RIMS Kôkyûroku Bessatsu
B12 (2009), 115–148

Around Kummer theories

By

Noriyuki SUWA[*]

Abstract

We establish several theories of Kummer type in connection with the unit group scheme of a group algebra, following a method presented by Serre in ⟨Groupes algébriques et corps de classes⟩. The argument is developed not only over a field but also over a ring, as generally as possible.

Introduction

The Kummer theory is an important item in the classical Galois theory to describe explicitly cyclic extensions of a field. Nowadays it is standard to deduce the Kummer theory from Hilbert 90, applying the Galois cohomolgy theory to an exact sequence of algebraic groups

$$0 \longrightarrow \boldsymbol{\mu}_n \longrightarrow \mathbb{G}_m \xrightarrow{n} \mathbb{G}_m \longrightarrow 0.$$

However we have an elementary way to verify the Kummer theory by the Lagrange resolvants. Serre [15, Ch.IV, 8] formulated this method, combining the normal basis theorem and the unit group scheme of a group algebra.

In this article we established several theories of Kummer type after Serre while the previous artilce [16] employed the Galois cohomology theory or the étale cohomology theory.

In Section 1, we paraphrase the argument of Serre [15, Ch.IV, 8] in the framework of the group scheme theory. The section is concluded by the following

Corollary 1.7. *Let R be a ring, G an affine group scheme over R, Γ a constant finite subgroup scheme of G and S/R be an unramified Galois extension with group Γ. If there*

Received March 31, 2008. Revised June 23, 2008.
2000 Mathematics Subject Classification(s): Primary 13B05; Secondary 14L15, 12G05.
Partially supported by Grant-in-Aid for Scientific Research No.16540040

[*]Department of Mathematics, Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo 112-8551, JAPAN
e-mail: suwa@math.chuo-u.ac.jp

exists a commutative diagram

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

and S/R has a normal basis, then there exists a cartesian diagram

$$\begin{tikzcd}\operatorname{Spec} S \arrow[r] \arrow[d] & G \arrow[d] \\ \operatorname{Spec} R \arrow[r] & G/\Gamma.\end{tikzcd}$$

(For the notation, see Section 1.) This assertion is a key of the argument developed in the succeeding sections. We add there the following statement:

Let R be a ring, G an affine group scheme over R, Γ a constant finite subgroup scheme of G and S/R the unramified Galois extension defined by a cartesian diagram

$$\begin{tikzcd}\operatorname{Spec} S \arrow[r] \arrow[d] & G \arrow[d] \\ \operatorname{Spec} R \arrow[r] & G/\Gamma.\end{tikzcd}$$

If there there exists a commutative diagram

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

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

In Section 2, we treat
(1) the Kummer theory (Corollary 2.3);
(2) the Kummer-Artin-Schreier theory (Corollary 2.7);
(3) the Artin-Schreier theory (Corollary 2.10).
The argument for the Kummer theory is somewhat a repetition of Serre [15. Ch.VI, 9]. However we give a detailed account because a description of the most typical case will be a suitable guide map of the argument.

In Section 3, after recalling the definition of several group schemes, we establish
(4) the twisted Kummer theory of odd degree (Corollary 3.6);
(5) the twisted Kummer theory of even degree (Corollary 3.11).
It would be worthwhile to note that a cyclic extension S/R of even degree obtained by the twisted Kummer theory does not necessarily have a normal basis. The obstruction is given by an element of order 2 in $\operatorname{Pic}(R)$.

The article is concluded by
(6) the twisted Kummer-Artin-Schreier theory (Corollary 4.4)
in Section 4.

The author expresses his gratitude to Yukio Doi and Hiroshi Naruse for valuable discussions. This work began with a conversation at a historic temple in the spring.

Notation

For a ring R, $R^\times$ denotes the multiplicative group of invertible elements of R.

For a scheme X and a commutative group scheme G over X, $H^*(X, G)$ denotes the cohomology group with respect to the fppf-topology. It is known that, if G is smooth over X, the fppf-cohomology group coincides with the étale cohomology group (Grothendieck [4], III.11.7).

List of group schemes

$\mathbb{G}_{a,A}$ the additive group scheme over A

$\mathbb{G}_{m,A}$ the multiplicative group scheme over A

$\boldsymbol{\mu}_{n,A}$ $\mathrm{Ker}[n : \mathbb{G}_{m,A} \to \mathbb{G}_{m,A}]$

$\mathcal{G}^{(\lambda)}$ recalled in 1.2

$U(\mathit{\Gamma})$ defined in 1.3

$U_{B/A}$ defined in 3.1

$G_{B/A}$ defined in 4.1

List of homomorphisms

$\alpha^{(\lambda)} : \mathcal{G}^{(\lambda)} \to \mathbb{G}_{m,A}$ recalled in 1.2

$\chi_l : U(\mathit{\Gamma})_B \to \mathbb{G}_{m,B}$ defined in 2.1

$\sigma_1 : \mathbb{G}_{m,B} \to U_(\mathit{\Gamma})_B$ defined in 2.1

$\tilde{\chi} : U(\mathit{\Gamma})_B \to \mathcal{G}^{(\lambda)}$ defined in 2.5

$\tilde{\sigma} : \mathcal{G}^{(\lambda)} \to U_(\mathit{\Gamma})_B$ defined in 2.5

$\chi_l : U(\mathit{\Gamma})_A \to \prod_{B/A} \mathbb{G}_{m,B}$ defined in 3.2

$\varepsilon : U(\mathit{\Gamma})_A \to \mathbb{G}_{m,A}$ defined in 3.2

$\eta : U(\Gamma)_A \to \mathbb{G}_{m,A}$ defined in 3.2

$\nu : \prod_{B/A} \mathbb{G}_{m,B} \to \prod_{B/A} \mathbb{G}_{m,B}$ defined in 3.3

$\sigma_1 : \prod_{B/A} \mathbb{G}_{m,B} \to U(\Gamma)_A$ defined in 3.4

$\nu : \prod_{B/A} \mathbb{G}_{m,B} \to U_{B/A} \times_A \mathbb{G}_{m,A}$ defined in 3.10

$\tilde{\chi} : U(\Gamma)_A \to G_{B/A}$ defined in 4.2

$\tilde{\sigma} : G_{B/A} \to U(\Gamma)_A$ defined in 4.2

1. Group schemes

We refer to [1] or [17] on formalisms of affine group schemes, Hopf algebras and the cohomology with coefficients in group schemes.

1.1. As usual we denote by $\mathbb{G}_m = \operatorname{Spec} \mathbb{Z}[U, 1/U]$ and by $\mathbb{G}_a = \operatorname{Spec} \mathbb{Z}[T]$ the multiplicative group scheme and 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 A be a ring and $\lambda \in A$. We define a group A-scheme $\mathcal{G}^{(\lambda)}$ by

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

with
(a) the multiplication: $X \mapsto X \otimes 1 + 1 \otimes X + \lambda X \otimes X$;
(b) the unit: $X \mapsto 0$;
(c) the inverse: $X \mapsto -\dfrac{X}{1+\lambda X}$.

Moreover, we define a homomorphism of group A-schemes

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

by

$$U \mapsto 1 + \lambda X.$$

If λ is invertible, then $\alpha^{(\lambda)}$ is an isomorphism. On the other hand, if $\lambda = 0$, then $\mathcal{G}^{(\lambda)}$ is nothing but the additive group scheme $\mathbb{G}_{a,A}$.

Hereafter we recall the argument of Serre [15, Ch.VI, 8] in terms of the group scheme theory.

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

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

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

Put now

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

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

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

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

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

$$T_\gamma \mapsto e_\gamma : \mathbb{Z}[T_\gamma, \frac{1}{\varDelta_\varGamma}] \to \mathbb{Z}^\varGamma.$$

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

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

Terminology 1.4. Let R be a ring, $\varGamma$ a finite group and S an R-algebra. We shall say that:
(1) S/R is an *unramified Galois extension with group* $\varGamma$ if $\operatorname{Spec} S$ has a structure of right $\varGamma$-torsor over $\operatorname{Spec} R$;
(2) an unramified Galois extension S/R with group $\varGamma$ has a *normal basis* if there exists $s \in S$ such that $(\gamma s)_{\gamma\in\varGamma}$ is a basis of R-module S.

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

Example 1.5. 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 group Γ, and $(T_{\gamma^{-1}})_{\gamma\in\Gamma}$ is a nomal basis of the Galois extension S/R.

Proposition 1.6. *Let R be a ring, Γ a finite group and S/R an unramified Galois extension with group Γ. Then the Galois extension S/R has a normal basis if and only if there exist morphisms* $\operatorname{Spec} S \to U(\Gamma)$ *and* $\operatorname{Spec} R \to U(\Gamma)/\Gamma$ *such that the diagram*

$$\begin{tikzcd}
\operatorname{Spec} S \arrow[r] \arrow[d] & U(\Gamma) \arrow[d] \\
\operatorname{Spec} R \arrow[r] & U(\Gamma)/\Gamma
\end{tikzcd}$$

is cartesian.

Proof. Assume that the Galois extension S/R has a normal basis $(\gamma s)_{\gamma\in\Gamma}$. Put $s_\gamma = \gamma s$ for each $\gamma \in \Gamma$. Then the determinant of the matrix $(s_{\gamma\gamma'})_{\gamma,\gamma'\in\Gamma}$ is invertible in S since $\operatorname{Spec} S$ is étale over $\operatorname{Spec} R$. Hence a ring homomorphism $\varphi : \mathbb{Z}[T_\gamma, 1/\Delta_\Gamma] \to S$ is defined by $T_\gamma \mapsto s_{\gamma^{-1}}$. Moreover we obtain a cocartesian diagram

$$\begin{tikzcd}
S & \mathbb{Z}[T_\gamma, 1/\Delta_\Gamma] \arrow[l, "\varphi"'] \\
R \arrow[u] & \mathbb{Z}[T_\gamma, 1/\Delta_\Gamma]^\Gamma, \arrow[l, "\varphi"] \arrow[u]
\end{tikzcd}$$

noting that $R = S^\Gamma$.

Corollary 1.7. *Let R be a ring, G a affine group scheme and Γ a constant finite subgroup scheme of G.*

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

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

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

$$\begin{tikzcd}
\operatorname{Spec} S \arrow[r] \arrow[d] & G \arrow[d] \\
\operatorname{Spec} R \arrow[r] & G/\Gamma
\end{tikzcd}$$

is cartesian.

(2) *Let S/R be the unramified Galois extension with group $\varGamma$ defined by a cartesian diagram*

$$\begin{tikzcd}
\operatorname{Spec} S \arrow[r] \arrow[d] & G \arrow[d] \\
\operatorname{Spec} R \arrow[r] & G/\varGamma.
\end{tikzcd}$$

Assume that there exists a commutative diagram

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

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

Proof. We obtain the first assertion, combining two cartesian diagrams:

$$\begin{tikzcd}
\operatorname{Spec} S \arrow[r] \arrow[d] & U(\varGamma) \arrow[r] \arrow[d] & G \arrow[d] \\
\operatorname{Spec} R \arrow[r] & U(\varGamma)/\varGamma \arrow[r] & G/\varGamma.
\end{tikzcd}$$

Here the left square is given by Proposition 1.6, and the right square is deduced from the assumption of (1).

On the other hand, we obtain the second assertion, combining two cartesian diagrams:

$$\begin{tikzcd}
\operatorname{Spec} S \arrow[r] \arrow[d] & G \arrow[r] \arrow[d] & U(\varGamma) \arrow[d] \\
\operatorname{Spec} R \arrow[r] & G/\varGamma \arrow[r] & U(\varGamma)/\varGamma.
\end{tikzcd}$$

Here the left square is deduced from the assumption of (2), and the right square is given by Proposition 1.6.

Variant 1.8. Let R be a ring and $\varGamma$ a finite group. Then the exact sequence

$$1 \longrightarrow \varGamma \longrightarrow U(\varGamma) \longrightarrow U(\varGamma)/\varGamma \longrightarrow 1$$

yields an exact sequence of pointed sets

$$U(\varGamma)(R) \longrightarrow (U(\varGamma)/\varGamma)(R) \longrightarrow H^1(R,\varGamma) \longrightarrow H^1(R,U(\varGamma))$$

(cf. [1], Ch.III, 4.4). Proposition 1.6 asserts that an unramified Galois extension S/R with group $\varGamma$ has a normal basis if and only if the class $[S]$ in $H^1(R,\varGamma)$ is contained in $\operatorname{Ker}[H^1(R,\varGamma) \to H^1(R,U(\varGamma))]$.

Under the assumtion of 1.7(1), we obtain a commutative (up to sign) diagram with exact rows

$$\begin{tikzcd}
U(\Gamma)(R) \arrow[r] \arrow[d] & (U(\Gamma)/\Gamma)(R) \arrow[r] \arrow[d] & H^1(R,\Gamma) \arrow[r] \arrow[d, "\wr"] & H^1(R,U(\Gamma)) \arrow[d] \\
G(R) \arrow[r] & (G/\Gamma)(R) \arrow[r] & H^1(R,\Gamma) \arrow[r] & H^1(R,G).
\end{tikzcd}$$

Hence we obtain an implication

$$[S] \in \mathrm{Ker}[H^1(R,\Gamma) \to H^1(R,U(\Gamma))] \ \Rightarrow \ [S] \in \mathrm{Ker}[H^1(R,\Gamma) \to H^1(R,G)].$$

On the other hand, under the assumtion of 1.7(2), we obtain a commutative (up to sign) diagram with exact rows

$$\begin{tikzcd}
G(R) \arrow[r] \arrow[d] & (G/\Gamma)(R) \arrow[r] \arrow[d] & H^1(R,\Gamma) \arrow[r] \arrow[d, "\wr"] & H^1(R,G) \arrow[d] \\
U(\Gamma)(R) \arrow[r] & (U(\Gamma)/\Gamma)(R) \arrow[r] & H^1(R,\Gamma) \arrow[r] & H^1(R,U(\Gamma)).
\end{tikzcd}$$

Hence we obtain an implication

$$[S] \in \mathrm{Ker}[H^1(R,\Gamma) \to H^1(R,G)] \ \Rightarrow \ [S] \in \mathrm{Ker}[H^1(R,\Gamma) \to H^1(R,U(\Gamma))].$$

Remark 1.9. Let Γ be a finite group, R a ring and S/R an unramified Galois extension with group Γ. The normal basis theorem asserts that, if R is a field, the Galois extension S/R has a normal basis. We can verify the normal basis theorem for any local ring R by Nakayama's lemma.

2. Kummer, Kummer-Artin-Schreier and Artin-Schreier theories

Throughout the section, n denotes an integer ≥ 2 and Γ stands for a cyclic group of order n. We put $\zeta = e^{2\pi i/n}$ and $B = \mathbb{Z}[\zeta]$.

First we paraphrase over $\mathbb{Z}$ the argument of Serre [15, Ch.VI, 9], adding a remark on existence of a normal basis.

2.1. Fix a generator γ of Γ. Then we have

$$U(\Gamma) = \mathrm{Spec}\,\mathbb{Z}[T_0, T_1, \ldots, T_{n-1}, \frac{1}{\Delta}],$$

where

$$\Delta = \begin{vmatrix} T_0 & T_1 & T_2 & \ldots & T_{n-1} \\ T_1 & T_2 & T_3 & \ldots & T_0 \\ T_2 & T_3 & T_4 & \ldots & T_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ T_{n-1} & T_0 & T_1 & \ldots & T_{n-1} \end{vmatrix}.$$

The multiplication of $U(\varGamma)$ is defined by

$$T_k \mapsto \sum_{i+j\equiv k \bmod n} T_i \otimes T_j \ (0 \leq k < n).$$

As is well known, we have

$$\varDelta = (-1)^{(n-1)(n-2)/2} \prod_{l=0}^{n-1} \Big(\sum_{k=0}^{n-1} \zeta^{kl} T_k \Big).$$

Let $\chi_l : \varGamma \to \mathbb{C}^\times$ denote the character of $\varGamma$ defined by $\chi_l(\gamma) = \zeta^l$. For a B-algebra R, the character χ_l induces a homomorphism $\chi_l : R[\varGamma]^\times \to R^\times$, which is represented by the homomorphism of group B-schemes $\chi_l : U(\varGamma)_B \to \mathbb{G}_{m,B}$. More precisely,

$$\chi_l : U(\varGamma)_B = \operatorname{Spec} B[T_0, T_1, \ldots, T_{n-1}, \frac{1}{\varDelta}] \to \mathbb{G}_{m,B} = \operatorname{Spec} B[U, \frac{1}{U}]$$

is defined by

$$U \mapsto \sum_{k=0}^{n-1} \zeta^{kl} T_k : B[U, \frac{1}{U}] \to B[T_0, T_1, \ldots, T_{n-1}, \frac{1}{\varDelta}].$$

The homomorphism of group B-schemes

$$\chi = (\chi_0, \chi_1, \chi_2, \ldots, \chi_{n-1}) : U(\varGamma)_B \to \mathbb{G}_{m,B}^n$$

is an isomorphism over $B[1/n]$. In fact, χ is defined by

$$U_l \mapsto \sum_{k=0}^{n-1} \zeta^{kl} T_k : B[U_0, U_1, \ldots, U_{n-1}, \frac{1}{U_0}, \frac{1}{U_1}, \ldots, \frac{1}{U_{n-1}}] \to B[T_0, T_1, \ldots, T_{n-1}, \frac{1}{\varDelta}] \ (0 \leq l < n),$$

and the inverse s of χ is given by

$$T_l \mapsto \frac{1}{n} \sum_{k=0}^{n-1} \zeta^{-kl} U_k \ (0 \leq l < n)$$

over $B[1/n]$.

We define a homomorphism of group B-schemes $\sigma : \mathbb{G}_{m,B} \to \mathbb{G}_{m,B}^n$ by

$$U_l \to U^l : \mathbb{Z}[U_0, U_1, \ldots, U_{n-1}, \frac{1}{U_0}, \frac{1}{U_1}, \ldots, \frac{1}{U_{n-1}}] \to \mathbb{Z}[U, \frac{1}{U}] \ (0 \leq l < n).$$

Put $\sigma_1 = s \circ \sigma : \mathbb{G}_{m,B[1/n]} \to U(\varGamma)_{B[1/n]}$. Then the homomorphism σ_1 is defined by

$$T_l \mapsto \frac{1}{n} \sum_{k=0}^{n-1} \zeta^{-kl} U^k,$$

and σ_1 is a section of $\chi_1 : U(\varGamma)_{B[1/n]} \to \mathbb{G}_{m,B[1/n]}$. Moreover we have a commutative diagram of group B-schemes with exact rows

(1)
$$\begin{tikzcd}
0 \arrow[r] & \varGamma \arrow[r] \arrow[d] & U(\varGamma)_B \arrow[r] \arrow[d, "\chi_1"] & (U(\varGamma)/\varGamma)_B \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \boldsymbol{\mu}_{n,B} \arrow[r] & \mathbb{G}_{m,B} \arrow[r, "n"] & \mathbb{G}_{m,B} \arrow[r] & 0
\end{tikzcd}$$

and a commutative diagram of group $B[1/n]$-schemes with exact rows

(2)
$$\begin{tikzcd}
0 \arrow[r] & \boldsymbol{\mu}_{n,B[1/n]} \arrow[r] \arrow[d] & \mathbb{G}_{m,B[1/n]} \arrow[r, "n"] \arrow[d, "\sigma_1"] & \mathbb{G}_{m,B[1/n]} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \varGamma \arrow[r] & U(\varGamma)_{B[1/n]} \arrow[r] & (U(\varGamma)/\varGamma)_{B[1/n]} \arrow[r] & 0.
\end{tikzcd}$$

Proposition 2.2. *The homomorphism $\chi_1 : \varGamma \to \boldsymbol{\mu}_{n,B}$ is an isomorphism over $B[1/n]$, and the inverse is given by $\sigma_1 : \boldsymbol{\mu}_{n,B[1/n]} \to \varGamma$.*

Proof. For each l, put

$$E_l(U) = \frac{1}{n}\sum_{k=0}^{n-1} \zeta^{-kl} U^k.$$

Then we have

$$E_l(\zeta^j) = \begin{cases} 1 & (j \equiv l \mod n) \\ 0 & (j \not\equiv l \mod n). \end{cases}$$

Hence the result.

Applying Corollary 1.7 to (1) and (2), we obtain:

Corollary 2.3.(Kummer theory) *Let R be a $B[1/n]$-algebra and S an unramified cyclic extension of degree n. Then the following conditions are equivalent.*

(a) *the cyclic extension S/R has a normal basis*;

(b) *there exists $a \in R^\times$ such that S is isomorphic to $R[U]/(U^n - a)$ and that γ acts on S by $\gamma\alpha = \zeta\alpha$. Here α is the image of U in $S = R[U]/(U^n - a)$.*

If it is the case, $\displaystyle\frac{1}{n}\sum_{k=0}^{n-1} \alpha^k$ generates a normal basis of the cyclic extension S/R.

Example 2.4. Let R be a ring. The equivalent conditions (a) and (b) in 2.3 hold true under the assumption: $\mathrm{Pic}(R) = H^1(R, \mathbb{G}_{m,R}) = 0$.

Hereafter we recall the argument of [11], adding a remark on existence of a normal basis. We assume now that $n = p$ is a prime number.

2.4. Put $\lambda = \zeta - 1$ and $\varepsilon_k = (\zeta^k - 1)/(\zeta - 1)$ for each k. In particular, we have $\varepsilon_0 = 0$ and $\varepsilon_1 = 1$. As is well known, ε_k is a unit of $B = \mathbb{Z}[\zeta]$ if k is prime to p. Moreover we have

$$\lambda^{p-1}\varepsilon_1\varepsilon_2\cdots\varepsilon_{p-1} = (-1)^{p-1}p.$$

Hence (λ) is a prime ideal of B, and $B/(\lambda)$ is isomorphic to $\mathbb{F}_p$.

Put now

$$\Psi(X) = \frac{(1+\lambda X)^p - 1}{\lambda^p}.$$

Then we have

$$\Psi(X) = \prod_{k=0}^{p-1}(X - \varepsilon_k),$$

which implies that $\Psi(X) \in B[X]$ and $\Psi(X) \equiv X^p - X \mod \lambda$.

Define a homomorphism of group B-schemes

$$\Psi : \mathcal{G}^{(\lambda)} = \operatorname{Spec} B[X, \frac{1}{1+\lambda X}] \to \mathcal{G}^{(\lambda^p)} = \operatorname{Spec} B[X, \frac{1}{1+\lambda^p X}]$$

by

$$X \mapsto \Psi(X) = \frac{(1+\lambda X)^p - 1}{\lambda^p} : B[X, \frac{1}{1+\lambda^p X}] \to B[X, \frac{1}{1+\lambda X}].$$

Then we obtain a commutative diagram of group B-schemes with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Ker}\Psi \arrow[r] \arrow[d] & \mathcal{G}^{(\lambda)} \arrow[r, "\Psi"] \arrow[d, "\alpha^{(\lambda)}"] & \mathcal{G}^{(\lambda^p)} \arrow[r] \arrow[d, "\alpha^{(\lambda^p)}"] & 0 \\
0 \arrow[r] & \boldsymbol{\mu}_{n,B} \arrow[r] & \mathbb{G}_{m,B} \arrow[r, "p"] & \mathbb{G}_{m,B} \arrow[r] & 0.
\end{tikzcd}$$

2.5. A homomorphism of group B-schemes

$$\tilde{\chi} : U(\mathit{\Gamma})_B = \operatorname{Spec} B[T_0, T_1, \ldots, T_{p-1}, \frac{1}{\mathit{\Delta}}] \to \mathcal{G}^{(\lambda)} = \operatorname{Spec} B[X, \frac{1}{1+\lambda X}]$$

is defined by

$$X \mapsto \sum_{k=1}^{p-1}\varepsilon_k T_k \Big/ \sum_{k=0}^{p-1} T_k : B[X, \frac{1}{1+\lambda X}] \to B[T_0, T_1, \ldots, T_{p-1}, \frac{1}{\mathit{\Delta}}].$$

We can verify that the diagram of group B-schemes

$$\begin{tikzcd}
& U(\mathit{\Gamma})_B \arrow[dl, "\tilde{\chi}"'] \arrow[dr, "\chi_1/\chi_0"] & \\
\mathcal{G}^{(\lambda)} \arrow[rr, "\alpha^{(\lambda)}"] & & \mathbb{G}_{m,B},
\end{tikzcd}$$

is commutative, noting that

$$1+\lambda\Big(\sum_{k=1}^{p-1}\varepsilon_k T_k\Big/\sum_{k=0}^{p-1}T_k\Big)=\sum_{k=0}^{p-1}\zeta^k T_k\Big/\sum_{k=0}^{p-1}T_k.$$

Put

$$\Psi_l(X)=\frac{1}{p}\sum_{k=0}^{p-1}\zeta^{-kl}(1+\lambda X)^k$$

for each l. In particular, we have

$$\Psi_0(X)=\sum_{k=1}^{p-1}\frac{1}{p}\binom{p}{k}\lambda^{k-1}X^{k-1}+\frac{\lambda^{p-1}}{p}X^{p-1}.$$

Moreover we have

$$\Psi_0(\zeta^l X+\varepsilon_l)=\Psi_{p-l}(X),$$

which implies that $\Psi_l(X)\in B[X]$ for each l. It is readily seen that

$$\sum_{k=0}^{p-1}\zeta^{kl}\Psi_k(X)=(1+\lambda X)^l$$

for $0\le l<p$.

Define now a homomorphism of group B-schemes

$$\tilde{\sigma}:\mathcal{G}^{(\lambda)}=\operatorname{Spec}B[X,\frac{1}{1+\lambda X}]\to U(\mathit{\Gamma})=\operatorname{Spec}B[T_0,T_1,\dots,T_{p-1},\frac{1}{\mathit{\Delta}}]$$

by

$$T_l\mapsto\Psi_l(X)=\frac{1}{p}\sum_{k=0}^{p-1}\zeta^{-kl}(1+\lambda X)^k:B[T_0,T_1,\dots,T_{p-1},\frac{1}{\mathit{\Delta}}]\to B[X,\frac{1}{1+\lambda X}]\ (0\le l<p).$$

Then we obtain a commutative diagram of group $B[1/p]$-schemes

$$\begin{tikzcd} & U(\mathit{\Gamma})_{B[1/p]} & \\ \mathcal{G}^{(\lambda)}_{B[1/p]} \arrow[ur, "\tilde{\sigma}"] \arrow[rr, "\alpha^{(\lambda)}"] & & \mathbb{G}_{m,B[1/p]}. \arrow[ul, "\sigma_1"'] \end{tikzcd}$$

since $\sigma_1:U(\mathit{\Gamma})_{B[1/p]}\to\mathbb{G}_{m,B[1/p]}$ and $\alpha^{(\lambda)}:\mathcal{G}^{(\lambda)}_{B[1/p]}\to\mathbb{G}_{m,B[1/p]}$ are defined by

$$T_l\mapsto\frac{1}{p}\sum_{k=0}^{p-1}\zeta^{-kl}U^k:B[T_0,T_1,\dots,T_{p-1},\frac{1}{\mathit{\Delta}}]\to A[U,\frac{1}{U}]\ (0\le l<p)$$

and

$$U\mapsto 1+\lambda X:B[U,\frac{1}{U}]\to B[X,\frac{1}{1+\lambda X}],$$

respectively.

The homomorphism $\tilde{\sigma}$ is a section of $\tilde{\chi} : U(\mathit{\Gamma})_B \to \mathcal{G}^{(\lambda)}$ since we have

$$\sum_{k=1}^{p-1} \varepsilon_k \Psi_k(X) = X, \quad \sum_{k=0}^{p-1} \Psi_k(X) = 1.$$

Moreover we have commutative diagrams of group B-schemes with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \mathit{\Gamma} \arrow[r] \arrow[d] & U(\mathit{\Gamma})_B \arrow[r] \arrow[d, "\tilde{\chi}"] & (U(\mathit{\Gamma})/\mathit{\Gamma})_B \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \operatorname{Ker}\Psi \arrow[r] & \mathcal{G}^{(\lambda)} \arrow[r, "\Psi"] & \mathcal{G}^{(\lambda^p)} \arrow[r] & 0
\end{tikzcd} \tag{3}$$

and

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Ker}\Psi \arrow[r] \arrow[d] & \mathcal{G}^{(\lambda)} \arrow[r, "\Psi"] \arrow[d, "\tilde{\sigma}"] & \mathcal{G}^{(\lambda^p)} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathit{\Gamma} \arrow[r] & U(\mathit{\Gamma})_B \arrow[r] & (U(\mathit{\Gamma})/\mathit{\Gamma})_B \arrow[r] & 0.
\end{tikzcd} \tag{4}$$

Proposition 2.6. *The homomorphism $\tilde{\chi} : \mathit{\Gamma} \to \operatorname{Ker}\Psi$ is an isomorphism, and the inverse is given by $\tilde{\sigma} : \operatorname{Ker}\Psi \to \mathit{\Gamma}$.*

Proof. For each l, we have

$$\Psi_l(\varepsilon_j) = \begin{cases} 1 & (j \equiv l \mod p) \\ 0 & (j \not\equiv l \mod p). \end{cases}$$

Hence the result.

Applying Corollary 1.7 to (3) and (4), we obtain:

Corollary 2.7.(Kummer-Artin-Schreier theory) *Let R be a B-algebra and S an unramified cyclic extension of degree p. Then the following conditions are equivalent.*

(a) *the cyclic extension S/R has a normal basis*;

(b) *there exists $a \in R$ with $1+\lambda^p a \in R^\times$ such that S is isomorphic to $R[X]/(\Psi(X)-a)$ and that γ acts on S by $\gamma\alpha = \zeta\alpha+1$. Here α is the image of X in $S = R[X]/(\Psi(X)-a)$.*

If it is the case, $\Psi_0(\alpha) = \sum_{k=1}^{p-1} \frac{1}{p}\binom{p}{k}\lambda^{k-1}\alpha^{k-1} + \frac{\lambda^{p-1}}{p}\alpha^{p-1}$ generates a normal basis of the cyclic extension S/R.

Remark 2.8. The implication (b)⇒(a) is due to Childs [2]. We also refer to Ichimura [6] and Kawamoto [7] concerning related topics.

2.9. Reducing the diagrams (3) and (4) modulo λ, we obtain commutative diagrams of group $\mathbb{F}_p$-schemes with exact rows

(5)
$$\begin{tikzcd}
0 \arrow[r] & \Gamma \arrow[r] \arrow[d, "\wr"] & U(\Gamma)_{\mathbb{F}_p} \arrow[r] \arrow[d, "\tilde{\chi}"] & (U(\Gamma)/\Gamma)_{\mathbb{F}_p} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathbb{Z}/p\mathbb{Z} \arrow[r] & \mathbb{G}_{a,\mathbb{F}_p} \arrow[r, "F-1"] & \mathbb{G}_{a,\mathbb{F}_p} \arrow[r] & 0
\end{tikzcd}$$

and

(6)
$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}/p\mathbb{Z} \arrow[r] \arrow[d, "\wr"] & \mathbb{G}_{a,\mathbb{F}_p} \arrow[r, "F-1"] \arrow[d, "\tilde{\sigma}"] & \mathbb{G}_{a,\mathbb{F}_p} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \Gamma \arrow[r] & U(\Gamma)_{\mathbb{F}_p} \arrow[r] & (U(\Gamma)/\Gamma)_{\mathbb{F}_p} \arrow[r] & 0
\end{tikzcd}$$

since $\Psi(X) \equiv X^p - X \mod \lambda$. The homomorphism of group $\mathbb{F}_p$-schemes

$$\tilde{\chi} : U(\Gamma)_{\mathbb{F}_p} = \operatorname{Spec} \mathbb{F}_p[T_0, T_1, \ldots, T_{p-1}, \frac{1}{\Delta}] \to \mathbb{G}_{a,\mathbb{F}_p} = \operatorname{Spec} \mathbb{F}_p[X]$$

is defined by

$$X \mapsto \sum_{k=1}^{p-1} kT_k \Big/ \sum_{k=0}^{p-1} T_k : \mathbb{F}_p[X] \to \mathbb{F}_p[T_0, T_1, \ldots, T_{p-1}, \frac{1}{\Delta}],$$

and the homomorphism of group $\mathbb{F}_p$-schemes

$$\tilde{\sigma} : \mathbb{G}_{a,\mathbb{F}_p} = \operatorname{Spec} \mathbb{F}_p[X] \to U(\Gamma) = \operatorname{Spec} \mathbb{F}_p[T_0, T_1, \ldots, T_{p-1}, \frac{1}{\Delta}]$$

by

$$T_l \mapsto \Psi_l(X) = 1 - (X - l)^{p-1} : \mathbb{F}_p[T_0, T_1, \ldots, T_{p-1}, \frac{1}{\Delta}] \to \mathbb{F}_p[X] \ (0 \le l < p).$$

Corollary 2.10.(Artin-Schreier theory) *Let R be an $\mathbb{F}_p$-algebra and S a cyclic unramified extension of degree p. Then there exists $a \in R$ such that S is isomorphic to $R[T]/(T^p - T - a)$ and that γ acts on S by $\gamma\alpha = \alpha + 1$. Here α is the image of T in $S = R[T]/(T^p - T - a)$. Moreover $\Psi_0(\alpha) = 1 - \alpha^{p-1}$ generates a normal basis of the cyclic extension S/R.*

Proof. As is known, we have $H^1(R, \mathbb{G}_{a,R}) = 0$. Hence it follows from Corollary 1.7(2) that $[S] \in \operatorname{Ker}[H^1(R, \Gamma) \to H^1(R, U(\Gamma))]$. We obtain the last assertion, noting that $\Psi_0(X) \equiv 1 - T^{p-1} \mod \lambda$.

Remark 2.11.(Artin-Schreier-Witt theory) Let Γ denote a cyclic group of order p^n. Serre [15, Ch.VI, 9] constructed a commutative diagram of group $\mathbb{F}_p$-schemes with exact rows

$$\begin{tikzcd}[ampersand replacement=\&] 0 \arrow[r] \& \Gamma \arrow[r] \arrow[d, "\wr"] \& U(\Gamma)_{\mathbb{F}_p} \arrow[r] \arrow[d, "\tilde{\chi}"] \& (U(\Gamma)/\Gamma)_{\mathbb{F}_p} \arrow[r] \arrow[d] \& 0 \\ 0 \arrow[r] \& \mathbb{Z}/p^n\mathbb{Z} \arrow[r] \& W_{n,\mathbb{F}_p} \arrow[r, "F-1"] \& W_{n,\mathbb{F}_p} \arrow[r] \& 0, \end{tikzcd} \tag{7}$$

using the Artin-Hasse exponential series. We can construct also a commutative diagram of group $\mathbb{F}_p$-schemes with exact rows

$$\begin{tikzcd}[ampersand replacement=\&] 0 \arrow[r] \& \mathbb{Z}/p^n\mathbb{Z} \arrow[r] \arrow[d, "\wr"] \& W_{n,\mathbb{F}_p} \arrow[r, "F-1"] \arrow[d, "\tilde{\sigma}"] \& W_{n,\mathbb{F}_p} \arrow[r] \arrow[d] \& 0 \\ 0 \arrow[r] \& \Gamma \arrow[r] \& U(\Gamma)_{\mathbb{F}_p} \arrow[r] \& (U(\Gamma)/\Gamma)_{\mathbb{F}_p} \arrow[r] \& 0, \end{tikzcd} \tag{8}$$

following the Serre. The diagram (7) and (8) coincide with the diagrams (5) and (6) respectively when $n = 1$.

Let R be an $\mathbb{F}_p$-algebra and S/R an unramified cyclic extension of degree p^n. Then the Artin-Schreier-Witt theory asserts that there exist morphisms $\operatorname{Spec} S \to W_{n,\mathbb{F}_p}$ and $\operatorname{Spec} R \to W_{n,\mathbb{F}_p}$ such that the diagram

$$\begin{tikzcd} \operatorname{Spec} S \arrow[r] \arrow[d] & W_{n,\mathbb{F}_p} \arrow[d, "F-1"] \\ \operatorname{Spec} R \arrow[r] & W_{n,\mathbb{F}_p} \end{tikzcd}$$

is cartesian. Moreover the cyclic extension S/R has a normal basis.

Remark 2.12.(Kummer-Artin-Schreier-Witt theory of degree p^2) Let Γ denotes a cyclic group of order p^2. Put $A = \mathbb{Z}_{(p)}[\zeta]$, where ζ denotes a primitive p^2-th root of unity. Then it was shown independently by Green-Matignon [3] and [13] that there exists an exact sequence of group A-schemes

$$(\#) \qquad 0 \longrightarrow \operatorname{Ker} \Psi_2 \longrightarrow \mathcal{W}_2 \xrightarrow{\Psi_2} \mathcal{V}_2 \longrightarrow 0$$

such that

(1) the generic fiber of (#) is isomorphic to the Kummer sequence

$$0 \longrightarrow \boldsymbol{\mu}_{p^2} \longrightarrow (\mathbb{G}_m)^2 \xrightarrow{\Theta_2} (\mathbb{G}_m)^2 \longrightarrow 0.$$

Here

$$\Theta_2 : (\mathbb{G}_{m,\mathbb{Z}})^2 = \operatorname{Spec} \mathbb{Z}[U_0, U_1, \frac{1}{U_0}, \frac{1}{U_1}] \to (\mathbb{G}_{m,\mathbb{Z}})^2 = \operatorname{Spec} \mathbb{Z}[U_0, U_1, \frac{1}{U_0}, \frac{1}{U_1}]$$

is defined by

$$(U_0, U_1) \mapsto (U_0^p, U_0^{-1}U_1^p) : \mathbb{Z}[U_0, U_1, \frac{1}{U_0}, \frac{1}{U_1}] \longrightarrow \mathbb{Z}[U_0, U_1, \frac{1}{U_0}, \frac{1}{U_1}];$$

(2) the special fiber (#) is isomorphic to the Artin-Schreier-Witt sequence

$$0 \longrightarrow \mathbb{Z}/p^2\mathbb{Z} \longrightarrow W_2 \xrightarrow{F-1} W_2 \longrightarrow 0.$$

Furthermore it was shown by [12] that there exists a commutative diagram of group A-schemes with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \Gamma \arrow[r] \arrow[d, "\wr"] & U(\Gamma)_A \arrow[r] \arrow[d, "\tilde{\chi}"] & (U(\Gamma)/\Gamma)_A \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \operatorname{Ker}\Psi_2 \arrow[r] & \mathcal{W}_2 \arrow[r, "\Psi_2"] & \mathcal{V}_2 \arrow[r] & 0.
\end{tikzcd}$$

3. Twisted Kummer theory

Throughout the section, n denotes an integer ≥ 3 and Γ stands for a cyclic group of order n. We put $\zeta = e^{2\pi i/n}$, $\omega = \zeta + \zeta^{-1}$, $B = \mathbb{Z}[\zeta, 1/n]$ and $A = \mathbb{Z}[\omega, 1/n]$.

3.1. The A-algebra B is isomorphic to $A[t]/(t^2 - \omega t + 1)$. Hence the functor $R \mapsto (R \otimes_A B)^\times$ is represented by the group scheme (the Weil restriction of $\mathbb{G}_{m,B}$ to B/A)

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

with

(a) the multiplication

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

(b) the unit

$$U \mapsto 1,\ V \mapsto 0;$$

(c) the inverse

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

Moreover, the canonical injection $R^\times \to (R \otimes_A B)^\times$ is represented by the homomorphism of group schemes

$$i : \mathbb{G}_{m,A} = \operatorname{Spec} A[T, \frac{1}{T}] \to \prod_{B/A} \mathbb{G}_{m,B} = \operatorname{Spec} A[U, V, \frac{1}{U^2 + \omega UV + V^2}],$$

defined by

$$U \mapsto T,\ V \mapsto 0.$$

On the other hand, the norm map $\mathrm{Nr} : (R \otimes_A B)^\times \to R^\times$ is represented by the homomorphism of group schemes

$$\mathrm{Nr} : \prod_{B/A} \mathbb{G}_{m,B} = \operatorname{Spec} A[U, V, \frac{1}{U^2 + \omega UV + V^2}] \to \mathbb{G}_{m,A} = \operatorname{Spec} A[T, \frac{1}{T}],$$

defined by

$$T \mapsto U^2 + \omega UV + V^2.$$

Put

$$U_{B/A} = \mathrm{Ker}[\mathrm{Nr} : \prod_{B/A} \mathbb{G}_{m,B} \to \mathbb{G}_{m,A}].$$

Then we have

$$U_{B/A} = \operatorname{Spec} A[U, V]/(U^2 + \omega UV + V^2 - 1)$$

with

(a) the multiplication

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

(b) the unit

$$U \mapsto 1,\ V \mapsto 0;$$

(c) the inverse

$$U \mapsto U + \omega V,\ V \mapsto -V.$$

By the definition, we have an exact sequence of group A-schemes

$$0 \longrightarrow U_{B/A} \longrightarrow \prod_{B/A} \mathbb{G}_{m,B} \xrightarrow{\mathrm{Nr}} \mathbb{G}_{m,A} \longrightarrow 0.$$

Moreover, a homomorphism of group A-schemes

$$\gamma : \prod_{B/A} \mathbb{G}_{m,B} = \operatorname{Spec} A[U, V, \frac{1}{U^2 + \omega UV + V^2}] \to U_{B/A} = \operatorname{Spec} A[U, V]/(U^2 + \omega UV + V^2 - 1)$$

is defined by

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

We obtain an exact sequence of group A-schemes

$$0 \longrightarrow \mathbb{G}_{m,A} \xrightarrow{i} \prod_{B/A} \mathbb{G}_{m,B} \xrightarrow{\gamma} U_{B/A} \longrightarrow 0.$$

3.2. Assume that $1 \leq l < n/2$. The homomorphism

$$\chi_l : U(\varGamma)_B = \operatorname{Spec} B[T_0, T_1, \dots, T_{n-1}, \frac{1}{\varDelta}] \to \mathbb{G}_{m,B} = \operatorname{Spec} B[U, \frac{1}{U}]$$

defined by

$$U \mapsto \sum_{k=0}^{n-1} \zeta^{kl} T_k$$

induces a homomorphism of group A-schemes $\chi_l : U(\varGamma)_A \to \prod_{B/A} \mathbb{G}_{m,B}$. More precisely

$$\chi_l : U(G)_A = \operatorname{Spec} A[T_0, T_1, \dots, T_{n-1}, \frac{1}{\varDelta}] \to \prod_{B/A} \mathbb{G}_{m,B} = \operatorname{Spec} A[U, V, \frac{1}{U^2 + \omega UV + V^2}]$$

is defined by

$$U \mapsto \sum_{k=0}^{n-1} \frac{\zeta^{kl-1} - \zeta^{-kl+1}}{\zeta^{-1} - \zeta} T_k, \ V \mapsto \sum_{k=0}^{n-1} \frac{\zeta^{kl} - \zeta^{-kl}}{\zeta - \zeta^{-1}} T_k :$$
$$A[U, V, \frac{1}{U^2 + \omega UV + V^2}] \to A[T_0, T_1, \dots, T_{n-1}, \frac{1}{\varDelta}].$$

A homomorphism

$$\varepsilon : U(\varGamma) = \operatorname{Spec} \mathbb{Z}[T_0, T_1, \dots, T_{n-1}, \frac{1}{\varDelta}] \to \mathbb{G}_{m,\mathbb{Z}} = \operatorname{Spec} \mathbb{Z}[U, \frac{1}{U}]$$

is defined by

$$U \mapsto \sum_{k=0}^{n-1} T_k : \mathbb{Z}[U, \frac{1}{U}] \to \mathbb{Z}[T_0, T_1, \dots, T_{n-1}, \frac{1}{\varDelta}].$$

If n is even, then a homomorphism

$$\eta : U(\varGamma) = \operatorname{Spec} \mathbb{Z}[T_0, T_1, \dots, T_{n-1}, \frac{1}{\varDelta}] \to \mathbb{G}_{m,\mathbb{Z}} = \operatorname{Spec} \mathbb{Z}[U, \frac{1}{U}]$$

is defined by

$$U \to \sum_{k=0}^{n-1} (-1)^k T_k : \mathbb{Z}[U, \frac{1}{U}] \to \mathbb{Z}[T_0, T_1, \dots, T_{n-1}, \frac{1}{\varDelta}].$$

3.3. Assume now that n *is odd.* Put $r = (n-1)/2$. Then the homomorphism

$$\chi = (\varepsilon, \chi_1, \chi_2, \dots, \chi_r) : U(\varGamma)_A \to \mathbb{G}_{m,A} \times_A \prod_{B/A} \mathbb{G}^r_{m,B}$$

is an isomorphism. In fact,

$$\chi : U(\mathit{\Gamma})_A = \operatorname{Spec} A[T_0, T_1, \dots, T_{n-1}, \frac{1}{\mathit{\Delta}}] \to \mathbb{G}_{m,A} \times_A \prod_{B/A} \mathbb{G}^r_{m,B} =$$

$$\operatorname{Spec} A[U_0, U_1, \dots, U_m, V_1, \dots, V_m, \frac{1}{U_0}, \frac{1}{U_1^2 + \omega U_1 V_1 + V_1^2}, \dots, \frac{1}{U_r^2 + \omega U_r V_r + V_r^2}]$$

is defined by

$$U_0 \mapsto \sum_{k=0}^{n-1} T_k,\ U_l \mapsto \sum_{k=0}^{n-1} \frac{\zeta^{kl-1} - \zeta^{-kl+1}}{\zeta^{-1} - \zeta} T_k,\ V_l \mapsto \sum_{k=0}^{n-1} \frac{\zeta^{kl} - \zeta^{-kl}}{\zeta - \zeta^{-1}} T_k \ (1 \leq l \leq r),$$

and the inverse s of χ is given by

$$T_l \mapsto \frac{1}{n}\Big\{U_0 + \sum_{k=1}^{(n-1)/2} \zeta^{-kl}(U_k + \zeta V_k) + \sum_{k=1}^{(n-1)/2} \zeta^{kl}(U_k + \zeta^{-1} V_k)\Big\} \ (0 \leq l \leq r).$$

We define an endomorphism $\nu : \prod_{B/A} \mathbb{G}_{m,B} \to \prod_{B/A} \mathbb{G}_{m,B}$ by

$$U \mapsto \frac{1}{\zeta^{-1} - \zeta} \frac{\zeta^{-1}(U + \zeta V)^n - \zeta(U + \zeta^{-1} V)^n}{(U^2 + \omega UV + V^2)^{(n-1)/2}},\ V \mapsto \frac{1}{\zeta - \zeta^{-1}} \frac{(U + \zeta V)^n - (U + \zeta^{-1} V)^n}{(U^2 + \omega UV + V^2)^{(n-1)/2}}.$$

Then ν is an isogeny of degree n. Furthermore we obtain commutative diagrams of group A-schemes with exact rows and columns

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
 & \operatorname{Ker} n \arrow[r, "\sim"] \arrow[d] & \operatorname{Ker} \nu \arrow[d] & & \\
0 \arrow[r] & U_{B/A} \arrow[r] \arrow[d, "n"] & \prod_{B/A} \mathbb{G}_{m,B} \arrow[r, "\mathrm{Nr}"] \arrow[d, "\nu"] & \mathbb{G}_{m,A} \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & U_{B/A} \arrow[r] \arrow[d] & \prod_{B/A} \mathbb{G}_{m,B} \arrow[r, "\mathrm{Nr}"] \arrow[d] & \mathbb{G}_{m,A} \arrow[r] & 0 \\
 & 0 & 0 & &
\end{tikzcd} \tag{9}$$

and

(10)
$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & \\
 & & \operatorname{Ker}\nu \arrow[r, "\sim"] \arrow[d] & \operatorname{Ker} n \arrow[d] & \\
0 \arrow[r] & \mathbb{G}_{m,A} \arrow[r, "i"] \arrow[d, equal] & \prod_{B/A}\mathbb{G}_{m,B} \arrow[r, "\gamma"] \arrow[d, "\nu"] & U_{B/A} \arrow[r] \arrow[d, "n"] & 0 \\
0 \arrow[r] & \mathbb{G}_{m,A} \arrow[r, "i"] & \prod_{B/A}\mathbb{G}_{m,B} \arrow[r, "\gamma"] \arrow[d] & U_{B/A} \arrow[r] \arrow[d] & 0 \\
 & & 0 & 0 & .
\end{tikzcd}$$

3.4. Define now a homomorphism of group A-schemes $\sigma : \prod_{B/A}\mathbb{G}_{m,B} \to \mathbb{G}_{m,A} \times_A \prod_{B/A}\mathbb{G}^r_{m,B}$ by

$$U_0 \mapsto 1,\ U_l \mapsto \frac{\zeta^{-1}(U+\zeta V)^l - \zeta(U+\zeta^{-1}V)^l}{\zeta^{-1}-\zeta},\ V_l \mapsto \frac{(U+\zeta V)^l - (U+\zeta^{-1}V)^l}{\zeta-\zeta^{-1}}\ (1 \le l \le r).$$

Put $\sigma_1 = s \circ \sigma : \prod_{B/A}\mathbb{G}_{m,B} \to U(\mathit{\Gamma})$. Then the homomorphism σ_1 is defined by

$$T_l \mapsto \frac{1}{n}\Big\{1 + \sum_{k=1}^{(n-1)/2} \zeta^{-kl}(U+\zeta V)^k + \sum_{k=1}^{(n-1)/2} \zeta^{kl}(U+\zeta^{-1}V)^k\Big\}\ (0 \le l \le r),$$

and σ_1 is a section of $\chi_1 : U(\mathit{\Gamma}) \to \prod_{B/A}\mathbb{G}_{m,B}$. Moreover we have a commutative diagrams of group A-schemes with exact rows

(11)
$$\begin{tikzcd}
0 \arrow[r] & \mathit{\Gamma} \arrow[r] \arrow[d] & U(\mathit{\Gamma})_A \arrow[r] \arrow[d, "\chi_1"] & (U(\mathit{\Gamma})/\mathit{\Gamma})_A \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \operatorname{Ker}\nu \arrow[r] & \prod_{B/A}\mathbb{G}_{m,B} \arrow[r, "\nu"] & \prod_{B/A}\mathbb{G}_{m,B} \arrow[r] & 0
\end{tikzcd}$$

and

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Ker}\nu \arrow[r] \arrow[d] & \prod_{B/A} \mathbb{G}_{m,B} \arrow[r, "\nu"] \arrow[d, "\sigma_1"] & \prod_{B/A} \mathbb{G}_{m,B} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \varGamma \arrow[r] & U(\varGamma)_A \arrow[r] & (U(\varGamma)/\varGamma)_A \arrow[r] & 0.
\end{tikzcd} \tag{12}$$

Proposition 3.5. *The homomorphism $\chi_1 : \varGamma \to \operatorname{Ker}\nu$ is an isomorphism, and the inverse is given by $\sigma_1 : \operatorname{Ker}\nu \to \varGamma$.*

Proof. For each l, put

$$E_l(U,V) = \frac{1}{n}\Big\{1 + \sum_{k=1}^{(n-1)/2} \zeta^{-kl}(U+\zeta V)^k + \sum_{k=1}^{(n-1)/2} \zeta^{-kl}(U+\zeta^{-1}V)^k\Big\}$$

and

$$u_l = \frac{\zeta^{l-1} - \zeta^{-l+1}}{\zeta^{-1} - \zeta},\ v_l = \frac{\zeta^{l} - \zeta^{-l}}{\zeta - \zeta^{-1}}.$$

Then we have

$$E_l(u_j,v_j) = \begin{cases} 1 & (j \equiv l \mod n) \\ 0 & (j \not\equiv l \mod n). \end{cases}$$

Hence the result.

Corollary 3.6.(twisted Kummer theory of odd degree) *Let R be an A-algebra and S an unramified cyclic extension of degree n. Then the following conditions are equivalent.*

(a) *the cyclic extension S/R has a normal basis*;

(b) *there exist $u, v \in R$ with $u^2 + \omega uv + v^2 = 1$ such that*

(1) *S is isomorphic to*

$$R[U,V]/(\frac{\zeta^{-1}(U+\zeta V)^n - \zeta(U+\zeta^{-1}V)^n}{\zeta^{-1}-\zeta} - u, \frac{(U+\zeta V)^n - (U+\zeta^{-1}V)^n}{\zeta - \zeta^{-1}} - v);$$

(2) $\alpha^2 + \omega\alpha\beta + \beta^2 = 1$;

(3) *γ acts on S by $\gamma(\alpha,\beta) = (-\beta, \alpha + \omega\beta)$.*

Here α and β are the images of U and V in S, respectively.

If it is the case, $\frac{1}{n}\Big\{1 + \sum_{k=1}^{(n-1)/2} (\alpha+\zeta\beta)^k + \sum_{k=1}^{(n-1)/2} (\alpha+\zeta^{-1}\beta)^k\Big\}$ generates a normal basis of the cyclic extension S/R.

Proof. We obtain a commutative diagram of group A-schemes with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \varGamma \arrow[r] \arrow[d, "\wr"] & U(\varGamma)_A \arrow[r] \arrow[d] & (U(\varGamma)/\varGamma)_A \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \operatorname{Ker} n \arrow[r] & U_{B/A} \arrow[r, "n"] & U_{B/A} \arrow[r] & 0,
\end{tikzcd} \tag{13}$$

combining the commutative diagrams with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \mathit{\Gamma} \arrow[r] \arrow[d, "\wr"] & U(\mathit{\Gamma})_A \arrow[r] \arrow[d, "\chi_1"] & (U(\mathit{\Gamma})/\mathit{\Gamma})_A \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \operatorname{Ker}\nu \arrow[r] & \prod_{B/A}\mathbb{G}_{m,B} \arrow[r, "\nu"] & \prod_{B/A}\mathbb{G}_{m,B} \arrow[r] & 0
\end{tikzcd}$$

and

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Ker}\nu \arrow[r] \arrow[d, "\wr"] & \prod_{B/A}\mathbb{G}_{m,B} \arrow[r, "\nu"] \arrow[d, "\gamma"] & \prod_{B/A}\mathbb{G}_{m,B} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \operatorname{Ker} n \arrow[r] & U_{B/A} \arrow[r, "n"] & U_{B/A} \arrow[r, "n"] & 0.
\end{tikzcd}$$

We obtain also a commutative diagram of group A-schemes with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Ker} n \arrow[r] \arrow[d, "\wr"] & U_{B/A} \arrow[r, "n"] \arrow[d] & U_{B/A} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathit{\Gamma} \arrow[r] & U(\mathit{\Gamma})_A \arrow[r] & (U(\mathit{\Gamma})/\mathit{\Gamma})_A \arrow[r] & 0,
\end{tikzcd} \tag{14}$$

combining the commutative diagrams with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Ker} n \arrow[r] \arrow[d, "\wr"] & U_{B/A} \arrow[r, "n"] \arrow[d, "\chi_1"] & U_{B/A} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \operatorname{Ker}\nu \arrow[r] & \prod_{B/A}\mathbb{G}_{m,B} \arrow[r, "\nu"] & \prod_{B/A}\mathbb{G}_{m,B} \arrow[r] & 0
\end{tikzcd}$$

and

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Ker}\nu \arrow[r] \arrow[d, "\wr"] & \prod_{B/A}\mathbb{G}_{m,B} \arrow[r, "\nu"] \arrow[d, "\sigma_1"] & \prod_{B/A}\mathbb{G}_{m,B} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathit{\Gamma} \arrow[r] & U(\mathit{\Gamma})_A \arrow[r] & (U(\mathit{\Gamma})/\mathit{\Gamma})_A \arrow[r] & 0.
\end{tikzcd}$$

Applying Corollary 1.7 to (13) and (14), we obtain the assertion.

3.7. We complete now the statement of [16, Cor.3.12], after recalling an equivariant compactification of the isogeny $n : U_{B/A} \to U_{B/A}$, constructed in [16, 2.7].

A rational map of A-schemes

$$\iota : U_{B/A} = \operatorname{Spec} A[U,V]/(U^2 - \omega UV + V^2 - 1) \to \mathbb{P}^1_A = \operatorname{Proj} A[T_1, T_2]$$

is defined by

$$T = \frac{T_1}{T_2} \mapsto \frac{1-U}{V} = \frac{\omega U + V}{1+U}.$$

The inverse of ι is given by

$$U \mapsto \frac{T_1^2 - T_2^2}{T_1^2 + \omega T_1 T_2 + T_2^2},\ V \mapsto \frac{2T_1T_2 + \omega T_2^2}{T_1^2 + \omega T_1 T_2 + T_2^2}.$$

The rational map ι is defined everywhere and an open immesrion.

Define a rational map $\nu : \operatorname{Proj} A[T_1, T_2] \to \operatorname{Proj} A[T_1, T_2]$ by

$$(T_1, T_2) \mapsto \Big(\frac{\zeta^{-1}(T_1 + \zeta T_2)^n - \zeta(T_1 + \zeta^{-1}T_2)^n}{\zeta^{-1} - \zeta}, -\frac{(T_1 + \zeta T_2)^n - (T_1 + \zeta^{-1}T_2)^n}{\zeta^{-1} - \zeta}\Big).$$

Then we obtain a commutative diagram of rational maps

$$\begin{tikzcd} U_{B/A} \arrow[r, "\iota"] \arrow[d, "n"'] & \mathbb{P}^1_A \arrow[d, "\nu"] \\ U_{B/A} \arrow[r, "\iota"'] & \mathbb{P}^1_A. \end{tikzcd} \tag{15}$$

Moreover, Γ acts on $U_{B/A}$ and on $\mathbb{P}^1_A$ by

$$\gamma : U \mapsto -V,\ V \mapsto U + \omega V$$

and by

$$\gamma : T_1 \mapsto T_1 - T_2,\ T_2 \mapsto T_1 + (1 + \omega)T_2,$$

respectively. The commutative diagram (15) is Γ-equivariant.

Corollary 3.8. *Let R be a local A-algebra and S an unramified cyclic extension of degree n. Assume that one of the following conditions is satisfied:*

(1) *the unramified extension $S \otimes_R k/k$ is not trivial, where k denotes the residue field of R.*

(2) 2 *is invertible in R.*

Then there exists $c \in R$ with $c^2 + \omega c + 1 \in R^\times$ such that S is isomorphic to

$$R[T]/(\frac{\zeta^{-1}(T + \zeta)^n - \zeta(T + \zeta^{-1})^n}{\zeta^{-1} - \zeta} - c\frac{(T + \zeta)^n - (T + \zeta^{-1})^n}{\zeta - \zeta^{-1}})$$

and that γ acts on S by $\gamma\tau = \dfrac{\tau - 1}{\tau + 1 + \omega}$. Here τ is the images of T in S. Furthermore,

$$\frac{1}{n}\Big\{1 + \sum_{k=1}^{(n-1)/2}\Big(\frac{\tau + \zeta}{\tau + \zeta^{-1}}\Big)^k + \sum_{k=1}^{(n-1)/2}\Big(\frac{\tau + \zeta^{-1}}{\tau + \zeta}\Big)^k\Big\}$$

generates a normal basis of the cyclic extension S/R.

Proof. The cyclic extension S/R has normal basis since R is a local ring. Then, by Corollary 3.6, there exist $u, v \in R$ with $u^2 + \omega uv + v^2 = 1$ such that

(1) S is isomorphic to

$$R[U,V]/(\frac{\zeta^{-1}(U+\zeta V)^n-\zeta(U+\zeta^{-1}V)^n}{\zeta^{-1}-\zeta}-u, \frac{(U+\zeta V)^n-(U+\zeta^{-1}V)^n}{\zeta-\zeta^{-1}}-v);$$

(2) $\alpha^2+\omega\alpha\beta+\beta^2=1$;
(3) γ acts on S by $\gamma(\alpha,\beta)=(-\beta,\alpha+\omega\beta)$.
Here α and β denotes the images of U and V in S, respectively.

Let $\mathfrak{m}$ denote the maximal ideal of R. Assume first that v is invertible in R. Put $c=(1+u)/v$. Then we have

$$c^2+\omega c+1=\frac{2+2u+\omega v}{v^2}, \ \frac{1}{c^2+\omega c+1}=\frac{(-2+2u+\omega)v^2}{\omega^2-4}.$$

Furthermore β is invertible since $v=\{(\alpha+\zeta\beta)^n-(\alpha+\zeta^{-1}\beta)^n\}/(\zeta-\zeta^{-1})$ is invertible. Let τ denote the image of T in

$$R[T]/(\frac{\zeta^{-1}(T+\zeta)^n-\zeta(T+\zeta^{-1})^n}{\zeta^{-1}-\zeta}-c\frac{(T+\zeta)^n-(T+\zeta^{-1})^n}{\zeta-\zeta^{-1}}).$$

Then an isomorphism of R-algebras

$$\varphi: R[T]/(\frac{\zeta^{-1}(T+\zeta)^n-\zeta(T+\zeta^{-1})^n}{\zeta^{-1}-\zeta}-c\frac{(T+\zeta)^n-(T+\zeta^{-1})^n}{\zeta-\zeta^{-1}})\rightarrow$$
$$S=R[U,V]/(\frac{\zeta^{-1}(U+\zeta V)^n-\zeta(U+\zeta^{-1}V)^n}{\zeta^{-1}-\zeta}-u, \frac{(U+\zeta V)^n-(U+\zeta^{-1}V)^n}{\zeta-\zeta^{-1}}-v)$$

is defined by

$$\tau\mapsto\frac{1+\alpha}{\beta}.$$

In fact, the inverse of φ is given by

$$\alpha\mapsto\frac{\tau^2-1}{\tau^2+\omega\tau+1}, \ \beta\mapsto\frac{2\tau+\omega}{\tau^2+\omega\tau+1}.$$

These imply the last two assertions.

Now assume that the unramified extension $S\otimes_R k/k$ is not trivial. Then $v\notin\mathfrak{m}$, that is, v is invertible in R.

At last assume that 2 is invertible in R and v is not invertible in R. Then $1-u^2\in\mathfrak{m}$. If $1-u\in\mathfrak{m}$, then $1+u\notin\mathfrak{m}$. Putting $c=v/(1+u)$, we can proceed the argument mentioned above. If $1+u\notin\mathfrak{m}$, then $1-u\in\mathfrak{m}$, and therefore we can replace (u,v) by $(-u,-v)$ since we have $(-u,-v)=(u,v)(-1,0)^n$ in $U_{B/A}(R)$.

Remark 3.9. We have

$$\begin{pmatrix}1 & -1\\ 1 & 1+\omega\end{pmatrix}^k=\frac{1}{\zeta-\zeta^{-1}}\begin{pmatrix}-\zeta^{-1}(1+\zeta)^k+\zeta(1+\zeta^{-1})^k & -(1+\zeta)^k+(1+\zeta^{-1})^k\\ (1+\zeta)^k-(1+\zeta^{-1})^k & \zeta(1+\zeta)^k-\zeta^{-1}(1+\zeta^{-1})^k\end{pmatrix}$$

and

$$\begin{aligned}\frac{-\zeta^{-1}(1+\zeta)^k+\zeta(1+\zeta^{-1})^k}{\zeta-\zeta^{-1}} &= -\Big(2\cos\frac{\pi}{n}\Big)^{k-1}\sin\frac{(k-2)\pi}{n}\Big/\sin\frac{\pi}{n},\\ \frac{(1+\zeta)^k-(1+\zeta^{-1})^k}{\zeta-\zeta^{-1}} &= \Big(2\cos\frac{\pi}{n}\Big)^{k-1}\sin\frac{k\pi}{n}\Big/\sin\frac{\pi}{n},\\ \frac{\zeta(1+\zeta)^k+\zeta^{-1}(1+\zeta^{-1})^k}{\zeta-\zeta^{-1}} &= \Big(2\cos\frac{\pi}{n}\Big)^{k-1}\sin\frac{(k+2)\pi}{n}\Big/\sin\frac{\pi}{n}.\end{aligned}$$

Put $\eta_k=\sin\frac{k\pi}{n}\Big/\sin\frac{\pi}{n}$. Then, under the notation of 3.8, we have

$$\gamma^k(\tau)=\frac{-\eta_{k-2}\tau-\eta_k}{\eta_k\tau+\eta_{k+2}}$$

for each k. Moreover we obtain a factorization

$$\frac{\zeta^{-1}(T+\zeta)^n-\zeta(T+\zeta^{-1})^n}{\zeta^{-1}-\zeta}-c\frac{(T+\zeta)^n-(T+\zeta^{-1})^n}{\zeta-\zeta^{-1}}=\prod_{k=0}^{n-1}\Big(T-\frac{-\eta_{k-2}\tau-\eta_k}{\eta_k\tau+\eta_{k+2}}\Big).$$

3.10. Assume now that n *is even*, and put $r=n/2-1$. Then the homomorphism

$$\chi=(\varepsilon,\eta,\chi_1,\chi_2,\dots,\chi_r):U(G)_A\to\mathbb{G}^2_{m,A}\times_A\prod_{B/A}\mathbb{G}^r_{m,B}$$

is an isomorphism. In fact,

$$\chi:U(G)_A=\operatorname{Spec}A[T_0,T_1,\dots,T_{n-1},\frac{1}{\Delta}]\to\mathbb{G}^2_{m,A}\times_A\prod_{B/A}\mathbb{G}^r_{m,B}=$$

$$\operatorname{Spec}A[U_0,U_1,\dots,U_r,U_{r+1},V_1,\dots,V_r,\frac{1}{U_0},\frac{1}{U_m},\frac{1}{U_1^2+\omega U_1V_1+V_1^2},\dots,\frac{1}{U_r^2+\omega U_rV_r+V_r^2}]$$

is defined by

$$U_0\mapsto\sum_{k=0}^{n-1}T_k,\ \ U_{r+1}\mapsto\sum_{k=0}^{n-1}(-1)^kT_k,$$

$$U_l\mapsto\sum_{k=0}^{n-1}\frac{\zeta^{kl-1}-\zeta^{-kl+1}}{\zeta^{-1}-\zeta}T_k,\ \ V_l\mapsto\sum_{k=0}^{n-1}\frac{\zeta^{kl}-\zeta^{-kl}}{\zeta-\zeta^{-1}}T_k\ (0<l\le r),$$

and the inverse s of χ is given by

$$T_l\mapsto\frac{1}{n}\Big\{U_0+(-1)^lU_{n/2}+\sum_{k=1}^{n/2-1}\zeta^{-kl}(U_k+\zeta V_k)+\sum_{k=1}^{n/2-1}\zeta^{kl}(U_k+\zeta^{-1}V_k)\Big\}.$$

Define now a homomorphism

$$\nu : \prod_{B/A} \mathbb{G}_{m,B} = \operatorname{Spec} A[U, V, \frac{1}{U^2 + \omega UV + V^2}]$$
$$\to U_{B/A} \times_A \mathbb{G}_{m,A} = \operatorname{Spec} A[U, V, T, \frac{1}{T}]/(U^2 + \omega UV + V^2 - 1)$$

by

$$U \mapsto \frac{1}{\zeta^{-1} - \zeta} \frac{\zeta^{-1}(U + \zeta V)^n - \zeta(U + \zeta^{-1}V)^n}{(U^2 + \omega UV + V^2)^{n/2}}, \; V \mapsto \frac{1}{\zeta - \zeta^{-1}} \frac{(U + \zeta V)^n - (U + \zeta^{-1}V)^n}{(U^2 + \omega UV + V^2)^{n/2}},$$
$$T \mapsto U^2 + \omega UV + V^2.$$

Then ν is an isogeny of degree n. Moreover we obtain a commutative diagram of group A-schemes

$$(16) \qquad \begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
 & \operatorname{Ker} n \arrow[r, "\sim"] \arrow[d] & \operatorname{Ker} \nu \arrow[d] & & \\
0 \arrow[r] & U_{B/A} \arrow[r] \arrow[d, "n"] & \prod_{B/A} \mathbb{G}_{m,B} \arrow[r, "\mathrm{Nr}"] \arrow[d, "\nu"] & \mathbb{G}_{m,A} \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & U_{B/A} \arrow[r] \arrow[d] & U_{B/A} \times_A \mathbb{G}_{m,A} \arrow[r, "\mathrm{pr}"] \arrow[d] & \mathbb{G}_{m,A} \arrow[r] & 0 \\
 & 0 & 0 & & .
\end{tikzcd}$$

Moreover we have a commutative diagram of group A-schemes with exact rows

$$(17) \qquad \begin{tikzcd}
0 \arrow[r] & \Gamma \arrow[r] \arrow[d] & U(\Gamma)_A \arrow[r] \arrow[d, "\chi_1"] & (U(\Gamma)/\Gamma)_A \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \operatorname{Ker} \nu \arrow[r] & \prod_{B/A} \mathbb{G}_{m,B} \arrow[r, "\nu"] & U_{B/A} \times_A \mathbb{G}_{m,A} \arrow[r] & 0.
\end{tikzcd}$$

Proposition 3.11. *The homomorphism $\chi_1 : \Gamma \to \operatorname{Ker} \nu$ is an isomorphism.*

Proof. For each l, put

$$E_l(U, V) = \frac{1}{2n} \Big\{ 2 + \sum_{k=1}^{n-1} \zeta^{-kl} (U + \zeta V)^k + \sum_{k=1}^{n-1} \zeta^{kl} (U + \zeta^{-1} V)^k \Big\}$$

and

$$u_l = \frac{\zeta^{l-1} - \zeta^{-l+1}}{\zeta^{-1} - \zeta},\ v_l = \frac{\zeta^l - \zeta^{-l}}{\zeta - \zeta^{-1}}.$$

Then we have

$$E_l(u_j, v_j) = \begin{cases} 1 & (j \equiv l \mod n) \\ 0 & (j \not\equiv l \mod n). \end{cases}$$

Hence the result.

Applying Corollary 1.7 to (17), we obtain:

Corollary 3.12.(twisted Kummer theory of even degree) *Let R be an A-algebra and S an unramified cyclic extension of degree n. If the cyclic extension S/R has a normal basis, there exist $u, v \in R$ with $u^2 + \omega uv + v^2 = 1$ and $c \in R^\times$ such that S is isomorphic to*

$$R[U,V]/(\frac{1}{\zeta^{-1}-\zeta}\frac{\zeta^{-1}(U+\zeta V)^n - \zeta(U+\zeta^{-1}V)^n}{c^{n/2}} - u, \frac{1}{\zeta-\zeta^{-1}}\frac{(U+\zeta V)^n - (U+\zeta^{-1}V)^n}{c^{n/2}} - v),$$

and that γ acts on S by $\gamma(\alpha, \beta) = (-\beta, \alpha + \omega\beta)$. Here α and β are the images of U and V in S, respectively.

Remark 3.13. Let $\sigma : \prod_{B/A} \mathbb{G}_{B,A} \to U(\Gamma)_A$ be a homorphism of group A-schemes. Then the composite $\eta \circ \sigma$ ia a power of $\mathrm{Nr} : \prod_{B/A} \mathbb{G}_{B,A} \to \mathbb{G}_{m,A}$, and therefore we obtain an inclusion $\mathrm{Ker}\,\nu \subset \mathrm{Ker}\,\eta \circ \sigma$. On the other hand, we have $\eta(\gamma) = -1$.

It follows that there does not exist a homorphism of $\prod_{B/A} \mathbb{G}_{B,A}$ to $U(\Gamma)_A$ which induces an isomorphism of $\mathrm{Ker}\,\nu$ to Γ.

3.14. We conclude the section by constructing an equivariant compactification of the isogeny $\nu : \prod_{B/A} \mathbb{G}_{m,B} \to U_{B/A} \times_A \mathbb{G}_{m,A}$.

(a) An open immersion

$$\iota : \prod_{B/A} \mathbb{G}_{m,B} = \mathrm{Spec}\, A[U, V, \frac{1}{U^2 + \omega UV + V^2}] \to \mathrm{Spec}\, A[\frac{T_1}{T_0}, \frac{T_2}{T_0}] \subset \mathbb{P}^2_A = \mathrm{Proj}\, A[T_0, T_1, T_2]$$

is defined by

$$\frac{T_1}{T_0} \mapsto U,\ \frac{T_2}{T_0} \mapsto V.$$

If R is a local A-algebra, then the map $\iota : (\prod_{B/A} \mathbb{G}_{m,B})(R) \to \mathbb{P}^2(R)$ is given by

$$(u, v) \mapsto (1 : u : v).$$

(b) An open immersion

$$\begin{aligned}\iota : U_{B/A} \times_A \mathbb{G}_{m,A} = \operatorname{Spec} A[U,V]/(U^2+\omega UV+V^2-1) \times_A \operatorname{Spec} A[T, \frac{1}{T}] \\ \to \mathbb{P}^1 \times_A \mathbb{P}^1 = \operatorname{Proj} A[U_1, U_2] \times_A \operatorname{Proj} A[V_1, V_2]\end{aligned}$$

is defined by

$$\frac{U_1}{U_2} \mapsto \frac{1+U}{V} = \frac{\omega U + V}{1-U}, \ \frac{V_1}{V_2} \mapsto T.$$

If R is a local A-algebra, then the map $\iota : U_{B/A}(R) \times \mathbb{G}_m(R) \to \mathbb{P}^1(R) \times \mathbb{P}^1(R)$ is given by

$$((u,v),t) \mapsto \big((1+u:v),(t:1)\big).$$

(c) A rational map

$$\mathbb{P}^2_A = \operatorname{Proj} A[T_0, T_1, T_2] \to \mathbb{P}^1 \times_A \mathbb{P}^1 = \operatorname{Proj} A[U_1, U_2] \times_A \operatorname{Proj} A[V_1, V_2]$$

is defined by

$$U_1 \mapsto \frac{\zeta^{-1}(T_1+\zeta T_2)^{n/2} - \zeta(T_1+\zeta^{-1}T_2)^{n/2}}{\zeta^{-1}-\zeta}, \ U_2 \mapsto \frac{(T_1+\zeta T_2)^{n/2} - (T_1+\zeta^{-1}T_2)^{n/2}}{\zeta-\zeta^{-1}},$$
$$V_1 \mapsto T_1^2 + \omega T_1 T_2 + T_2^2, \ V_2 \mapsto T_0^2.$$

If R is a local A-algebra, then the map $\nu : \mathbb{P}^2(R) \to \mathbb{P}^1(R) \times \mathbb{P}^1(R)$ is given by

$$(t_0 : t_1 : t_2) \mapsto$$
$$\big((\frac{\zeta^{-1}(t_1+\zeta t_2)^{n/2} - \zeta(t_1+\zeta^{-1}t_2)^{n/2}}{\zeta^{-1}-\zeta} : \frac{(t_1+\zeta t_2)^{n/2} - (t_1+\zeta^{-1}t_2)^{n/2}}{\zeta-\zeta^{-1}}), (t_1^2+\omega t_1 t_2+t_2^2 : t_0^2)\big).$$

The rational map ν is defined outside of the locus $(T_0, T_1^2+\omega T_1 T_2+T_2^2) \cup (T_1, T_2)$ and finite of degree n.

It is readily seen that the diagram of rational maps

$$\begin{tikzcd} \prod_{B/A} \mathbb{G}_{m,B} \arrow[r, "\iota"] \arrow[d, "\nu"'] & \mathbb{P}^2_A \arrow[d, "\nu"] \\ U_{B/A} \times_A \mathbb{G}_{m,A} \arrow[r, "\iota"'] & \mathbb{P}^1_A \times_A \mathbb{P}^1_A. \end{tikzcd} \tag{18}$$

is commutative. Moreover Γ acts on $\prod_{B/A} \mathbb{G}_{m,B}$ by

$$\gamma : U \mapsto -V, \ V \mapsto U + \omega V.$$

Define now an action of Γ on $\mathbb{P}^2_A$ by

$$T_0 \mapsto T_0,\ T_1 \mapsto -T_2,\ T_2 \mapsto T_1 + \omega T_2.$$

Then the commutative diagram (18) is Γ-equivariant.

Remark 3.15. Let K be a field over A. The rational function field of $\mathbb{P}^2_K = \operatorname{Proj} K[T_0, T_1, T_2]$ is given by $K(s,t)$ by the identification $s = T_0/T_2$ and $t = T_1/T_2$. On the other hand, the rational function field of $\mathbb{P}^1_K \times_K \mathbb{P}^1_K = \operatorname{Proj} K[U_1, U_2] \times_K \operatorname{Proj} K[V_1, V_2]$ is given by $K(u,v)$ by the identification $u = U_1/U_2$ and $v = V_1/V_2$. The rational map $\nu : \mathbb{P}^2_K \to \mathbb{P}^1_K \times_K \mathbb{P}^1_K$ defines an embedding of fields $K(u,v) \to K(s,t)$. The extension $K(s,t)/K(u,v)$ is cyclic of degree n. More precisely, we have

$$\frac{\zeta^{-1}(t+\zeta)^{n/2} - \zeta(t+\zeta^{-1})^{n/2}}{\zeta^{-1} - \zeta} - u\frac{(t+\zeta)^{n/2} - (t+\zeta^{-1})^{n/2}}{\zeta - \zeta^{-1}},\ s^2 = v(t^2 + \omega t + 1),$$

and γ acts on $K(s,t)$ by

$$t \mapsto -\frac{1}{t+\omega},\ s \mapsto \frac{s}{t+\omega}.$$

Furhtermore we have

$$\begin{pmatrix} 0 & -1 \\ 1 & \omega \end{pmatrix}^k = \frac{1}{\zeta - \zeta^{-1}} \begin{pmatrix} -\zeta^{k-1} + \zeta^{k-1} & -\zeta^k + \zeta^{-k} \\ \zeta^k - \zeta^{-k} & \zeta^{k+1} - \zeta^{-k-1} \end{pmatrix}$$

for each k. Put

$$\eta_k = \frac{\zeta^k - \zeta^{-k}}{\zeta - \zeta^{-1}} = \sin\frac{2k\pi}{n} \Big/ \sin\frac{2\pi}{n}.$$

Then we have

$$\gamma^k(t) = \frac{-\eta_{k-1}t - \eta_k}{\eta_k t + \eta_{k+1}},\ \gamma^k(s) = \frac{s}{\eta_k t + \eta_{k+1}}$$

for each k. Moreover we obtain a factorization

$$\frac{\zeta^{-1}(T+\zeta)^{n/2} - \zeta(T+\zeta^{-1})^{n/2}}{\zeta^{-1} - \zeta} - u\frac{(T+\zeta)^{n/2} - (T+\zeta^{-1})^{n/2}}{\zeta - \zeta^{-1}} = \prod_{k=0}^{n/2-1}\Big(T - \frac{-\eta_{k-1}t - \eta_k}{\eta_k t + \eta_{k+1}}\Big).$$

The minimal polynomial of s over $K(u,v)$ is given by

$$\prod_{k=0}^{n-1}\Big(T - \frac{s}{\eta_k t + \eta_{k+1}}\Big) = \prod_{k=0}^{n/2-1}\Big\{T^2 - \Big(\frac{s}{\eta_k t + \eta_{k+1}}\Big)^2\Big\}.$$

By expansion we obtain a polynomial closely related to the generic polynomial for cyclic extensions of degree n, discovered by Hashimoto-Rikuna [5], or to the Chebyshev polynomial of degree n, noting that

$$\Big(\frac{-\eta_{k-1}t - \eta_k}{\eta_k t + \eta_{k+1}} + \zeta\Big)\Big(\frac{-\eta_{k-1}t - \eta_k}{\eta_k t + \eta_{k+1}} + \zeta^{-1}\Big) = \frac{t^2 + \omega t + 1}{(\eta_k t + \eta_{k+1})^2} = \frac{1}{v}\Big(\frac{s}{\eta_k t + \eta_{k+1}}\Big)^2.$$

4. Twisted Kummer-Artin-Schreier theory

Throughout the section, p denotes a prime number ≥ 3 and Γ stands for a cyclic group of order p. We put $\zeta = e^{2\pi i/p}$, $\omega = \zeta + \zeta^{-1}$, $\lambda = \zeta - \zeta^{-1}$, $B = \mathbb{Z}[\zeta]$ and $A = \mathbb{Z}[\omega]$.

First we recall the twisted Kummer-Artin-Schreier thoery, estabilshed in [16, Section 4].

4.1. A commutative group A-scheme $G_{B/A}$ is defined by

$$G_{B/A} = \operatorname{Spec} A[X,Y]/(X^2 + \omega XY + Y^2 - Y)$$

with
(a) the multiplication

$$X \mapsto X \otimes 1 + 1 \otimes X - \omega X \otimes X - 2X \otimes Y - 2Y \otimes X - \omega Y \otimes Y,$$
$$Y \mapsto Y \otimes 1 + 1 \otimes Y + (\omega^2 - 2)Y \otimes Y + \omega X \otimes Y + \omega Y \otimes X + 2X \otimes X;$$

(b) the unit

$$X \mapsto 0,\ Y \mapsto 0;$$

(c) the inverse

$$X \mapsto -X - \omega Y,\ Y \mapsto Y.$$

Put now

$$\Theta(T) = \sum_{i=0}^{\frac{p-1}{2}} \binom{p}{i} (-1)^i T^{p-2i}.$$

Then we have

$$\lambda^p = \Theta(\zeta) - \Theta(\zeta^{-1}).$$

Furthermore, put

$$\theta = \Theta(\zeta),\ \tilde{B} = A[\theta] \subset B$$

and

$$\tilde{\omega} = \operatorname{Tr}_{B/A} \theta = \Theta(\zeta) + \Theta(\zeta^{-1}),\ \tilde{\eta} = \operatorname{Nr}_{B/A} \theta = \Theta(\zeta)\Theta(\zeta^{-1}).$$

A commutative group A-scheme $G_{\tilde{B}/A}$ is defined by

$$G_{\tilde{B}/A} = \operatorname{Spec} A[X,Y]/(X^2 + \tilde{\omega} XY + \tilde{\eta} Y^2 - Y)$$

with
(a) the multiplication

$$X \mapsto X \otimes 1 + 1 \otimes X - \tilde{\omega} X \otimes X - 2\tilde{\eta} X \otimes Y - 2\tilde{\eta} Y \otimes X - \tilde{\omega}\tilde{\eta} Y \otimes Y,$$
$$Y \mapsto Y \otimes 1 + 1 \otimes Y + (\tilde{\omega}^2 - 2\tilde{\eta})Y \otimes Y + \tilde{\omega} X \otimes Y + \tilde{\omega} Y \otimes X + 2X \otimes X;$$

(b) the unit

$$X \mapsto 0,\ Y \mapsto 0;$$

(c) the inverse

$$X \mapsto -X - \tilde{\omega}Y,\ Y \mapsto Y.$$

We define also a homomorphism of group A-schemes

$$\Psi : G_{B/A} = \operatorname{Spec} A[X,Y]/(X^2+\omega XY+Y^2-Y) \to G_{\tilde{B}/A} = \operatorname{Spec} A[X,Y]/(X^2+\tilde{\omega}XY+\tilde{\eta}Y^2-Y)$$

by

$$\begin{aligned} X &\mapsto \Xi(X,Y) = \frac{1}{\lambda^{2p}}\Big[-\Theta(\zeta^{-1})\big\{1+\lambda(X+\zeta Y)\big\}^p + \tilde{\omega} - \Theta(\zeta)\big\{1-\lambda(X+\zeta^{-1}Y)\big\}^p\Big],\\ Y &\mapsto \Upsilon(X,Y) = \frac{1}{\lambda^{2p}}\Big[\big\{1+\lambda(X+\zeta Y)\big\}^p - 2 + \big\{1-\lambda(X+\zeta^{-1}Y)\big\}^p\Big]. \end{aligned}$$

The homomorphism Ψ is étale finite of degree p. The exact sequence of group A-schemes

$$0 \longrightarrow \operatorname{Ker}\Psi \longrightarrow G_{B/A} \xrightarrow{\Psi} G_{\tilde{B}/A} \longrightarrow 0$$

is called the twisted Kummer-Artin-Schreier sequence.

4.2. We define a homomorphism of group A-schemes

$$\tilde{\chi} : U(\mathit{\Gamma})_A = \operatorname{Spec} A[T_0,T_1,\dots,T_{p-1},\frac{1}{\mathit{\Delta}}] \to G_{B/A} = \operatorname{Spec} A[X,Y]/(X^2+\omega XY+Y^2-Y)$$

as the composite of the homomorphisms

$$\chi_1 : U(\mathit{\Gamma})_A = \operatorname{Spec} A[T_0,T_1,\dots,T_{p-1},\frac{1}{\mathit{\Delta}}] \to \prod_{B/A}\mathbb{G}_{m,B} = \operatorname{Spec} A[U,V,\frac{1}{U^2+\omega UV+V^2}]$$

defined by

$$U \mapsto \sum_{k=1}^{p-1}\frac{\zeta^{k-1}-\zeta^{-k+1}}{\zeta^{-1}-\zeta}T_k,\ V \mapsto \sum_{k=1}^{p-1}\frac{\zeta^{k}-\zeta^{-k}}{\zeta-\zeta^{-1}}T_k$$

and

$$\gamma : \prod_{B/A}\mathbb{G}_{m,B} = \operatorname{Spec} A[U,V,\frac{1}{U^2+\omega UV+V^2}] \to G_{B/A} = \operatorname{Spec} A[X,Y]/(X^2+\omega XY+Y^2-Y)$$

is defined by

$$X \mapsto \frac{UV}{U^2+\omega UV+V^2},\ Y \mapsto \frac{V^2}{U^2+\omega UV+V^2}.$$

Then the homomorphism $\tilde{\chi}$ is deifined by

$$X \mapsto \frac{\Big(\sum_{k=0}^{p-1}\frac{\zeta^{k-1}-\zeta^{-k+1}}{\zeta^{-1}-\zeta}T_k\Big)\Big(\sum_{k=0}^{p-1}\frac{\zeta^{k}-\zeta^{-k}}{\zeta-\zeta^{-1}}T_k\Big)}{\Big(\sum_{k=0}^{p-1}\zeta^{k}T_k\Big)\Big(\sum_{k=0}^{p-1}\zeta^{-k}T_k\Big)},\ Y \mapsto \frac{\Big(\sum_{k=0}^{p-1}\frac{\zeta^{k}-\zeta^{-k}}{\zeta-\zeta^{-1}}T_k\Big)^2}{\Big(\sum_{k=0}^{p-1}\zeta^{k}T_k\Big)\Big(\sum_{k=0}^{p-1}\zeta^{-k}T_k\Big)}.$$

On the other hand, a homomorphism of group A-schemes

$$\alpha : G_{B/A} = \operatorname{Spec} A[X,Y]/(X^2+\omega XY+Y^2-Y) \to U_{B/A} = \operatorname{Spec} A[U,V]/(U^2+\omega UV+V^2-1)$$

is defined by

$$U \mapsto 1-\omega X-2Y,\ V \mapsto 2X+\omega Y,$$

and a homomorphism of group schemes

$$\chi_1 : U_{B/A} = \operatorname{Spec} A[U,V]/(U^2+\omega UV+V^2-1) \to U(\mathit{\Gamma})_A = \operatorname{Spec} A[T_0,T_1,\dots,T_{p-1},\frac{1}{\mathit{\Delta}}]$$

is defined over $A[1/p]$ by

$$T_l \mapsto E_l(U,V) = \frac{1}{p}\Big\{1+\sum_{k=1}^{(p-1)/2}\zeta^{-kl}(U+\zeta V)^k+\sum_{k=1}^{(p-1)/2}\zeta^{kl}(U+\zeta^{-1}V)^k\Big\}\ (0 \le l < p).$$

Put now $\tilde{E}_l(X,Y) = E_l(1-\omega X-2Y, 2X+\omega Y)$ for each l. Then we have

$$\tilde{E}_l(X,Y) = \frac{1}{p}\Big[1+\sum_{k=1}^{(p-1)/2}\zeta^{-kl}\big\{1+\lambda(X+\zeta Y)\big\}^k+\sum_{k=1}^{(p-1)/2}\zeta^{kl}\big\{1-\lambda(X+\zeta^{-1}Y)\big\}^{-k}\Big].$$

Moreover we obtain an identity in $A[X,Y]/(X^2+\omega XY+Y^2-Y)$

$$\begin{aligned}\tilde{E}_0(X,Y) &= \Big\{\sum_{k=1}^{p-1}\frac{1}{p}\binom{p}{k}\lambda^{k-1}(X+\zeta Y)^{k-1}+\frac{\lambda^{p-1}}{p}(X+\zeta Y)^{p-1}\Big\}\Big\{1-\lambda(X+\zeta^{-1}Y)\Big\}^{\frac{p-1}{2}}\\ &= \Big\{\sum_{k=1}^{p-1}\frac{1}{p}\binom{p}{k}(-\lambda)^{k-1}(X+\zeta^{-1}Y)^{k-1}+\frac{\lambda^{p-1}}{p}(X+\zeta^{-1}Y)^{p-1}\Big\}\Big\{1+\lambda(X+\zeta Y)\Big\}^{\frac{p-1}{2}}.\end{aligned}$$

It follows that $\tilde{E}_l(X,Y) \in A[X,Y]/(X^2+\omega XY+Y^2-Y)$ for each l. Hence a homomorphism of group A-schemes

$$\tilde{\sigma} : G_{B/A} = \operatorname{Spec} A[X,Y]/(X^2+\omega XY+Y^2-Y) \to U(\mathit{\Gamma})_A = \operatorname{Spec} A[T_0,T_1,\dots,T_{p-1},\frac{1}{\mathit{\Delta}}]$$

is defined by

$$T_l \mapsto \tilde{E}_l(X,Y)\ (0 \le l < p).$$

Moreover we have a commutative diagrams of group A-schemes with exact rows

$$\begin{tikzcd} 0 \arrow[r] & \mathit{\Gamma} \arrow[r] \arrow[d] & U(\mathit{\Gamma})_A \arrow[r] \arrow[d, "\tilde{\chi}"] & (U(\mathit{\Gamma})/\mathit{\Gamma})_A \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & \operatorname{Ker}\Psi \arrow[r] & G_{B/A} \arrow[r, "\Psi"] & G_{\tilde{B}/A} \arrow[r] & 0 \end{tikzcd} \tag{19}$$

and

(20)
$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Ker}\Psi \arrow[r] \arrow[d] & G_{B/A} \arrow[r, "\Psi"] \arrow[d, "\tilde{\sigma}"] & G_{\tilde{B}/A} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \varGamma \arrow[r] & U(\varGamma)_A \arrow[r] & (U(\varGamma)/\varGamma)_A \arrow[r] & 0.
\end{tikzcd}$$

Proposition 4.3. *The homomorphism* $\tilde{\chi} : \varGamma \to \operatorname{Ker}\Psi$ *is an isomorphism, and the inverse is given by* $\frac{p+1}{2} \circ \tilde{\sigma} : \operatorname{Ker}\Psi \to \varGamma$.

Proof. For each l, put

$$\xi_l = u_l v_l = \Big(\frac{\zeta^{l-1} - \zeta^{-l+1}}{\zeta^{-1} - \zeta}\Big)\Big(\frac{\zeta^{l} - \zeta^{-l}}{\zeta - \zeta^{-1}}\Big),\ \eta_l = v_l^2 = \Big(\frac{\zeta^{l} - \zeta^{-l}}{\zeta - \zeta^{-1}}\Big)^2.$$

Then we obtain

$$\tilde{E}_{2l}(\xi_l, \eta_l) = \begin{cases} 1 & (j \equiv l \mod p) \\ 0 & (j \not\equiv l \mod p), \end{cases}$$

noting that

$$\tilde{E}_l(UV, V^2) = \frac{1}{p}\Big\{1 + \sum_{k=1}^{(p-1)/2} \zeta^{-kl}(U + \zeta V)^{2k} + \sum_{k=1}^{(p-1)/2} \zeta^{kl}(U + \zeta^{-1}V)^{-2k}\Big\}.$$

Hence the result.

Applying Corollary 1.7 to (19) and (20), we obtain:

Corollary 4.4.(twisted Kummer-Artin-Schreier theory) *Let R be an A-algebra and S an unramified cyclic extension of degree p. Then the following conditions are equivalent.*

(a) *the cyclic extension S/R has a normal basis*;

(b) *there exist $a, b \in R$ with $a^2 + \tilde{\omega}ab + \tilde{\eta}b^2 = b$ such that*

(1) *S is isomorphic to*

$$R[X, Y]/(\Xi(X, Y) - a, \Upsilon(X, Y) - b);$$

(2) $\alpha^2 + \omega\alpha\beta + \beta^2$;

(3) *γ acts on S by* $\gamma(\alpha, \beta) = (-\alpha - \omega\beta, 1 + \omega\alpha + (\omega^2 - 1)\beta)$.

Here α and β are the images of X and Y in S, respectively. If it is the case,

$$\frac{1}{p}\Big[1 + \sum_{k=1}^{(p-1)/2} \big\{1 + \lambda(\alpha + \zeta\beta)\big\}^k + \sum_{k=1}^{(p-1)/2} \big\{1 - \lambda(\alpha + \zeta^{-1}\beta)\big\}^k\Big]$$

generates a normal basis of the cyclic extension S/R.

REFERENCES

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

[2] L. CHILDS, *The group of unramified Kummer extensions of prime degree*, Proc. London Math. Soc. 35 (1977), 407–422.

[3] B. GREEN and M. MATIGNON, *Liftings of Galois covers of smooth curves*, Compositio Math. 113 (1998) 237–272.

[4] A. GROTHENDIECK, *Le groupe de Brauer*, Dix exposés sur la cohomologie des schémas, North-Holland (1968), 46–188.

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

[6] H. ICHIMURA, *On power integral bases of unramified cyclic extensions of prime degree*, J. Algebra 235 (2001), 104–112.

[7] F. KAWAMOTO, *On normal integral bases*, Tokyo J. Math. 7 (1984), 221–231.

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

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

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

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

[12] 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.

[13] T. SEKIGUCHI and N. SUWA, *A note on extensions of algebraic and formal groups IV*, Tôhoku Math. J. 53 (2001), 203–240.

[14] 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.

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

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

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

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

[19] W. C. WATERHOUSE and B. WEISFEILER, *One-dimensional affine group schemes*, J. Algebra 66 (1980), 550–568.