T)^p - 1\}/\lambda^p \equiv T^p - T \mod \lambda$.

To sum up, the exact sequence

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathcal{G}^{(\lambda)} \xrightarrow{\Psi} \mathcal{G}^{(\lambda^p)} \longrightarrow 0$$

unifies the Kummer and Artin-Schreier sequences (cf. [14], [7], [5]).

Now we examine the sculpture and embedding problems for the Weil restriction $\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)}$.

6.3. For simplicity, we put

$$\chi = \chi_p : U(\Gamma) \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$$

and

$$\varepsilon = \chi_1 : U(\Gamma) \to \mathbb{G}_{m,\mathbb{Z}}\,.$$

Let R be a ring. Then the homomorphism χ induces a homomorphism of multiplicative groups

$$R[\Gamma]^\times \to (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])^\times : \sum_{k=0}^{p-1} a_k \gamma^k \mapsto \sum_{k=0}^{p-1} a_k \otimes \zeta^k\,,$$

and the homomorphism ε induces a homomorphism of multiplicative groups

$$R[\Gamma]^\times \to R^\times : \sum_{k=0}^{p-1} a_k \gamma^k \mapsto \sum_{k=0}^{p-1} a_k\,.$$

All the elements of $\mathrm{Ker}[\varepsilon : R[\Gamma]^\times \to R^\times]$ are expressed uniquely in the form of

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

The homomorphism $\chi : \mathrm{Ker}[\varepsilon : U(\Gamma) \to \mathbb{G}_{m,\mathbb{Z}}] \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ is factorized as

$$\mathrm{Ker}[\varepsilon : U(\Gamma) \to \mathbb{G}_{m,\mathbb{Z}}] \xrightarrow{\tilde{\chi}} \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}]} \mathcal{G}^{(\lambda)} \xrightarrow{\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \alpha^{(\lambda)}} \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}\,.$$

Indeed, the homomorphism of group schemes $\chi : \mathrm{Ker}[\varepsilon : U(\Gamma) \to \mathbb{G}_{m,\mathbb{Z}}] \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ gives a homomorphism of multiplicative groups

$$R[\Gamma]^\times \to (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])^\times : 1 + \sum_{k=1}^{p-1} a_k(\gamma^k - 1) \mapsto 1 + \sum_{k=1}^{p-1} a_k \otimes (\zeta^k - 1)\,.$$

By the definition of $\mathcal{G}^{(\lambda)}$, we have

$$\sum_{k=1}^{p-1} a_k \otimes \frac{\zeta^k - 1}{\zeta - 1} \in \mathcal{G}^{(\lambda)}(R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])$$

and

$$\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \alpha^{(\lambda)} : \sum_{k=1}^{p-1} a_k \otimes \frac{\zeta^k - 1}{\zeta - 1} \mapsto 1 + (1 \otimes \lambda)\left(\sum_{k=1}^{p-1} a_k \otimes \frac{\zeta^k - 1}{\zeta - 1}\right) = 1 + \sum_{k=1}^{p-1} a_k \otimes (\zeta^k - 1)\,.$$

It is readily seen that the constant group scheme Γ is contained in $\mathrm{Ker}[\varepsilon : U(\Gamma) \to \mathbb{G}_{m,\mathbb{Z}}]$ and

$$\tilde{\chi}(\gamma^k) = 1 \otimes \frac{\zeta^k - 1}{\zeta - 1}$$

for each k. Furthermore $\tilde{\chi} : \mathrm{Ker}[\varepsilon : U(\Gamma) \to \mathbb{G}_{m,\mathbb{Z}}] \longrightarrow \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}]} \mathcal{G}^{(\lambda)}$ is an isomorphism of group schemes. Indeed, the inverse of $\tilde{\chi}$ is defined by

$$\sum_{k=1}^{p-1} a_k \otimes \frac{\zeta^k - 1}{\zeta - 1} \mapsto \left(1 - \sum_{k=1}^{p-1} a_k\right) + \sum_{k=1}^{p-1} a_k \gamma^k$$

Moreover, define a homomorphism of group schemes

$$s : U(\Gamma) \to \mathrm{Ker}[\varepsilon : U(\Gamma) \to \mathbb{G}_{m,\mathbb{Z}}]$$

by

$$\sum_{k=0}^{p-1} a_k \gamma^k \mapsto \sum_{k=0}^{p-1} a_k \gamma^k \Big/ \sum_{k=0}^{p-1} a_k\,.$$

Then s gives a splitting of the exact sequence

$$0 \longrightarrow \mathrm{Ker}[\varepsilon : U(\Gamma) \to \mathbb{G}_{m,\mathbb{Z}}] \xrightarrow{i} U(\Gamma) \xrightarrow{\varepsilon} \mathbb{G}_{m,\mathbb{Z}} \longrightarrow 0\,.$$

Therefore we obtain the following assertions:

PROPOSITION 6.4. *Both the sculpture and embedding problems are affirmatively solved over $\mathbb{Z}$ for the embedding $\Gamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)}$. Indeed, the diagrams*

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

and

$$\begin{array}{ccc} \Gamma & \longrightarrow & \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \\ \Vert & & \big\downarrow{\scriptstyle i\circ\tilde{\chi}^{-1}} \\ \Gamma & \longrightarrow & U(\Gamma) \end{array}$$

are commutative.

Now we describe the homomorphism $\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \alpha^{(\lambda)} : \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ more precisely.

6.5. Description of $U(\Gamma)$. Put

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

Then we have

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

Furthermore, we have

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

The multiplication is defined by

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

6.6. Description of $\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$. Let R be a ring. Then all the elements of $R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta]$ are expressed uniquely in the form of

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

since $\{\zeta, \zeta^2, \dots, \zeta^{p-1}\}$ is a basis of $\mathbb{Z}[\zeta]$ over $\mathbb{Z}$.

Put now

$$N_p(X_1, X_2, \dots, X_{p-1}) = \prod_{j=1}^{p-1} \left(\sum_{k=1}^{p-1} \zeta^{jk} X_k \right).$$

Then $N_p(X_1, X_2, \dots, X_{p-1}) \in \mathbb{Z}[X_1, X_2, \dots, X_{p-1}]$. Furthermore,

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

Hence we obtain

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

where the multiplication is given by

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

The homomorphism of group schemes

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

is defined by

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

Furthermore, the homomorphism of group schemes

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

is defined by

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

Hence we obtain

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

6.7. Description of $\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)}$. Let R be a ring. Then all the elements of $R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta]$ are expressed uniquely in the form of

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

since $\{1, 1+\zeta, \ldots, 1+\zeta+\cdots+\zeta^{p-2}\}$ is a basis of $\mathbb{Z}[\zeta]$ over $\mathbb{Z}$. Noting that

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

we can verify that:

$$\sum_{k=1}^{p-1} a_k \otimes \frac{\zeta^k - 1}{\zeta - 1} \in \mathcal{G}^{(\lambda)}(R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta]) \ \Leftrightarrow$$
$$N_p(-1+2a_1+a_2+\cdots+a_{p-1}, -1+a_1+2a_2+\cdots+a_{p-1}, \ldots, -1+a_1+a_2+\cdots+2a_{p-1}) \in R^\times .$$

Put now

$$F(X_1, X_2, \ldots, X_{p-1}) =$$
$$N_p(-1+2X_1+X_2+\cdots+X_{p-1}, -1+X_1+2X_2+\cdots+X_{p-1}, \ldots, -1+X_1+X_2+\cdots+2X_{p-1}) .$$

Then we have

$$F(X_1, X_2, \ldots, X_{p-1}) \equiv 1 \mod p .$$

Indeed, by the definition of $N_p(X_1, X_2, \ldots, X_{p-1})$ and $F(X_1, X_2, \ldots, X_{p-1})$, we obtain

$$F(X_1, X_2, \ldots, X_{p-1}) = \prod_{j=1}^{p-1} \left\{ 1 + \sum_{k=1}^{p-1} (\zeta^k - 1) X_k \right\} .$$

This implies that

$$F(X_1, X_2, \ldots, X_{p-1}) \equiv 1 \mod \lambda .$$

Therefore we obtain the result, noting that $F(X_1, X_2, \ldots, X_{p-1}) \in \mathbb{Z}[X_0, X_1, \ldots, X_{p-1}]$.

Define $\tilde{N}_p(X_1, X_2, \ldots, X_{p-1}) \in \mathbb{Z}[X_1, X_2, \ldots, X_{p-1}]$ by

$$F(X_1, X_2, \ldots, X_{p-1}) = 1 + p\tilde{N}_p(X_1, X_2, \ldots, X_{p-1}) .$$

Then we arrive at the assertion:

$$\sum_{k=1}^{p-1} a_k \otimes \frac{\zeta^k - 1}{\zeta - 1} \in \mathcal{G}^{(\lambda)}(R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta]) \ \Leftrightarrow \ 1 + p\tilde{N}_p(a_1, a_2, \ldots, a_{p-1}) \in R^\times .$$

Hence we obtain

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

where the multiplication is defined by

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

The homomorphism of group schemes

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

is defined by

$$X_i \mapsto X_i + (-1 + X_1 + X_2 + \cdots + X_{p-1})\ (1 \le i \le p-1)\,.$$

The homomorphism $\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \alpha^{(\lambda)}$ is isomorphic over $\mathbb{Z}[1/p]$. Indeed, the inverse is given by

$$X_i \mapsto X_i + \frac{1}{p}(1 - X_1 - \cdots - X_{p-1})\ (1 \le i \le p-1)\,.$$

Furthermore, the homomorphism

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

is defined by

$$X_j \mapsto T_j/(T_0 + T_1 + \cdots + T_{p-1})\ \ (j = 1, 2, \dots, p-1)\,,$$

and the homomorphism

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

$$\to U(\Gamma) = \operatorname{Spec} \mathbb{Z}\left[T_0, T_1, \ldots, T_{p-1}, \frac{1}{\Delta_p(T_0, T_1, \ldots, T_{p-1})}\right]$$

is defined by

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

EXAMPLE 6.8. Here are a few examples of N_p and $\tilde{N}_p$.

(1) In the case of $p = 3$, we have

$$N_p(X_1, X_2) = X_1^2 - X_1X_2 + X_2^2$$

and

$$\tilde{N}_p(X_1, X_2) = -X_1 - X_2 + X_1^2 + X_1X_2 + X_2^2 .$$

(2) In the case of $p = 5$, we have

$$\begin{aligned}
&N_p(X_1, X_2, X_3, X_4) \\
&=(X_1^4 + X_2^4 + X_3^4 + X_4^4) - (X_1^3X_2 + X_2^3X_4 + X_4^3X_3 + X_3^3X_1) \\
&\quad - (X_1X_2^3 + X_2X_4^3 + X_4X_3^3 + X_3X_1^3) - (X_2^3X_3 + X_4^3X_1 + X_3^3X_2 + X_2^1X_4) \\
&\quad + (X_1^2X_2^2 + X_2^2X_4^2 + X_4^2X_3^2 + X_3^2X_1^2) + (X_1^2X_4^2 + X_2^2X_3^2) \\
&\quad + 2(X_1^2X_2X_3 + X_2^2X_4X_1 + X_4^2X_3X_2 + X_3^2X_1X_4) \\
&\quad + 2(X_1X_2X_3^2 + X_2X_4X_1^2 + X_4X_3X_2^2 + X_3X_1X_4^2) \\
&\quad - 3(X_1X_2^2X_3 + X_2X_4^2X_1 + X_4X_3^2X_2 + 3X_3X_1^2X_4) - X_1X_2X_3X_4
\end{aligned}$$

and

$$\begin{aligned}
&\tilde{N}_p(X_1, X_2, X_3, X_4) \\
&= -(X_1 + X_2 + X_4 + X_3) + 2(X_1^2 + X_2^2 + X_4^2 + X_3^2) \\
&\quad + 4(X_1X_2 + X_2X_4 + X_4X_3 + X_3X_1) + 3(X_1X_4 + X_2X_3) \\
&\quad - 2(X_1^3 + X_2^3 + X_4^3 + X_3^3) - 6(X_1^2X_2 + X_2^2X_4 + X_4^2X_3 + X_3^2X_1) \\
&\quad - 5(X_1X_2^2 + X_2X_4^2 + X_4X_3^2 + X_3X_1^2) - 3(X_2^2X_3 + X_4^2X_1 + X_3^2X_2 + X_1^2X_4) \\
&\quad - 9(X_1X_2X_3 + X_2X_4X_1 + X_4X_3X_2 + X_3X_1X_4) \\
&\quad + (X_1^4 + X_2^4 + X_4^4 + X_3^4) + 4(X_1^2X_2^2 + X_2^2X_4^2 + X_4^2X_3^2 + X_3^2X_1^2) + (X_1^2X_4^2 + X_2^2X_3^2) \\
&\quad + 2(X_1X_2^3 + X_2X_4^3 + X_4X_3^3 + X_3X_1^3) + (X_2^3X_3 + X_4^3X_1 + X_3^3X_2 + X_1^3X_4) \\
&\quad + 3(X_1^3X_2 + X_2^3X_4 + X_4^3X_3 + X_3^3X_1)
\end{aligned}$$

$$+ 7(X_1^2X_2X_3 + X_2^2X_4X_1 + X_4^2X_3X_2 + X_3^2X_1X_4)$$
$$+ 4(X_1X_2^2X_3 + X_2X_4^2X_1 + X_4X_3^2X_2 + X_3X_1^2X_4)$$
$$+ 6(X_1X_2X_3^2 + X_2X_4X_1^2 + X_4X_3X_2^2 + X_3X_1X_4^2) + 11X_1X_2X_3X_4.$$

We conclude the article, by mentioning the sculpture and embedding problems for the analogues of norm tori in the Kummer-Artin-Schreier theory.

6.9. Put $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, and let g be a generator G. Let R be a ring. Then a homomorphism of multiplicative group $g_R : (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])^\times \to (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])^\times$ is defined by $r \otimes a \mapsto r \otimes g(a)$. The homomorphism $g_R : (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])^\times \to (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])^\times$ is represented by a homomorphism of group schemes $g : \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$.

Now we describe the endomorphism g of $\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ in terms of Hopf algebras. Take an integer $i(g)$ so that $g(\zeta) = \zeta^{i(g)}$. Then the homomorphism

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

is defined by

$$X_j \mapsto X_{i(g)^{-1}j} \quad (j = 1, 2, \dots, p-1)\,.$$

Here $i(g)^{-1}j$ stands for the integer $l \in \{1, 2, \dots, p-1\}$ such that $i(g)l \equiv j \mod p$.

Furthermore, for $\theta \in \mathbb{Z}[G]$, an endomorphism θ of $\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ is defined since the group law of $\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ is commutative. More explicitly, let

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

and let R be a ring. Then the homomorphism of multiplicative groups $\theta_R : (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])^\times \to (R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])^\times$ is given by

$$\theta_R(r \otimes \alpha) = \prod_{k=0}^{p-2} \big(r \otimes g^k(\alpha)\big)^{n_k}\,.$$

6.10. Now define a morphism of affine schemes

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

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

by

$$X_j \mapsto X_{i(g)^{-1}j} \ (j = 1, 2, \dots, p-1) .$$

Then it is verified without difficulty that $g : \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)}$ is a homomorphism of group schemes. Furthermore, the diagram

$$\begin{array}{ccc}
\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} & \xrightarrow{g} & \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \\
{\scriptstyle \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \alpha^{(\lambda)}}\Big\downarrow & & \Big\downarrow{\scriptstyle \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \alpha^{(\lambda)}} \\
\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} & \xrightarrow[g]{} & \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}
\end{array}$$

is commutative.

More generally, for $\theta \in \mathbb{Z}[G]$, an endomorphism θ of $\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)}$ is defined since the group law of $\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)}$ is commutative. Furthermore, the diagram

$$\begin{array}{ccc}
\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} & \xrightarrow{\theta} & \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \\
{\scriptstyle \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \alpha^{(\lambda)}}\Big\downarrow & & \Big\downarrow{\scriptstyle \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \alpha^{(\lambda)}} \\
\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} & \xrightarrow[\theta]{} & \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}
\end{array}$$

is commutative.

EXAMPLE 6.11. Assume that $p > 2$. Put

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

and

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

Then we obtain a commutative diagram with exact raws

$$\begin{tikzcd}
0 \arrow[r] & \prod\limits_{\mathbb{Z}[\zeta]/\mathbb{Z}}{}^{(1)}\mathcal{G}^{(\lambda)} \arrow[r] \arrow[d] & \prod\limits_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \arrow[r, "\nu"] \arrow[d, "\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \alpha^{(\lambda)}"] & \prod\limits_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \arrow[d, "\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \alpha^{(\lambda)}"] \\
0 \arrow[r] & \prod\limits_{\mathbb{Z}[\zeta]/\mathbb{Z}}{}^{(1)}\mathbb{G}_{m,\mathbb{Z}[\zeta]} \arrow[r] & \prod\limits_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]} \arrow[r, "\nu"'] & \prod\limits_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}
\end{tikzcd}$$

The induced homomorphism $\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \alpha^{(\lambda)} : \prod^{(1)}_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \to \prod^{(1)}_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}[\zeta]}$ is isomorphic over $\mathbb{Z}[1/p]$.

We have also

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

where the multiplication is defined by

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

It is worthwhile to remark that $\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}}{}^{(1)}\mathcal{G}^{(\lambda)}$ is smooth over $\mathbb{Z}$, while $\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}}{}^{(1)}\mathbb{G}_{m,\mathbb{Z}[\zeta]}$ is not smooth at the locus (p).

PROPOSITION 6.12. *Assume that $p > 2$. Then both the sculpture and embedding problems are affirmatively solved over $\mathbb{Z}$ for the embedding $\Gamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}}{}^{(1)}\mathcal{G}^{(\lambda)}$.*

PROOF. The embedding problem for $\Gamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}}{}^{(1)}\mathcal{G}^{(\lambda)}$ is affirmatively solved since the embedding problem for $\Gamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)}$ is affirmatively solved.

Now we prove that the sculpture problem for $\Gamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}}{}^{(1)}\mathcal{G}^{(\lambda)}$ is affirmatively solved. Put $\sigma = g - 1 \in \mathbb{Z}[G]$. Then the homomorphism $\sigma : \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)}$ is factorized as

$$\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \xrightarrow{\sigma} \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}}{}^{(1)}\mathcal{G}^{(\lambda)} \xrightarrow{\text{inclusion}} \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)}$$

since $\nu\sigma = (1 + g + \cdots + g^{p-2})(1 - g) = 0$ in $\mathbb{Z}[G]$. Moreover, σ induces an automorphism of Γ since $\sigma = g - 1 : \gamma \mapsto \gamma^{i(g)-1}$. Hence we obtain a commutative diagram

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

and therefore, a commutative diagram

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

combining with the commutative diagram

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

EXAMPLE 6.13. Assume that $p > 2$. For each positive divisor d of $p-1$ ($d \neq p-1$), put

$$\nu_d = 1 + g^d + g^{2d} + \cdots + g^{(p-1)-d} \in \mathbb{Z}[G].$$

Put

$$\boldsymbol{G}_p = \bigcap_{\substack{d|(p-1) \\ d\neq p-1}} \mathrm{Ker}\Big[\nu_d : \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)}\Big].$$

Then $\boldsymbol{G}_p \otimes_{\mathbb{Z}} \mathbb{Z}[1/p]$ is an algebraic torus over $\mathbb{Z}[1/p]$ with character group $\mathbb{Z}[\zeta_{p-1}]$ as is remarked in 5.2.

THEOREM 6.14. *Assume that $p > 2$. Then both the sculpture and embedding problems are affirmatively solved over $\mathbb{Z}$ for the embedding $\Gamma \to \boldsymbol{G}_p$.*

PROOF. The embedding problem for $\Gamma \to \boldsymbol{G}_p$ is affirmatively solved since the embedding problem for $\Gamma \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)}$ is affirmatively solved.

Now we prove that the sculpture problem for $\Gamma \to \boldsymbol{G}_p$ is affirmatively solved. Put

$$\tilde{\sigma} = \prod_{\substack{d|(p-1)\\ d\neq p-1}} \Phi_d(g) \in \mathbb{Z}[G]\,,$$

where $\Phi_d(T)$ denotes the d-th cyclotomic polynomial. Then the homomorphism $\tilde{\sigma}$: $\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \to \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)}$ is factorized as

$$\prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \xrightarrow{\tilde{\sigma}} \boldsymbol{G}_p \xrightarrow{\text{inclusion}} \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)}$$

since

$$\nu_d\,\tilde{\sigma} = \left\{\prod_{\substack{d'|(p-1)\\ d\nmid d'}} \Phi_{d'}(g)\right\}\left\{\prod_{\substack{d'|(p-1)\\ d'\neq p-1}} \Phi_{d'}(g)\right\} = 0 \text{ in } \mathbb{Z}[G]$$

for all positive divisor d of $p-1$ ($d \neq p-1$). Moreover, $\tilde{\sigma}$ induces an automorphism of Γ.

Indeed, put

$$F(T) = \prod_{\substack{d|(p-1)\\ d\neq p-1}} \Phi_d(T)\,.$$

Then we have in $\mathbb{F}_p[T]$

$$F(T) = \prod_{\substack{a\in\mathbb{F}_p^\times\\ \text{the order of } a\,\neq\, p-1}} (T-a)\,.$$

Moreover, $i(g)$ is a primitive root of $\mathbb{F}_p$. Then we have $F(i(g)) \neq 0$ in $\mathbb{F}_p$. Then $\tilde{\sigma}(\zeta) = \zeta^{F(i(g))} \neq 1$.

Hence we obtain a commutative diagram

$$\begin{array}{ccc} \Gamma & \longrightarrow & \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \\ \big\downarrow \wr & & \big\downarrow \tilde{\sigma} \\ \Gamma & \longrightarrow & \boldsymbol{G}_p \end{array}\,,$$

and therefore, a commutative diagram

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

combining with the commutative diagram

$$\begin{tikzcd} \Gamma \arrow[r] \arrow[d, equal] & U(\Gamma) \arrow[d, "\tilde{\chi}\circ s"] \\ \Gamma \arrow[r] & \prod_{\mathbb{Z}[\zeta]/\mathbb{Z}} \mathcal{G}^{(\lambda)} \end{tikzcd}.$$

References

[1] M. DEMAZURE and P. GABRIEL, *Groupes algébriques, Tome I*, Masson & Cie, Editeur, Paris; North-Holland Publishing, Amsterdam, 1970.

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

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

[4] B. MAZUR, K. RUBIN and A. SILVERBERG, Twisting commutative algebraic groups, J. Algebra **314** (2007), 419–438.

[5] T. SEKIGUCHI and N. SUWA, Théories de Kummer-Artin-Schreier, C. R. Acad. Sci. Paris Sér. I Math. **312** (1991), 418–420.

[6] 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.

[7] 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.

[8] J. P. SERRE, *Groupes algébriques et corps de classes*, Hermann, Paris, 1959.

[9] N. SUWA, Twisted Kummer and Kummer-Artin-Schreier theories, Tôhoku Math. J. **60** (2008), 183–218.

[10] N. SUWA, Around Kummer theories, RIMS Kôkyûroku Bessatsu **B12** (2009), 115–148.

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

[12] R. SWAN, Invariant rational functions and a problem of Steenrods, Invent. Math. **7** (1969), 148–158.

[13] W. C. WATERHOUSE, *Introduction to affine group schemes*, Springer, 1979.

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

Present Address:
DEPARTMENT OF MATHEMATICS,
CHUO UNIVERSITY,
1–13–27 KASUGA, BUNKYO-KU, TOKYO 112–8551, JAPAN.
e-mail: suwa@math.chuo-u.ac.jp